Malware Analysis Appliance by Blue Coat Systems, Inc. Task Details Host: mag2, Sample ID: 718, Task ID: 450008 450008 Task ID: Risk Level: Date Processed 2016-04-08 16:37:33 (UTC) Processing Time: 61.27 seconds Virtual Environment: IntelliVM Execution Arguments: c:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe" Sample ID: Type: basic Owner: admin 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb Label: Date Added: 2016-04-08 16:37:32 (UTC) File Type: PE32:win32:gui 955904 bytes File Size: 4c838f1570b3a7ff6f491e6ec1ef6895 SHA256: 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb Description: Pattern Matching Results 3 Long sleep detected 5 Possible injector Creates malicious events: FakeIE [PUA , Downware] 1 YARA score 1 3 Connects to local host 4 Checks whether debugger is present HTTP connection - response code 404 (file not found) 3 HTTP connection - response code 200 (success) Static Events YARA rule hit: Nonexecutable YARA rule hit: Process/Thread Events Creates process C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe ["C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe"] jscript.dll:eval Calls function: mshtml.dll:document.write Named Object Events Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0 Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1 Creates mutex: \Sessions\1\BaseNamedObjects\!IETld!Mutex Creates mutex: $\verb|\Sessions|1\BaseNamedObjects|\ZonesCounterMutex|$ \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: Creates mutex: $\verb|\Sessions|1| BaseNamedObjects| ZonesLockedCacheCounterMutex| \\$ Creates mutex: \Sessions\1\BaseNamedObjects_!MSFTHISTORY!_ Creates mutex: \Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet files!content.ie5! Creates mutex: \Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies! \Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5! Creates mutex: \Sessions\1\BaseNamedObjects\WininetStartupMutex Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex Creates mutex: \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile \Sessions\1\BaseNamedObjects\!PrivacIE!SharedMemory!Mutex Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects__DDrawExclMode

 Creates mutex:
 \Sessions\1\BaseNamedObjects_DDrawExc1Mode_

 Creates mutex:
 \Sessions\1\BaseNamedObjects_DDrawCheckExc1Mode_

 Creates mutex:
 \Sessions\1\BaseNamedObjects\DDrawDriverObjectListMutex

 Creates mutex:
 \Sessions\1\BaseNamedObjects\DDrawDriverObjectListMutex

Creates mutex: \Sessions\1\BaseNamedObjects\DirectSound Dl1Main mutex (0x00000868) \ 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 mutey:

Creates mutex:

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

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

Creates mutex:

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

Creates mutex: \Sessions\1\BaseNamedObjects\MSIMGSIZECacheMutex

Creates event: \KernelObjects\MaximumCommitCondition

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

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

Creates event: \BaseNamedObjects\BFE_Notify_Event_{fb2792fd-3c83-43f2-a0e0-

dc8ce04e0dfd}

Creates event: \Sessions\1\BaseNamedObjects\DINPUTWINMM

File System Events

Creates: C:\Users\Admin

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

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

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

 $\label{lem:condition} Creates: $$C:\Users\land Admin\land ppData\Roaming\Microsoft\Windows\Cookies$$ Ceates: $$C:\Users\land Admin\land ppData\Local\uMicrosoft\Windows\History$$$

```
Creates
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
   Creates:
C: \verb|Vusers| Admin| AppData| Roaming \verb|Microsoft| Windows| Cookies| admin@baidu[2].txt| txt| C: \verb|Vusers| Admin| AppData| Roaming| Microsoft| Windows| Cookies| Admin| AppData| Roaming| Microsoft| Windows| Microsoft| Windows| Microsoft| Windows| Microsoft| M
   Creates:
                                                     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
    Creates
Files\Content.IE5\266VNL5S\bd_logo1[1].png
                                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\266VNL5S\baidu_jgylogo3[1].gif
                                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\jquery-1.10.2.min_f2fb5194[1].js
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\zbios_62c636fe[1].png
                                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\nuomi_510f7472[1].png
Creates: 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
Files \verb|\| Content.IE5 \verb|\| TZILKL9J \verb|\| async_search_d0d1b2ec[1].js \\
                                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
    Creates:
Files\Content.IE5\TZILKL9J\every_cookie_aa168cb4[1].js
   Creates:
                                                     C:\Users\Admin\AppData\Roaming\Adobe\Flash Player
                                                      C: \space{MinNappDataRoaming\adobe\flash Player\assetCache C: \space{MinNappDataRoaming\adobe\flash Player\assetCache\flash Player\assetCache\flash
    Creates:
    Creates
    Creates
                                                      C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\VU73CBGV\www.baidu[1].xml
   Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\266VNL5S\quickdelete_9c14b01a[1].png
                                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\nu_instant_search_ebeb5baa[1].js
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\env_beb83b45[1].swf
                                                     C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData
    Creates:
                                                     C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Creates:
Explorer\UserData\index.dat
                                                      C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\LQCEJFP0
    Creates:
                                                     C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\94Y0F91B
    Creates:
                                                     C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Q98WTANC
   Creates:
                                                     C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\TPFUMBD0
                                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
    Creates:
Files\Content.IE5\266VNL5S\bdsug_async_1cb857eb[1].js
                                                     C:\Users\Admin\AppData\Roaming\Macromedia
   Creates:
                                                      C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player
    Creates
    Creates:
                                                     C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
   Creates:
                                                     C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\WV4FGR7F
                                                     {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash\ Player\macromedia.com}
   Creates:
                                                     C: \verb|\Users\Admin\AppData\Roaming\Macromedia\Flash| \\
Player\macromedia.com\support
                                                     C:\Users\Admin\AppData\Roaming\Macromedia\Flash
    Creates:
Player\macromedia.com\support\flashplayer
   Creates:
                                                      C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys
                                                      C:\Users\Admin\AppData\Roaming\Macromedia\Flash
   Creates:
Player\mad
                            nedia.com\support\flashplayer\sys\settings.sxx
   Creates:
                                                      {\tt C:\Wsers\Admin\AppData\Roaming\Macromedia\Flash}
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
    Creates:
                                                      C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
   Creates:
                                                      C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\WV4FGR7F\s1.bdstatic.com
                                                      C:\Users\Admin\AppData\Roaming\Macromedia\Flash
    Creates
Player\#SharedObjects\WV4FGR7F\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                                                     C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Creates:
Explorer\UserData\LQCEJFPO\userDataBIDUPSID[1].xml
                                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
    Creates:
    Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\Historv\Historv.IE5\MSHist012016040820160409
    Creates:
C: \verb|Visers| Admin App Data \verb|Local| Microsoft| Windows \verb|History| IE5 \verb|MSHist012016040820160409| index.dat| Admin App Data \verb|Local| Microsoft| Windows \verb|History| IE5 \verb|MSHist012016040820160409| index.dat| Admin App Data \verb|Local| Microsoft| Windows \verb|History| IE5 \verb|MSHist012016040820160409| index.dat| Admin App Data \verb|Local| Microsoft| Windows Admin App Data \verb|Local| Microsoft| Windows Admin App Data \verb|Local| Microsoft| Windows Admin App Data Admin Admin App Data Admin Admin App Data Admin Admin App Data Admin 
   Creates:
                                                     C:\Users\Admin\Favorites
                                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
    Creates:
Files\Content.IE5\WM60WM90\baiduia_b45d552b[1].js
                                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
    Creates:
Files\Content.IE5\VB8EH8F1\favicon[1].ico
                                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Creates:
Files\Content.IE5\VB8EH8F1\favicon[2].ico
    Creates:
                                                     C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
                                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
    Creates
Files\Content.IE5\TZILKL9J\JSocket_9a52fc3e[1].swf
                                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\union[1].gif
                                                     C:\Windows\Prefetch\62DDFBF757BE511F30B6D330963C1-E2075B81.pf
   Opens:
    Opens:
                                                      C:\Windows
                                                      C:\Windows\System32\wow64.dll
    Opens:
                                                     C:\Windows\System32\wow64win.dll
    Opens:
                                                     C:\Windows\System32\wow64cpu.dll
    Opens:
    Opens:
                                                      C:\Windows\system32\wow64log.dll
                                                      C:\Windows\SysWOW64
    Opens:
                                                     C:\Windows\SysWOW64\sechost.dll
    Opens:
    Opens:
C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe.Local\
                                                     C:\Windows\winsxs\x86_microsoft.windows.common
```

```
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                                                        C:\Windows\winsxs\x86 microsoft.windows.common-
   Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
                                                        C:\windows\temp\MSIMG32.dll
    Opens:
                                                        C:\Windows\SysWOW64\msimg32.dll
    Opens:
                                                        C:\windows\temp\VERSION.dll
    Opens:
                                                        C:\Windows\SysWOW64\version.dll
    Opens:
    Opens:
                                                        C:\Windows\SysWOW64\imm32.dll
                                                        C:\Windows\WindowsShell.Manifest
    Opens:
                                                        C:\program files\qqd1eae\log.dat
    Opens:
                                                        C:\Windows\SysWOW64\ntdll.dll
    Opens:
                                                        C:\windows\temp\msdialg100_D.dll
C:\Windows\SysWOW64\msdialg100_D.dll
    Opens:
    Opens:
                                                        C:\Windows\system\msdialg100_D.dll
    Opens:
                                                        C:\Windows\msdialg100_D.dll
    Opens:
    Opens:
                                                        C: \verb|\windows\SysWOW64\Wbem\msdialg100_D.dl1| \\
                                                        C:\Windows\SysWOW64\WindowsPowerShell\v1.0\msdialg100_D.dll
    Opens:
                                                        C:\windows\temp\MFC90ENut.dll
    Opens:
                                                        C:\Windows\SysWOW64\MFC90ENut.dll
    Opens:
    Opens:
                                                        C:\Windows\system\MFC90ENut.dll
                                                        C:\Windows\MFC90ENut.dll
    Opens:
                                                        C:\Windows\SysWOW64\Wbem\MFC90ENut.dll
    Opens:
    Opens:
                                                        C:\Windows\SysWOW64\WindowsPowerShell\v1.0\MFC90ENut.dll
                                                        C:\windows\temp\Afx100net.dll
    Opens:
                                                        C:\Windows\SysWOW64\Afx100net.dll
    Opens
    Opens:
                                                        C:\Windows\system\Afx100net.dll
    Opens:
                                                        C:\Windows\Afx100net.dll
                                                        C:\Windows\SysWOW64\Wbem\Afx100net.dll
    Opens:
    Opens:
                                                        C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Afx100net.dll
    Opens:
                                                         C:\program files\qqd1eae\Log.dat
                                                        C:\Program Files\QQd1eae\slowt64.dll
C:\Windows\SysWOW64\rpcss.dll
    Opens:
    Opens:
                                                        C:\Windows\SysWOW64\uxtheme.dll
    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
    Opens:
    Opens:
                                                        C:\Windows\Fonts\tahoma.ttf
    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
    Opens:
                                                        C:\Windows\Fonts\mingliu.ttc
    Opens:
                                                        C:\Windows\Fonts\simsun.ttc
    Opens:
                                                        {\tt C:\Windows\Fonts\gulim.ttc}\\
                                                        C:\Windows\SysWOW64\en-US\user32.dll.mui
    Opens:
    Opens:
                                                        C:\Windows\Globalization\Sorting\SortDefault.nls
                                                        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
                                                        C:\Windows\SysWOW64\ole32.dll
    Opens
    Opens:
                                                        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
    Opens:
                                                        {\tt C:\windows\temp\apphelp.dll}
                                                        C:\Windows\SysWOW64\apphelp.dll
    Opens:
                                                        C:\Windows\SysWOW64\en-US\ieframe.dll.mui
    Opens:
    Opens:
                                                        C:\WINDOWS\Temp\MJPGC.TMP
    Opens:
                                                        C:\Windows\SysWOW64\wininet.dll
                                                        C:\windows\temp\profapi.dll
    Opens:
    Opens:
                                                        C:\Windows\SysWOW64\profapi.dll
                                                        C:\Users\Admin
    Opens:
    Opens:
                                                        C:\Users\Admin\AppData\Local
                                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
    Opens:
    Opens:
                                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\desktop.ini
                                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Opens:
Files\Content.IE5
                                                        {\tt C:\Wers\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:
                                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\History
    Opens:
    Opens:
                                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
    Opens:
                                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
    Opens
\textbf{C:} \\ \textbf{VBers} \\ \textbf{Admin} \\ \textbf{AppData} \\ \textbf{Local} \\ \textbf{Microsoft} \\ \textbf{Windows} \\ \textbf{History}. \\ \textbf{IE5} \\ \textbf{desktop.ini} \\ \textbf{Microsoft} \\ \textbf{Windows} \\ \textbf{Microsoft} \\ \textbf{Mi
    Opens:
                                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\index.dat
    Opens:
                                                        C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
    Opens:
\verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\Index.data | Fig.\Color=1.00 | 
    Opens:
                                                        C:\windows\temp\dnsapi.DLL
    Opens:
                                                         C:\Windows\SysWOW64\dnsapi.dll
                                                        C:\windows\temp\iphlpapi.DLL
C:\Windows\SysWOW64\IPHLPAPI.DLL
    Opens:
    Opens:
    Opens:
                                                        C:\windows\temp\WINNSI.DLL
                                                        C:\Windows\SysWOW64\winnsi.dll
    Opens:
    Opens:
                                                        C:\windows\temp\RASAPI32.dll
                                                        C:\Windows\SysWOW64\rasapi32.dll
    Opens:
    Opens:
                                                        C:\windows\temp\rasman.dll
                                                        C:\Windows\SysWOW64\rasman.dll
    Opens:
    Opens:
                                                        C:\windows\temp\rtutils.dll
                                                        C:\Windows\SysWOW64\rtutils.dll
    Opens:
    Opens:
                                                        C:\ProgramData\Microsoft\Network\Connections\Pbk\
                                                        C:\Windows\SysWOW64\ras
    Opens:
```

```
C:\windows\temp\sensapi.dll
  Opens:
  Opens:
                          C:\Windows\SysWOW64\SensApi.dll
                          C:\Windows\SysWOW64\nlaapi.dll
                          C:\windows\temp\rasadhlp.dll
C:\Windows\SysWOW64\rasadhlp.dll
  Opens:
  Opens:
                          C:\Windows\SysWOW64\mswsock.dll
  Opens:
  Opens:
                          C:\Windows\SysWOW64\WSHTCPIP.DLL
                          C:\windows\temp\MLANG.dll
  Opens:
                          C:\Windows\SysWOW64\mlang.dll
  Opens:
                          C:\Windows\SysWOW64\wship6.dll
  Opens:
  Opens
                          C:\windows\temp\dhcpcsvc6.DLL
C:\Windows\SysWOW64\dhcpcsvc6.dll
  Opens:
  Opens:
                          C:\windows\temp\dhcpcsvc.DLL
  Opens:
  Opens:
                          C:\Windows\SysWOW64\dhcpcsvc.dll
                          C:\Windows\System32\drivers\etc\hosts
  Opens:
                          C:\Windows\SysWOW64\FWPUCLNT.DLL
  Opens:
  Opens:
Opens
Opens:
                          C:\Windows\System32\C_20127.NLS
                          C:\Windows\SysWOW64\mshtml.dll
  Opens:
                          C:\Windows\SysWOW64\msls31.dll
  Opens:
  Opens
                          {\tt C:\backslash Users\backslash Admin\backslash AppData\backslash Local\backslash Microsoft\backslash Windows\backslash Temporary\ Internet}
Files \verb|\Content.IE5\TZILKL9J\index[1].php|
                          C:\Windows\SysWOW64\msimtf.dll
  Opens:
                          C:\Windows\SysWOW64\jscript.dll
  Opens
  Opens:
                          C:\windows\temp\CRYPTSP.dll
  Opens:
                          C:\Windows\SysWOW64\cryptsp.dll
                          C:\Windows\SysWOW64\rsaenh.dll
  Opens:
                          C:\windows\temp\RpcRtRemote.dll
  Opens:
                          C:\Windows\SysWOW64\RpcRtRemote.dll
C:\Windows\SysWOW64\iepeers.dll
C:\Windows\SysWOW64\winspool.drv
  Opens:
  Opens:
  Opens:
                          C:\Windows\SysWOW64\dxtrans.dll
  Opens:
                          C:\Windows\SysWOW64\atl.dll
C:\Windows\SysWOW64\ddrawex.dll
  Opens:
  Opens:
                          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:
  Opens:
                          C:\Windows\SysWOW64\dxtmsft.dll
  Opens:
                          C:\windows\temp\SXS.DLL
C:\Windows\SysWOW64\sxs.dll
  Opens:
  Opens:
                          C:\Windows\SysWOW64\kernel32.dll
                          C:\windows\temp\ImgUtil.dll
  Opens:
  Opens:
                          C:\Windows\SysWOW64\imgutil.dll
                          C:\Windows\Fonts\arial.ttf
  Opens:
                           C:\Windows\SysWOW64\pngfilt.dll
  Opens:
                          C:\Windows\SysWOW64\en-US\mlang.dll.mui
C:\Windows\System32\C_1250.NLS
C:\Windows\System32\C_1251.NLS
  Opens:
  Opens:
  Opens:
                          C:\Windows\System32\C_1253.NLS
  Opens:
                          C:\Windows\System32\C_1254.NLS
C:\Windows\System32\C_1255.NLS
  Opens:
  Opens:
                          C:\Windows\System32\C_1256.NLS
  Opens
                          C:\Windows\System32\C_1257.NLS
  Opens:
  Opens:
                          C: \verb|\windows\System32\C_1258.NLS| \\
                          C:\Windows\System32\C_874.NLS
  Opens:
                          C:\Windows\System32\C_932.NLS
  Opens:
  Opens:
                          C:\Windows\System32\C_936.NLS
  Opens:
                          C:\Windows\System32\C_949.NLS
C:\Windows\System32\C_950.NLS
  Opens:
  Opens:
                          C:\Windows\System32\C_1361.NLS
                          C:\Windows\Fonts\arialbd.ttf
  Opens:
  Opens:
                          C:\Windows\Fonts\ariali.ttf
                          C:\Windows\SysWOW64\en-US\mshtml.dll.mui
  Opens:
  Opens
Opens:
C:\windows\temp\D3DIM700.DLL
  Opens:
  Opens:
                          C:\Windows\SysWOW64\d3dim700.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\VB8EH8F1\jquery-1.10.2.min_f2fb5194[1].js
                          C:\Windows\SysWOW64\tzres.dll
  Opens:
                          C:\Windows\SysWOW64\en-US\tzres.dll.mui
                          C:\Windows\SysWOW64\en-US\jscript.dll.mui
  Opens:
                          C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
  .
Opens
                           {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
  Opens:
Files\Content.IE5\TZILKL9J\all_async_search_d0d1b2ec[1].js
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\every_cookie_aa168cb4[1].js
                          C:\Windows\SysWOW64\Macromed\Flash\Flash10h.ocx
C:\Windows\SysWOW64\Macromed\Flash\WINMM.dll
  Opens:
  Opens:
  Opens:
                          C:\Windows\SysWOW64\winmm.dll
  Opens:
                          C:\Windows\SysWOW64\Macromed\Flash\DSOUND.dll
  Opens:
                          {\tt C:\Windows\SysWOW64\dsound.dll}
                          C:\Windows\SysWOW64\Macromed\Flash\POWRPROF.dll
  Opens:
  Opens:
                          C:\Windows\SysWOW64\powrprof.dll
                          C:\Windows\SysWOW64\Macromed\Flash\mscms.dll
  Opens:
  Opens:
                          {\tt C:\Windows\SysWOW64\mscms.dll}
                          C:\Windows\SysWOW64\Macromed\Flash\USERENV.dll
  Opens:
  Opens:
                          C:\Windows\SysWOW64\userenv.dll
  Opens:
                          C:\
                          C:\Windows\SysWOW64\Macromed\Flash\ss.sgn
  Opens:
                          C:\Windows\SysWOW64\Macromed\Flash
  Opens:
  Opens:
                          C:\Windows\SysWOW64\Macromed\Flash\ss.cfg
                          C:\Windows\SysWOW64\Macromed\Flash\mms.cfg
  Opens
```

C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk

Opens

```
Opens
                                   C:\Windows\SvsWOW64\Macromed\Flash\oem.cfg
                                   C:\Windows\SysWOW64\oem.cfg
  Opens:
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache
                                    C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\
  Opens:
  Opens:
                                    {\tt C:\Users\Admin\AppData\Roaming\Adobe\Flash\ Player}
                                   C:\Users\Admin\AppData\Roaming\Adobe
  Opens:
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache\FYPNSNG6
  Opens:
                                    C:\Windows\SysWOW64\stdole2.tlb
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\DOMStore
  Opens:
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\index.dat
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\VU73CBGV\www.baidu[11.xml
                                   C:\windows\temp\XmlLite.dll
  Opens:
                                    C:\Windows\SysWOW64\xmllite.dll
  Opens:
  Opens:
                                   C:\Windows\SysWOW64\mshtml.tlb
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt
                                   C:\Windows\SvsWOW64\urlmon.dll
  Opens:
                                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens
Files\Content.IE5\WM60WM90\nu_instant_search_ebeb5baa[1].js
                                   {\tt C:\Wers\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
  Opens:
Files\Content.IE5\VB8EH8F1\env_beb83b45[1].swf
  Opens
                                   C:\Windows\SysWOW64\msxm13.dll
                                   {\tt C:\Windows\SysWOW64\msxml3r.dll}
  Opens:
                                   C:\Windows\SvsWOW64\en-US\msxml3r.dll.mui
  Opens:
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData\
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData
  Onens:
                                   C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Internet|
Explorer\UserData\index.dat
                                   C:\windows\temp\MMDevAPI.DLL
  Opens:
                                   C:\Windows\SysWOW64\MMDevAPI.dll
  Opens:
  Opens:
                                   {\tt C:\windows\temp\PROPSYS.dll}
                                   C:\Windows\SysWOW64\propsys.dll
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Opens
Explorer\UserData\LQCEJFPO
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Opens:
Explorer\UserData\94Y0F91B
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Q98WTANC
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\TPFUMBDQ
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\*.*94Y0F91B\desktop.ini
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\LQCEJFPO\desktop.ini
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Q98WTANC\desktop.ini
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Internet
  Opens:
Explorer\UserData\TPFUMBDQ\desktop.ini
                                   C:\windows\temp\Secur32.dll
  Opens:
                                    \begin{tabular}{ll} $C:\Windows\SysWOW64\secur32.dll} $C:\Wisers\Admin\AppData\Local\Microsoft\Windows\Temporary Internet \end{tabular} 
  Opens:
  Opens
Files\Content.IE5\266VNL5S\bdsug_async_1cb857eb[1].js
  Opens:
                                   C:\windows\temp\credssp.dll
                                   C:\Windows\SysWOW64\credssp.dll
  Opens:
                                    C:\Windows\SysWOW64\schannel.dll
  Opens
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
  Opens
  Opens:
                                   C: \verb|Vsers\Admin\AppData\Roaming\Macromedia\Flash\ Player\\|
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\
  Opens:
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia
  Opens:
                                    C:\Users\Admin\AppData
                                   {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
  Opens:
Player\#SharedObjects\WV4FGR7F
                                   {\tt C:\Wsers\Admin\AppData\Roaming\Macromedia\Flash}
  Opens:
Player\#SharedObjects\WV4FGR7F\macromedia.com\support\flashplayer\sys\settings.sol
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\WV4FGR7F\macromedia.com\support\flashplayer\sys\
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
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:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\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
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\macromedia.com\
  Opens:
                                    \verb|C:\Users\Admin\AppData\Roaming\Macromedia\Flash\ Player\macromedia.com| \\
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Opens
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
{\tt Player\+Shared0bjects\+WV4FGR7F\+s1.bdstatic.com\+shared0bjectBIDUPSID.sol}
                                   {\tt C:\Users\Admin\AppData\Roaming\Macromedia\Flash}
  Opens:
Player\#SharedObjects\WV4FGR7F\s1.bdstatic.com\
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
{\tt Player\s1.bdstatic.com\shared0bjectBIDUPSID.sol}
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\s1.bdstatic.com\
  Opens:
                                    C:\Users\Admin\AppData\Roaming\Macromedia\Flash
  Opens:
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\FlashedObjects\WV4FGR7F\macromedia.com\support\flashplayer\sy\$s1.bdstatic.com\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\FlashedObjects\WV4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.com\support\W4FGR7F\macromedia.co
                                   C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sol
```

```
Opens
                                           C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
   Opens:
                                           C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
   Opens:
                                           C: \verb|\Users\Admin\AppData\Roaming\Macromedia\Flash|
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
   Opens:
                                            C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\WV4FGR7F\s1.bdstatic.com
                                           {\tt C:\Wsers\Admin\AppData\Roaming\Macromedia\Flash}
   Opens:
Player\#SharedObjects\WV4FGR7F\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                                            C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Opens:
{\tt Explorer \backslash UserData \backslash LQCEJFPO \backslash userDataBIDUPSID[1].xml}
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
   Opens:
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
   Opens
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db
   Opens:
                                           C:\Users\desktop.ini
                                           C:\Users
   Opens:
   Opens:
                                            C:\Users\Admin\AppData\Local\Microsoft
                                            C:\Users\Admin\AppData\Local\Microsoft\Windows
   Opens:
   Opens:
                                           C:\Program Files (x86)\Internet Explorer\ieproxy.dll
   Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409\
   Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History\TE5\MSHist012016040820160409
   Opens:
\label{thm:c:users} $$C: \dot Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409\index.dat $$C: \dot Users\Admin\AppData\Local\Microsoft\Windows\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\History\His
   Opens:
                                           C:\Windows\SysWOW64\en-US\shell32.dll.mui
                                           C:\Users\Admin\Favorites
   Opens:
   Opens:
                                           {\tt C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico}\\
   Opens:
                                            {\tt C:\Users\Admin\AppData\Local\Microsoft\Internet\ Explorer}
                                           {\tt C:\Users\Admin\AppData\Local\Microsoft\Internet\ Explorer\MSIMGSIZ.DAT}
   Opens:
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Opens:
Files\Content.IE5\WM60WM90\baiduia_b45d552b[1].js
                                           {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\VB8EH8F1\favicon[1].ico
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Opens:
Files\Content.IE5\VB8EH8F1\favicon[2].ico
                                           {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
   Opens:
Files\Content.IE5\TZILKL9J\JSocket_9a52fc3e[1].swf
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Opens:
Files\Content.IE5\266VNL5S\union[1].gif
   Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
   Writes to:
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
Files\Content.IE5\266VNL5S\bd_logo1[1].png
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Writes to:
Files\Content.IE5\266VNL5S\baidu_jgylogo3[1].gif
                                           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\zbios_62c636fe[1].png
                                            C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\nuomi_510f7472[1].png
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Writes to:
Files\Content.IE5\VB8EH8F1\icons_0e814c16[1].png
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\all_async_search_00d1b2ec[1].js
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\every_cookie_aa168cb4[1].js
                                           C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\VU73CBGV\www.baidu[1].xml
   Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt
   Writes to:
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\quickdelete_9c14b01a[1].png
   Writes to:
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\nu_instant_search_ebeb5baa[1].js
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\env_beb83b45[1].swf
                                           C:\Users\Admin\AppData\Roaming\Microsoft\Internet
   Writes to:
Explorer\UserData\index.dat
   .
Writes to:
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\bdsug_async_1cb857eb[1].js
   Writes to:
                                           C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\svs\settings.sxx
                                            C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Writes to: C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\WV4FGR7F\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
                                            C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\LQCEJFPO\userDataBIDUPSID[1].xml
   Writes to:
C: \verb|Visers| Admin App Data \verb|Local| Microsoft| Windows \verb|History| IE5 \verb|MSHist012016040820160409| index.dat| Admin App Data \verb|Local| Microsoft| Windows \verb|History| IE5 \verb|MSHist012016040820160409| index.dat| Admin App Data \verb|Local| Microsoft| Windows \verb|History| IE5 \verb|MSHist012016040820160409| index.dat| Admin App Data \verb|Local| Microsoft| Windows Admin App Data \verb|Local| Microsoft| Windows Admin App Data \verb|Local| Microsoft| Windows Admin App Data Admin Admin App Data Admin Admin App Data Admin Admin App Data Admin 
                                            C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\Content.IE5| \verb|\WM60WM90| baiduia_b45d552b[1].js \\
                                           C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
   Writes to:
Files\Content.IE5\VB8EH8F1\favicon[2].ico
                                           {\tt C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico}\\
   Writes to:
                                           {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\TZILKL9J\JSocket 9a52fc3e[1].swf
   Reads from:
                                           C:\Windows\Fonts\StaticCache.dat
   Reads from:
C:\Windows\Temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                           C:\Windows\System32\drivers\etc\hosts
   Reads from:
                                            C:\Windows\win.ini
   Reads from:
                                            C:\Windows\SysWOW64\dxtmsft.dll
```

```
Reads from:
                                                  C:\Windows\SvsWOW64\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
   Reads from:
                                                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Reads from:

Files\Content.IE5\TZILKL9J\every_cookie_aa168cb4[1].js

Reads from:

C:\Windows\SysWOW64\Macromed\Flash\mms.cfg
    Reads from:
                                                   C:\Windows\SysWOW64\Macromed\Flash\Flash10h.ocx
    Reads from:
                                                  C:\Windows\SysWOW64\stdole2.tlb
                                                  C:\Windows\SysWOW64\iepeers.dll
    Reads from:
    Reads from:
                                                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\all_async_search_d0d1b2ec[1].js
   Reads from:
                                                  C:\Windows\SysWOW64\mshtml.tlb
                                                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
    Reads from:
Files\Content.IE5\WM60WM90\nu_instant_search_ebeb5baa[1].js
                                                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
    Reads from:
Files\Content.IE5\VB8EH8F1\env_beb83b45[1].swf
                                                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
   Reads from:
Player\#SharedObjects\WV4FGR7F\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
   Reads from:
                                                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\bdsug_async_1cb857eb[1].js
Reads from: C:\Windows\SysWOW64\ieframe.dll
    Reads from:
                                                   C:\Users\desktop.ini
    Reads from:
                                                  C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini|
\label{lem:calwindows} Reads from: $$C:\Users\admin\appData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\WM60WM90\baiduia_b45d552b[1].js
    Reads from:
                                                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\favicon[2].ico
                                                  {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\TZILKL9J\JSocket_9a52fc3e[1].swf
   Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
   Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
   Deletes:
C: \verb|Vsers| Admin| AppData| Roaming \verb|Microsoft| Windows| Cookies| admin@www.baidu[1].txt| txt| for the context of the cookies of the cooki
   Deletes:
                                                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
{\tt Player\macromedia.com\support\flashplayer\sys\settings.sxx}
   Deletes:
                                                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
```

Network Events

DNS query:	www.baidu.com
DNS query:	s1.bdstatic.com
DNS query:	<pre>fpdownload2.macromedia.com</pre>
DNS query:	sclick.baidu.com
DNS response:	www.a.shifen.com ⇒ 103.235.46.39
DNS response:	wwwbaidu.jomodns.com ⇒ 119.146.74.40
DNS response:	a1293.d.akamai.net ⇒ 58.27.86.10
DNS response:	a1293.d.akamai.net ⇒ 58.27.86.66
DNS response:	s.a.shifen.com ⇒ 123.125.115.95
Connects to:	127.0.0.1:61136
Connects to:	103.235.46.39:80
Connects to:	119.146.74.40:80
Connects to:	58.27.86.10:80
Connects to:	123.125.115.95:80
Sends data to:	8.8.8:53
Sends data to:	127.0.0.1:61136
Sends data to:	www.a.shifen.com:80 (103.235.46.39)
Sends data to:	wwwbaidu.jomodns.com:80 (119.146.74.40)
Sends data to:	a1293.d.akamai.net:80 (58.27.86.10)
Sends data to:	s.a.shifen.com:80 (123.125.115.95)
Receives data from:	8.8.8.8:53
Receives data from:	127.0.0.1:61136
Receives data from:	www.a.shifen.com:80 (103.235.46.39)
Receives data from:	wwwbaidu.jomodns.com:80 (119.146.74.40)
Receives data from:	a1293.d.akamai.net:80 (58.27.86.10)
Receives data from:	s.a.shifen.com:80 (123.125.115.95)

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

Player\#SharedObjects\WV4FGR7F\s1.bdstatic.com\sharedObjectBIDUPSID.sxx

Windows Registry Events

windows Registry Events		
Creates key:	HKLM\software\wow6432node\microsoft\internet	
explorer\main\featurecontrol\feature_scripturl_mitigation		
Creates key:	HKCU\software\explore	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings</pre>	
Creates key:	<pre>HKLM\software\wow6432node\microsoft\tracing</pre>	
Creates key:	<pre>HKLM\software\wow6432node\microsoft\tracing\rasapi32</pre>	
Creates key:	<pre>HKLM\software\wow6432node\microsoft\tracing\rasmancs</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings\connections		
Creates key:	<pre>HKCU\software\microsoft\windows nt\currentversion\network\location</pre>	
awareness		
Creates key:	<pre>HKLM\system\currentcontrolset\services\tcpip\parameters</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\runmru</pre>	
Creates key:	HKCU\software\microsoft\internet explorer\typedurls	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\typedpaths</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings\p3p\history		
Creates key:	<pre>HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows script\settings</pre>	
Creates key:	<pre>HKLM\software\wow6432node\microsoft\direct3d\mostrecentapplication</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings\5.0\cache\ex	tensible cache\userdata	
Creates key:	HKLM\system\currentcontrolset\control\securityproviders\schannel	
Creates key:	<pre>HKCU\software\microsoft\internet explorer\domstorage\total</pre>	
Creates key:	<pre>HKCU\software\microsoft\internet explorer\domstorage\baidu.com</pre>	
Creates key:	HKCU\software\macromedia\flashplayer	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	

```
settings\5.0\cache\extensible cache\mshist012016040820160409
                                                                                   HKCU\software\microsoft\internet explorer\main\windowssearch
     Creates key:
     Creates key
                                                                                   HKLM\software\wow6432node\microsoft\downloadmanager
     Deletes value:
                                                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
                                                                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
     Deletes value:
settings\zonemap[proxybypass]
     Deletes value:
                                                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
     Deletes value:
                                                                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[intrane
     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]
     Deletes value
                                                                                   HKCU\software\macromedia\flashplayer[flashplayerversion]
     Opens key:
                                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options
     Opens kev
                                                                                   HKLM\system\currentcontrolset\control\session manager
      Opens key:
                                                                                   HKLM\software\microsoft\wow64
     Opens key:
                                                                                   HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
     Opens key:
                                                                                   HKLM\system\currentcontrolset\control\safeboot\option
      Opens key:
                                                                                   HKLM\system\currentcontrolset\control\srp\gp\dll
     Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
     Opens key:
                                                                                   HKLM\software\policies\microsoft\windows\safer\codeidentifiers
      Opens key:
                                                                                    \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \end{tabular}
     Opens key:
                                                                                   HKLM\system\currentcontrolset\control\nls\customlocale
                                                                                   HKLM\system\currentcontrolset\control\nls\language
     Opens key:
                                                                                   HKLM\system\currentcontrolset\control\mui\uilanguages
     Opens key:
                                                                                   HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
      Opens key:
     Opens key:
                                                                                   \label{lem:hklm} \verb+Kklm \+ system \+ control \+ mui \+ uilanguages \+ pending deleter \+ on the lem \+ on the le
                                                                                   HKLM\software\wow6432node\policies\microsoft\mui\settings
     Opens key:
     Opens key:
                                                                                   HKLM\software\policies\microsoft\mui\settings
     Opens key:
                                                                                   HKCU\
                                                                                   \label{thm:local_equation} \parellet AKCU \control panel \cdot \
     Opens key:
     Opens key:
                                                                                   HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
                                                                                   HKCU\software\policies\microsoft\control panel\desktop
      Opens key:
     Opens key:
                                                                                   HKCU\control panel\desktop\languageconfiguration
     Opens key:
                                                                                   HKCU\control panel\desktop
                                                                                   HKCU\control panel\desktop\muicached
      Opens key:
      Opens key:
                                                                                   HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
     Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
     Opens key:
                                                                                   HKLM\system\currentcontrolset\control\nls\sorting\versions
                                                                                   HKLM\
      Opens key:
     Opens key:
                                                                                   HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
     Opens key:
                                                                                   HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
                                                                                   HKLM\software\wow6432node\microsoft\windows
Opens key: HKLM\sof nt\currentversion\compatibility32
     Opens key
                                                                                   HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
                                                                                   HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
     Opens key:
     Opens key:
                                                                                   HKLM\software\wow6432node\microsoft\ole
                                                                                   HKLM\software\wow6432node\microsoft\ole\tracing
      Opens key:
                                                                                   HKLM\software\microsoft\ole\tracing
     Opens key:
     Opens key:
                                                                                   HKLM\software\wow6432node\microsoft\oleaut
     Opens key:
                                                                                   HKLM\system\currentcontrolset\services\crypt32
     Opens key:
                                                                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
     Opens key:
HKLM \label{limits} \label{limits} HKLM \label{limits} Wow 6432 node \label{limits} ode \label{limits} \label{limits} Wow \label{limits} Wow \label{limits} Wow \label{limits} Wow \label{limits} \label{limits} Wow \
                                                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
     Opens key:
settings
     Opens key:
                                                                                   HKCU\software\microsoft\internet explorer\main
      Opens key:
                                                                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol
                                                                                   HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
     Opens key:
      Opens key:
                                                                                   {\tt HKLM \ } system \verb|\ current control \ \\ settended locale
                                                                                   HKLM\system\currentcontrolset\control\nls\locale
      Opens key:
     Opens key:
                                                                                   HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
                                                                                   \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:
      Opens key:
                                                                                   HKLM\software\microsoft\windows
     Opens key:
nt\current version\label{languagepack\datastore\_v1.0}
                                                                                   HKLM\software\microsoft\windows
     Opens kev:
nt\currentversion\languagepack\surrogatefallback
                                                                                   HKLM\software\microsoft\windows
     Opens key:
Opens key:
                                                                                   HKLM\software\wow6432node\microsoft\windows
nt\currentversion\fontsubstitutes
                                                                                   HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
     Opens key:
     Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus ctf \setminus compatibility \setminus 62 ddfbf757 be 511f30 be 64330963 c 1345e8 be f0774b2 baa23 c 901e164b0 c 7afbb. executable for the following properties of the 
     Opens key:
                                                                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
     Opens key:
                                                                                   HKCU\software\explore
                                                                                   HKCU\software\classes\
      Opens key:
     Opens key:
                                                                                   HKLM\software\microsoft\com3
                                                                                   HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
     Opens key:
00c04fd705a2}
                                                                                   HKCR \setminus wow 6432 \\ node \\ clsid \\ \{8856f961-340a-11d0-a96b-00c04fd705a2\} \\ node \\ nod
      Opens key:
      Opens kev:
                                                                                   HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\treatas
                                                                                   HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{8856f961 - 340a - 11d0 - a96b - 00c04fd705a2\} \setminus treatas
     Opens key:
     Opens key:
                                                                                   HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
```

```
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}\inprocser
                                                    er32
    Opens key:
                                                    HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
    Opens key:
                                                     HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
   Opens key:
                                                    HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
    Opens key:
                                                    HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler
                                                    HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
   Opens key:
00c04fd705a2}\inprochandler
    Opens key:
                                                     HKLM\software\wow6432node\microsoft\rpc
    Opens key:
                                                     HKLM \verb|\system| current control set \verb|\computername| active computername| active computerna
    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\sqmclient\windows
    Opens kev:
                                                     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:
    Opens key:
                                                     HKCR\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
    Opens key:
                                                     \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ app\ management
    Opens key:
                                                     HKLM\software\wow6432node\policies\microsoft\windows\app management
                                                     HKLM\software\policies\microsoft\windows\app management
    Opens key:
    Opens key:
                                                     HKCU\software\classes\wow6432node\clsid\{004b0726-a010-4abf-8556-
fcdb7f1fca1e}
                                                     HKCR\wow6432node\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
    Opens key:
                                                     HKCU\software\classes\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
    Opens key:
                                                     HKCR\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
    Opens key:
Opens~key: \\ HKLM\software\wow6432node\microsoft\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}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                                    HKLM\software\wow6432node\microsoft\ctf\
    Opens key:
    Opens key:
                                                     Opens key:
                                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings
    Opens key:
                                                    HKCU\software\microsoft\windows\currentversion\internet settings
    Opens key:
                                                     HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_http_username_password_disable|
    Opens key:
                                                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature http username password disable
    Opens key:
                                                    HKLM\software\wow6432node\policies\microsoft\internet
explorer\main\featurecontrol
    Opens key:
                                                     HKLM \verb|\software\policies\microsoft\internet explorer \verb|\main\featurecontrol| \\
                                                    HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
    Opens kev:
                                                     HKCU\software\microsoft\internet explorer\main\featurecontrol
    Opens kev
    Opens key:
                                                    {\tt HKCU \backslash software \backslash microsoft \backslash internet}
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_allow\_reverse\_solidus\_in\_userinfo\_kb932562
    Opens key:
                                                    {\tt HKCU \backslash software \backslash microsoft \backslash internet}
explorer\main\featurecontrol\feature use ietldlist for domain determination
                                                     HKLM\software\wow6432node\microsoft\internet
    Opens key:
\verb| explorer | \verb| main | feature control | feature use iethdlist for domain determination| \\
    Opens key:
                                                     HKLM\system\currentcontrolset\control\lsa\accessproviders
    Opens key:
                                                     HKLM\system\currentcontrolset\services\ldap
    Opens key:
                                                     HKCU\software\microsoft\internet explorer\ietld
    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
                                                     HKLM\software\policies\microsoft\internet explorer\main
    Opens key:
    Opens key:
                                                     HKCU\software\policies\microsoft\internet explorer\main
    Opens key
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
                                                    HKLM\software\microsoft\windows\currentversion\policies\explorer
    Opens key:
    Opens key:
                                                     HKCU\software\microsoft\windows\currentversion\policies\explorer
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibilitv\applications\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                                    HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Opens key:
08002b30309d}\shellfolde
    Opens key:
                                                    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 kev:
HKLM\software\wow6432node\microsoft\windows\currentyersion\policies\nonenum
                                                    \label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} irror of twindows \current version \end{tabular} policies \end{tabular} none number \end{tabular}
    Opens key:
    Opens key:
                                                    HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32
                                                    HKCR\
                                                                      w6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32
Opens key: extensions\blocked
                                                    HKLM\software\wow6432node\microsoft\windows\currentversion\shell
    Opens key:
                                                     HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
    Opens key:
                                                     {\tt HKLM \ } system \verb|\ current control \ \\ session \ manager \verb|\ app compatibility| \\
    Opens key:
                                                     HKLM\software\wow6432node\policies\microsoft\windows\appcompat
    Opens key:
                                                     HKLM\software\policies\microsoft\windows\appcompat
                                                     \label{thm:linear} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \shell extensions \cached } \end{tabular}
    Opens key:
    Opens key:
                                                     HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d
    Opens key:
                                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
                                                     HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{871c5380-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1069-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-1060-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a2ea-42a0-a
    Opens key:
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}\nrogid
                                                                        HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
     Opens key:
     Opens key:
                                                                        HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
     Opens key
                                                                        HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea
08002b30309d}\progid
                                                                        HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid
     Opens key:
     Opens key:
                                                                        HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler32
                                                                       HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Opens key:
08002b30309d}\inprochandler32
     Opens key:
                                                                       HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler
                                                                       HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Opens key:
08002b30309d}
                                      \inprochandler
     Opens key:
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
     Opens key:
                                                                       HKLM\software\wow6432node\policies\microsoft\internet
explorer\browseremulation
     Opens key:
                                                                        HKLM\software\policies\microsoft\internet explorer\browseremulation
     Opens key:
                                                                        HKCU\software\policies\microsoft\internet explorer\browseremulation
     Opens key:
                                                                        HKLM\software\wow6432node\microsoft\internet explorer\mediatypeclass
     Opens key:
                                                                       HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\accepted documents
     Opens key:
HKLM\softwar
                                     e\wow6432node\microsoft\windows\currentversion\policies\ratings
     Opens key:
                                                                       HKLM\software\microsoft\windows\currentversion\policies\ratings
                                                                       HKCU\software\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
                                                                       HKLM\software\wow6432node\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
Opens key: HKLM\software\wow6432node\policies
     Opens key:
                                                                        HKCU\software\policies
     Opens key:
                                                                        HKCU\software
                                                                       HKLM\software\wow6432node
     Opens key:
     Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ \ wow \ for the property of the pr
    Opens key:
                                                                       HKCU\software\microsoft\internet
explorer\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\
                                                                       HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens key:
settings\zonemap\domains
                                                                       HKCU\software\policies\microsoft\windows\currentversion\internet
    Opens kev:
settings\zon
    Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
     Opens key:
                                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges
                                                                       HKCU\software\policies\microsoft\windows\currentversion\internet
    Opens key:
settings\zonemap\ranges\
                                                                        HKCU\software\microsoft\internet
     Opens key:
\verb|explorer\main\featurecontrol\feature\_unc\_savedfilecheck| \\
    Opens key:
                                                                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
     Opens key:
                                                                        HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
    Opens key:
                                                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                                                                       HKLM\software\wow6432node\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
     Opens key:
HKLM \backslash software \backslash wow 6432 node \backslash policies \backslash microsoft \backslash windows \backslash current version \backslash internet settings \backslash zone map for the following of the f
    Opens key:
                                                                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
Opens key:
                                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
    Opens key:
                                                                       HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
     Opens kev
                                                                        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
     Opens key:
                                                                        HKLM\software\policies\microsoft\internet explorer
     Opens key:
                                                                        HKLM\software\policies\microsoft\internet explorer\security
     Opens key:
                                                                        \label{thm:linear} \mbox{HKCU\software\mbox{\sc windows\currentversion\internet\ settings\zones\sc windows\correntversion\sc windows\correntversion\sc windows\correntversion\sc windows\sc windows\
                                                                        HKCU\software\microsoft\windows\currentyersion\internet settings\zones\0
     Opens key:
     Opens key:
                                                                        HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
     Opens key:
                                                                        \label{local-observation} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet\ settings\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\colors\co
     Opens key:
                                                                        HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
     Opens key:
     Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
    Opens key:
                                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
                                                                        \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\zones\
    Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
    Opens key:
                                                                        \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\0
```

```
Opens kev:
                                                                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
      Opens key:
                                                         \verb|e|wow6432| node \verb|policies|microsoft|windows| current version| internet settings| zones| 1|
HKLM\softwa
      Opens key:
                                                                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
       Opens key:
                                                                                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                                                                                                             HKLM\software\wow6432node\microsoft\windows\currentversion\internet
      Opens key:
settings\zonemap\
       Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
                                                                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
      Opens kev:
settings\zones\2
      Opens key:
                                                                                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
      Opens kev:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ zones \ \ 3200 \ description \ des
                                                                                                              HKLM\software\policies\microsoft\windows\currentversion\internet
      Opens key:
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
                                                                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
      Opens key:
settings\zones\4
      Opens key:
                                                                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
      Opens key:
                                                                                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
      Opens key:
                                                                                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
      Opens key:
settings\lockdown_zones\
                                                                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
      Opens key:
settings\lockdown_zones
      Opens key:
                                                                                                             \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\
      Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
      Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
      Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
\verb|settings\lockdown_zones\0|
                                                                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
      Opens key:
settings\lockdown_zones\0
                                                                                                             HKCU\software\policies\microsoft\windows\currentversion\internet
      Opens key:
settings\lockdown_zones\0
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
      Opens kev:
settings\lockdown_zones\1
      Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                                                                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                                                                                                             \label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}
      Opens key:
settings\landslockdown_zones\1
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
       Opens key:
settings\lockdown_zones\2
      Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                                                                                             \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM\software\policies\microsoft\windows\currentversion\notation{\coloratesized by the content of the 
      Opens key:
settings\lockdown zones\2
      Opens key:
                                                                                                             \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdo
                                                                          _zones\2
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
      Opens key:
settings\lockdown_zones\3
       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\3
                                                                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
      Opens key:
settings\lockdown zones\3
      Opens key:
                                                                                                             \label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \label{thm:local_hammon} Software \begin{tabular}{l} PKCU \label{thm:local
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} on the local constraints of the local constraints 
settings\lockdown zones\4
      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\lockdown_zones\4
      Opens key:
                                                                                                             HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache
      Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
      Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
      Opens key:
                                                                                                             settings\5.0\cache\content
      Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
       Opens key:
HKLM \label{lem:hklm} Software \label{lem:hklm} Which is a few and the software \lab
33be-4251-ba85-6007caedcf9d}
      Opens key:
HKLM \label{lem:hklm} White the latest and the la
33be-4251-ba85-6007caedcf9d}\propertybag
```

```
Opens key:
                                                                                                            HKCU\software\microsoft\windows\currentversion\explorer
                                                                                                           HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
        Opens key:
        Opens key:
 \label{thm:linear} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \session in folders} \end{tabular}
        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
                                                                                                           HKCU\software\policies\microsoft\windows\explorer
        Opens key:
        Opens key:
 6fba-4fcf-9d55-7b8e7f157091}
       Opens kev:
 HKLM \label{lem:hklm} \verb| knd \label{lem:hklm} White \label{lem:hkklm} W
 6fba-4fcf-9d55-7b8e7f157091}\propertybag
       Opens key:
 0e22-4760-9afe-ea3317b67173}
       Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus f
0e22-4760-9afe-ea3317b67173}\propertybag
                                                                                                           HKLM\software\wow6432node\microsoft\windows
        Opens key:
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 key:
Opens key:
                                                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
       Opens key:
                                                                                                           HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| windows \verb|\currentversion\\| internet model in the context of 
 settings\5.0\cache\cookies
       Opens key:
 HKL\ M\ Noftware \ New M432 node \ Microsoft\ New McL\ M\ Noftware \ New M6432 node \ Microsoft\ New M6432 node \ New M6432
 c0e9-4171-908e-08a611b84ff6}
       Opens key:
c0e9-4171-908e-08a611b84ff6}\propertybag
       Opens key:
65f9-4cf6-a03a-e3ef65729f3d}
        Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus \{3eb68
OF59-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet
Settings\5.0\cache\history

Onens kev: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings\5.0\cache\history
       Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d9dc8a3b-d
b784-432e-a781-5a1130a75963}
       Opens kev:
 HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}\propertybag
                                                                                                           HKCU\software\microsoft\windows\currentversion\internet
       Opens key:
 settings\5.0\cache\extensible cache
                                                                                                           HKCU\software\microsoft\windows\currentversion\internet
 {\tt settings \ 1.0 \ cache \ extensible \ cache \ domstore}
                                                                                                           HKCU\software\microsoft\windows\currentversion\internet
       Opens key:
settings\5.0\cache\extensible cache\feedplat
                                                                                                           HKCU\software\microsoft\windows\currentversion\internet
        Opens key:
 settings\5.0\cache\extensible cache\iecompat
                                                                                                           HKCU\software\microsoft\windows\currentversion\internet
       Opens key:
 settings\5.0\cache\extensible cache\ietld
                                                                                                           HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\privacie:
                                                                                                           HKCU\software\microsoft\internet
       Opens key:
 \verb|explorer\main\featurecontrol\retry_headeronly post\_on connection reset|\\
                                                                                                           HKLM\software\wow6432node\microsoft\internet
        Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_bufferbreaking_818408
        Opens key:
                                                                                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954 | left by the control of the control
       Opens key:
                                                                                                           HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954
         Opens key:
\label{thm:local-condition} \begin{tabular}{ll} HKLM \end{tabular} Software \wow 6432 node \policies \microsoft \windows \current version \times the settings \end{tabular} Software \wow 6432 node \policies \microsoft \windows \current version \times \microsoft \
       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:
 \verb|explorer| \verb|main| featurecontrol| feature_fix\_chunked\_proxy\_script\_download\_kb843289|
                                                                                                           HKCU\software\microsoft\internet
       Opens key:
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:
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
                                                                                                           HKLM\software\wow6432node\microsoft\internet
        Opens key:
 explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
                                                                                                           HKCU\software\microsoft\internet
        Opens key:
 explorer\main\featurecontrol\feature_allow_long_international_filenames
        Opens key:
                                                                                                           HKLM\software\wow6432node\microsoft\internet
```

```
explorer\main\featurecontrol\feature_allow_long_international_filenames
                                                                                 HKCU\software\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                                                                                 HKLM\software\wow6432node\microsoft\internet
     Opens key:
explorer \verb|\main| featurecontrol| feature\_permit\_cache\_for\_authenticated\_ftp\_kb910274| \\
                                                                                 HKCU\software\microsoft\internet
     Opens key:
explorer \verb|\main| featurecontrol| feature\_disable\_unicode\_handle\_closing\_callback| featurecontrol| feature\_disable\_unicode\_handle\_closing\_callback| featurecontrol| feature\_disable\_unicode\_handle\_closing\_callback| featurecontrol| feature\_disable\_unicode\_handle\_closing\_callback| featurecontrol| featur
     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
     Opens key:
                                                                                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                                                                                 HKCU\software\microsoft\internet
     Opens key:
explorer \verb|\main| featurecontrol \verb|\feature_digest_no_extras_in_urial and the control and the contr
     Opens key:
                                                                                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature digest no extras in uri
      Opens kev:
                                                                                 HKLM\software\wow6432node\microsoft\internet
\verb|explorer|| \verb|main|| featurecontrol|| feature_enable_passport_session_store_kb948608||
     Opens key:
                                                                                 \label{local_hammon_hammon} \mbox{HKCU\software\mbox{\sc 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 key:
                                                                                 HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_use\_utf8\_for\_basic\_auth\_kb967545
                                                                                 HKCU\software\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
     Opens key:
                                                                                 HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature_release_keys\_on\_unload\_kb975619
                                                                                 HKCU\software\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                                                                                 HKLM\software\wow6432node\microsoft\internet
     Opens key:
explorer\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:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries
     Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000000
      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 \label{lem:hkkm} \label{lem:hkkm} HKLM \label{lem:hkkm} Which is a substitution of the last substitution of the la
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\protocol_catalog9\catalog_entries\00000000010
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
     Opens key:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_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\0000000000004
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\0000000000005
     Opens kev
Opens key:
                                                                                  HKCU\software\microsoft\windows\currentversion\internet settings\wpad
     Opens key:
                                                                                  HKCU\software\microsoft\internet
explorer \verb|`main\featurecontrol\feature_return_failed\_connect\_content\_kb942615|
     Opens key:
                                                                                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_return_failed connect content kb942615
     Opens key:
                                                                                 HKLM\software\wow6432node\microsoft\tracing\rasapi32
      Opens key:
                                                                                  HKLM\software\wow6432node\microsoft\tracing\rasmancs
     Opens key:
                                                                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
     Opens key:
                                                                                  \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} 
                                                                                  HKLM\software\microsoft\sqmclient\windows\disabledsessions\
      Opens key:
     Opens key:
                                                                                  HKLM\system\currentcontrolset\control\sqmservicelist
     Opens key:
                                                                                 HKU\
     Opens key:
                                                                                  \label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ dns \+ cache \+ parameters
                                                                                  HKLM \label{limits} \mbox{HKLM} \mbox{$\mbox{$N$} icrosoft \mbox{$\mbox{$w$} indows $nt$} \mbox{$\mbox{$d$} icrosoft \mbox{$\mbox{$w$} indows $nt$} \mbox{$\mbox{$w$} icrosoft \mbox{$\mbox{$\mbox{$w$} icrosoft \mbox{$\mbox{$\mbox{$w$} icrosoft \mbox{$\mbox{$\mbox{$w$} icrosoft \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$w$} icrosoft \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbo
      Opens key:
     Opens key:
                                                                                  HKLM\software\policies\microsoft\windows nt\dnsclient
                                                                                  HKLM\system\currentcontrolset\services\dns
     Opens key:
      Opens key:
                                                                                  HKCU\software\microsoft\internet explorer
     Opens key:
                                                                                  HKLM\software\wow6432node\microsoft\internet explorer
```

```
Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature mime handling
                                              HKLM\software\wow6432node\microsoft\internet
   Opens key:
 explorer\main\featurecontrol\feature_mime_handling
   Opens key:
                                              HKCU\software\classes\protocols\name-space handler\
                                              HKCR\protocols\name-space handler
   Opens key:
   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:
                                              HKCR\protocols\name-space handler\*
   Opens key:
                                              HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_enable_compat_logging
                                             HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_enable_compat_logging
                                              HKCU\software\microsoft\windows\currentversion\internet settings\user
  Opens key:
agent
  Opens kev:
                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent
                                              \label{local-equation} \mbox{HKCU\software\mbox{\sc windows\currentversion\internet}} \\
  Opens key:
settings\5.0\user agent
                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\user agent
  Opens key:
                                              \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ 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:
                                             HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings\user agent\pre platform
  Opens key:
                                             HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
                                             HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\user agent\pre platform
  Opens key:
                                             HKI M\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\post platform
   Opens key:
                                              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
                                             HKCU\software\microsoft\internet
   Opens key:
\verb|explorer\main\featurecontrol\feature_browser_emulation| \\
   Opens key:
                                             HKLM\software\wow6432node\microsoft\internet
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
                                              HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver
                                             HKLM\software\wow6432node\microsoft\internet
  Opens key:
                                            trol\feature_maxconnectionsper1_Oserver
explorer\main\featurecom
                                              HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:
   Opens key:
                                              HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
                                              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:
   Opens key:
                                              {\tt HKLM \ } system \verb| current control set \verb| services \verb| winsock \verb| setup migration \verb| providers migration \verb| providers migration \verb| providers migration \verb| providers migration m
   Opens key:
                                             {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ winsock \verb|\ setup| \\
migration\providers\tcpip
                                              HKCU\software\microsoft\windows\currentversion\urlmon settings
   Opens key:
                                              {\tt HKCU \ } software \verb|\ microsoft \> \ internet
   Opens key
explorer \verb|\main| featurecontrol| feature\_include\_port\_in\_spn\_kb908209
   Opens key:
                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
   Opens key:
                                              HKCU\software\microsoft\internet explorer\international
   Opens key:
                                             HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature_disable_legacy\_compression
   Opens key:
                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression
   Opens key:
                                              HKCU\software\classes\protocols\name-space handler
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\explorer\travellog
   Opens key:
HKLM \label{log} LKLM \label{log} HKLM \label{log} Windows \label{log} LKLM \label{log} LKLM \label{log} HKLM \label{log} Windows \label{log} LKLM \label{log} LKLM \label{log} Windows \label{log} LKLM \label{log} LKLM \label{log} Windows \label{log} LKLM \label{log} LKLM \label{log} Windows \label{log} Windows \label{log} LKLM \label{log} Windows \label{log} Win
                                             HKLM\system\currentcontrolset\services\winsock\setup
  Opens kev:
migration\providers\tcpip6
   Opens key:
HKCU\software\policies\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:
                                             HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
   Opens kev
HKLM\software\policies\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete
                                             HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
   Opens key:
00c04fd7d062}
   Opens key:
                                             HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
   Opens key:
                                             HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\treatas
   Opens key:
                                             HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas
   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 \setminus software \setminus classes \setminus clsid \setminus \{00bb2765-6a77-11d0-a535-00c04fd7d062\}
                                             HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
   Opens key:
   Opens key:
                                              HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535
00c04fd7d062}\progid
                                             HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid
   Opens key:
                                             HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
   Opens key:
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
                                             HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
   Opens key:
```

```
00c04fd7d062}\inprochandler32
                                           HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
  Opens key:
00c04fd7d062}\inprochandler
                                           HKCR\
                                                       ow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  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
   Opens key
                                           HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\progid
   Opens key:
                                            HKCR \setminus wow6432 node \\ clsid \setminus \{6935db93-21e8-4ccc-beb9-9fe3c77a297a\} \setminus progid
                                            HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
   Opens key:
   Opens key:
                                           HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
   Opens key
                                            HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9
9fe3c77a297a}\progid
                                            HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\progid
   Opens key:
   Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32
   Opens key:
                                           HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32
   Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler32
   Opens key
                                            HKCR\
                                                          /6432node\clsid\{6935db93-21e8-4ccc-beb9
9fe3c77a297a}\inprochandler32
  Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler
   Opens key:
                                            HKCR\wo
                                                         w6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler
                                           HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
  Opens key:
00c04fd7d062}
                                            HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}
   Opens key:
   Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\treatas
                                            Opens key:
   Opens key
                                            00c04fd7d062}\progid
                                            HKCR \setminus wow6432 \\ node \\ clsid \\ \{00bb2764-6a77-11d0-a535-00c04fd7d062\} \\ \setminus progid
   Opens key:
                                            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:
   Opens kev
                                           HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
                                           HKCR
                                                          v6432node\clsid\{00bb2764-6a77-11d0-a535-
   Opens key:
00c04fd7d062}\inprocser
                                          er32
  Opens kev
                                           HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
                                            HKCR\
                                                         w6432node\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
00c04fd7d062}\inprochandler
  Opens key
                                           HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}
                                            HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
   Opens key:
   Onens key
                                            HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\treatas
   Opens key:
                                            00c04fd7d062}\progid
   Opens key:
                                            HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid
   Opens key:
                                            HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
                                            HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
   Opens key:
   Opens key:
                                           HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\progid
   Opens key:
                                            HKCR \ clsid \ \{00bb2763-6a77-11d0-a535-00c04fd7d062\} \ \ progides the control of the control 
   Opens kev
                                           HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
                                           HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
   Opens key:
00c04fd7d062}\inprocserver32
   Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
                                           HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
   Opens key:
00c04fd7d062}\inprochandler32
  Opens kev
                                           HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler
   Opens key:
                                            HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32
   Opens key:
                                           HKCR
                                                         w6432node\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32
  Opens key:
\label{thm:limit} \begin{tabular}{ll} HKL\begin{tabular}{ll} ML\begin{tabular}{ll} ML\
   Opens key:
                                            HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd9973
                                           HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
   Opens key:
                                            HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
   Opens key
b61bb7cdd997}\treatas
   Opens key:
                                           HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas
                                            HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
   Opens key:
b61bb7cdd997}\progid
                                            \label{localized} HKCR\wow6432 node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\ \ progid
   Opens key:
   Opens key:
                                           HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32
                                           HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
```

b61bb7cdd997}\inprocserver32

```
Onens key
                                                                                                                       HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
 b61bb7cdd997}\inprochandler32
         Opens key:
                                                                                                                        HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
  b61bb7cdd997}\inprocha
                                                                                                           ndler32
                                                                                                                       HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
         Opens key:
 b61bb7cdd997}\inprochandler
         Opens key:
                                                                                                                       HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
 b61bb7cdd997}\inprochandler
                                                                                                                       HKLM\software\wow6432node\microsoft\rpc\extensions
         Opens key:
                                                                                                                       HKLM\software\microsoft\rpc\extensions
          Opens key:
                                                                                                                        {\tt HKLM \ } . \\ {\tt Software \ } . \\ {\tt None \ } \\ {\tt Policies \ } \\ {\tt microsoft \ } \\ {\tt system \ } \\ {\tt dnsclient \ } \\ {\tt Microsoft \ } \\ {\tt System \ } \\ {\tt dnsclient \ } \\ {\tt Microsoft \ } \\ {\tt System \ } \\ {\tt dnsclient \ } \\ {\tt Microsoft \ } \\ {\tt System \ } \\ {\tt dnsclient \ } \\ {\tt Microsoft \ } \\ {\tt System \ } \\ {\tt dnsclient \ } \\ {\tt Microsoft \ } \\ {\tt System \ } \\ {\tt dnsclient \ } \\ {\tt Microsoft \ } \\ {\tt System \ } \\ {\tt dnsclient \ } \\ {\tt Microsoft \ } \\ {\tt System \ } \\ {\tt dnsclient \ } \\ {\tt Microsoft \ } \\ {\tt Mi
          Opens key:
         Opens key:
                                                                                                                        HKLM\software\policies\microsoft\system\dnsclient
                                                                                                                       HKCU\software\microsoft\windows\currentversion\explorer\advanced
         Opens key:
          Opens key:
                                                                                                                        \label{local-operator} \begin{tabular}{ll} HKLM\system\current control set\services\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\dnscache\parameters\
          Opens key:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
         Opens key:
         Opens key:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
 e1e01c1f69b5}
         Opens key:
 HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \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-
 806e6f6e69633
        Opens key:
  HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \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-9
 806e6f6e6963}
        Opens key:
 \label{local-equation} HKL\ M \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{a91d0a5e-390e-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4979-9c38-4079-9c38-4079-9c38-4079-9c38-4070-9c38-4070-9c38-4070-9c38-4070-9c38-4
        Opens key:
 \label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} System \current control set \end{tabular} etc. \begin{tabular}{ll} HKLM \end{tabular} System \current control set \end{tabular} etc. \begin{tabular}{ll} HKLM \end{tabular} System \end{tabular} etc. \begin{tabular}{ll} HKLM 
  65fee5bae0b1}
                                                                                                                        \label{lem:hklm} \verb+KKLM\+ system \verb+ current control set \verb+ services \verb+ tcpip \verb+ linkage+ \\
         Opens key:
                                                                                                                       HKCU\software\microsoft\windows\currentversion\internet
  settings\p3p\history\baidu.com
         Opens key:
                                                                                                                       HKCU\software\classes\mime\database\content type\text/html; charset=utf-
        Opens key:
                                                                                                                        \label{local-equation} \mbox{HKCR} $$ \mbox{HKCR} \rightarrow \mbox{HKCR}, \mbox{ charset=utf-8} $$
         Opens key:
                                                                                                                        HKCU\software\classes\mime\database\content type\text/html
         Opens key:
                                                                                                                        {\it HKCR} \verb|\mime| database| content type| text/html|
         Opens key:
                                                                                                                        HKCU\software\classes\protocols\filter\text/html; charset=utf-8
                                                                                                                        HKCR\protocols\filter\text/html; charset=utf-8
         Opens key:
                                                                                                                        HKCU\software\classes\protocols\filter\text/html
         Opens key:
          Opens key:
                                                                                                                        {\tt HKCR \backslash protocols \backslash filter \backslash text/html}
         Opens key:
                                                                                                                       HKCU\software\microsoft\internet
  explorer\main\featurecontrol\feature_mime_sniffing
         Opens key:
                                                                                                                       HKLM\software\wow6432node\microsoft\internet
  explorer\main\featurecontrol\feature_mime_sniffing
        Opens key:
                                                                                                                       HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_feeds
                                                                                                                        HKLM\software\wow6432node\microsoft\internet
          Opens key:
  explorer\main\featurecontrol\feature_feeds
        Opens key:
                                                                                                                       HKCU\software\microsoft\internet
  explorer\main\featurecontrol\feature_safe_bindtoobject
                                                                                                                        HKLM\software\wow6432node\microsoft\internet
         Opens key:
  \verb|explorer\main\featurecontrol\feature\_safe\_bindtoobject|
                                                                                                                       HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
        Opens key:
 00aa00686f13}
                                                                                                                        HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
          Opens key:
         Opens key:
                                                                                                                        HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
 00aa00686f13}\treatas
         Opens key:
                                                                                                                        Opens key:
00aa00686f13}\progid
                                                                                                                        Opens key:
                                                                                                                       HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
         Opens key
                                                                                                                       HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{25336920 - 03f9 - 11cf - 8fd0 - 11cf - 11cf
                                                                                                                   er32
 00aa00686f13}\inprocserv
                                                                                                                       HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
        Opens key
 00aa00686f13}\inprocserver32
         Opens key:
                                                                                                                       HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
 00aa00686f13}\inprochandler32
                                                                                                                       HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
        Opens key
  00aa00686f13}\inprochandler32
                                                                                                                       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:
  \verb|explorer| main feature control feature css_data_respects_xss_zone_setting_kb912120| \\
         Opens kev:
                                                                                                                       HKLM\software\wow6432node\microsoft\internet
  explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                                                                                                                       HKCU\software\microsoft\internet
         Opens key:
 \begin{tabular}{ll} explorer $$ main feature control feature external_style_sheet_fix_for_smartnavigation_kb926131 $$ Opens key: $$ HKLM software \odd{tabular} $$ HKLM $$ ffware \odd{tabular} $$ explorer $$ main feature control feature external_style_sheet_fix_for_smartnavigation_kb926131 $$ Opens key: $$ HKLM $$ ffware \odd{tabular} $$ explorer $$ ffware \odd{tabular} $$ explorer $$ ffware \odd{tabular} $$ explorer $$ explorer $$ ffware \odd{tabular} $$ explorer $$ explorer $$ ffware \odd{tabular} $$ explorer $$ e
  \verb|explorer| main\featurecontrol| feature\_external\_style\_sheet\_fix\_for\_smartnavigation\_kb926131| feature\_external\_style\_sheet\_fix\_for\_smartnavigation\_sheet\_fix\_for\_smartnavigation\_fix\_for\_smartnavigation\_fix\_sheet\_fix\_for\_smartnavigation\_sheet\_fix\_for\_smartnavigation\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_sheet\_fix\_she
         Opens key:
                                                                                                                       HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature aria support
                                                                                                                       HKLM\software\wow6432node\microsoft\internet
         Opens key:
  explorer\mai
                                                                                                                    trol\feature_aria_support
        Opens key:
                                                                                                                       {\tt HKCU \ } software \verb|\ microsoft \> internet|
 explorer\main\featurecontrol\feature_legacy_dispparams
Opens key: HKLM\software\wow6432node\microsoft\internet
  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\wow6432node\microsoft\internet
```

explorer\main\featurecontrol\feature_css_show_hide_events

```
Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature display node advise kb833311
  Opens key:
                                    HKLM\software\wow6432node\microsoft\internet
                                   trol\feature_display_node_advise_kb833311
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
                                    HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer \verb|\main| featurecontrol| feature\_body\_size\_in\_editable\_if rame\_kb943245
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_databinding_support
                                    HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_databinding_support
                                   HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_enforce_bstr
                                   HKLM\software\wow6432node\microsoft\internet
  Opens key:
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 \ wow 6432 node \ microsoft \ internet
explorer\main\featurecontrol\feature object caching
  Opens key:
                                   HKCU\software\microsoft\internet
                                   trol\feature_legacy_tostring_in_compatview
explorer\main\featurecom
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature legacy tostring in compatview
                                    HKCU\software\microsoft\internet
  Opens key:
explorer \verb|\main| featurecontrol \verb|\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
                                    HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:
  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:hklmsoftware} \begin{tabular}{ll} HKLM\software\mbox{$\mbox{microsoft}\windows\currentversion\app\ paths\outlook.exe} \end{tabular}
  Opens key
                                    HKLM\software\wow6432node\microsoft\internet explorer\application
compatibility
                                    HKLM\software\wow6432node\policies\microsoft\internet
  Opens kev:
explorer\domstorage
  Opens key:
                                    \label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ internet explorer \+ dom storage
  Opens key:
                                   HKCU\software\policies\microsoft\internet explorer\domstorage
HKCU\software\microsoft\internet explorer\domstorage
  Opens key:
                                    HKLM\software\wow6432node\microsoft\internet explorer\domstorage
  Opens key:
  Opens key:
                                    HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus internet
explorer\safety\privacie
                                    HKLM\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
                                    HKCU\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet explorer\safety\privacie
  Opens key:
                                    HKLM\software\wow6432node\microsoft\internet explorer\safety\privacie
  Opens key:
                                    HKCU\software\microsoft\internet
\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
\verb|explorer\main\featurecontrol\feature_restrict_filedownload| \\
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet explorer\security\floppy
access
                                    HKCU\software\microsoft\internet explorer\securitv\adv addrbar spoof
  Opens key:
detection
  Opens key:
                                    HKLM\software\wow6432node\microsoft\internet explorer\security\adv
addrbar spoof detection
                                    HKCU\software\classes\protocols\name-space handler\about\
  Opens key:
  Opens key:
                                    HKCR\protocols\name-space handler\about
                                    HKCU\software\classes\protocols\handler\about
  Opens key:
  Opens key:
                                    HKCR\protocols\handler\about
                                    HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
  Opens kev:
00aa00bdce0b}
                                    HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\treatas
  Opens key:
                                    HKCR \land wow6432 node \land \{3050f406-98b5-11cf-bb82-00aa00bdce0b\} \land treat as the substitution of the substitu
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\progid
  Opens key:
                                    HKCR\wow6432 node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                   HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\progid
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
  Opens key:
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:
                                   HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
                                   HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\inprochandler32
  Opens key:
                                   HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
```

```
Opens key:
                                                               HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
     Opens key:
                                                               HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
 00aa00bdce0b}\inprochandler
     Opens key:
                                                               HKCU\software\microsoft\internet
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
                                                                HKLM\software\wow6432node\microsoft\internet
     Opens key:
 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:
                                                                HKCU\software\policies\microsoft\internet explorer\zoom
     Opens key:
     Opens key:
                                                                \label{local_equation} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\sc om}} \\
                                                               HKLM\software\wow6432node\microsoft\internet explorer\zoom
     Opens key:
     Opens kev
                                                                HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_weboc_document_zoom
    Opens key:
                                                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature weboc document zoom
                                                                HKLM\software\policies\microsoft\windows\currentversion\internet
     Opens key:
 settings\url history
Opens key:
settings\url history
                                                                HKCU\software\policies\microsoft\windows\currentversion\internet
     Opens key:
                                                                HKCU\software\microsoft\windows\currentversion\internet settings\url
history
    Opens key:
                                                               HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\url history
     Opens key:
                                                                HKCU\software\microsoft\internet
 explorer \verb|\main| featurecontrol| feature\_ipersistmoniker\_load\_redirected\_url\_kb976425
    Opens key:
                                                               HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_ipersistmoniker_load_redirected_url_kb976425
                                                                HKCU\software\policies\microsoft\internet explorer
     Opens key:
                                                                \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} & \begin{tabular}{ll} HKLM \label{thm:
     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:
     Opens key:
                                                                HKCU\software\microsoft\internet explorer\settings
                                                                HKLM\software\wow6432node\microsoft\internet explorer\settings
     Opens key:
     Opens key:
                                                                HKCU\software\microsoft\internet explorer\styles
     Opens key:
                                                                HKCU\software\microsoft\windows\currentversion\policies\activedesktop
                                                                HKCU\software\microsoft\windows\currentversion\policies
     Opens key:
     Opens key:
                                                                HKCU\software\microsoft\internet explorer\pagesetup
     Opens key:
                                                                \label{lem:hkcu} \verb+KKCU\+ 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
     Opens key:
     Opens key:
                                                                HKCU\software\microsoft\internet
     Opens kev:
 explorer\main\featurecontrol\feature_zone_elevation
                                                               HKLM\software\wow6432node\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_xssfilter
     Opens key:
                                                               HKLM \ software \ wow 6432 node \ microsoft \ internet
 explorer\main\featurecontrol\feature xssfilter
                                                                HKCU\software\microsoft\windows\currentversion\internet settings\zones
     Opens key:
                                                                HKLM\software\policies\microsoft\internet explorer\low rights
     Opens key:
     Opens key:
                                                                \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\internet explorer\low rights}}
     Opens key:
                                                               HKLM\software\wow6432node\microsoft\internet explorer\low rights
     Opens key:
                                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 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\wow6432node\microsoft\windows\currentversion\internet
 settings\zones\2
    Opens key:
                                                               HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings\zones\3
     Opens key:
                                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings\zones\4
Opens~key: \\ HKCU\software\microsoft\internet \\ explorer\min\featurecontrol\feature\_mshtml\_autoload\_ieframe \\
                                                                HKLM\software\wow6432node\microsoft\internet
     Opens key:
 explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
                                                                HKLM\software\wow6432node\policies\microsoft\internet explorer\dxtrans
     Opens kev:
                                                                HKLM\software\policies\microsoft\internet explorer\dxtrans
     Opens key:
                                                                \label{prop:hkcu} \begin{tabular}{ll} HKCU \end{tabular} in terms the explorer \end{tabular} \dot{\end{tabular} \dot{\end{tabular} in terms the explorer \end{tabular} \dot{\end{tabular} \dot{\end{tabular} in terms the explorer \end{tabular} \dot{\end{tabular} in terms the explorer \end{tabular} \dot{\end{tabular} \dot{\end{tabular} in terms the explorer} \dot{\end{tabular} in terms the 
     Opens key:
     Opens key:
                                                                HKLM\software\wow6432node\microsoft\internet explorer\dxtrans
                                                                HKCU\software\microsoft\internet
     Opens key:
 explorer\main\featurecontrol\feature_subdownload_lockdown
     Opens key:
                                                               HKLM\software\wow6432node\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_subdownload\_lockdownload| |
     Opens key:
                                                               HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_sslux
     Opens key:
                                                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature sslux
    Opens key:
                                                                \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \time the constraints of the constraints of
 settings\
     Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\internet settings\
     Opens key:
\label{twindows} \verb|HKLM| software wow 6432 node policies wire soft windows \verb|currentversion| internet settings \verb|conemap|| in the software wow 6432 node policies wire wow 6432 node policies wire software wow 6432 node policies wire wow 6432 node policies wire software wow 6432 node policies wire wow 6432 node policies wow 6432 node policies wire wow 6432 node policies wow 6432 node policies wow 6432 node policies wow 6432 node policies wire wow 6432 node policies wow 6432
    Opens key:
                                                                HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\zonemap\
    Opens key:
                                                                HKLM\software\wow6432node\policies\microsoft\internet
 explorer\restrictions
```

HKLM\software\policies\microsoft\internet explorer\restrictions

Opens key:

```
Opens key:
                                                                 HKCU\software\policies\microsoft\internet explorer\restrictions
                                                                 HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
    Opens key:
 f4ceaaf59cfc}
                                                                 HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
    Opens key:
f4ceaaf59cfc}\treatas
    Opens key:
                                                                 HKCR \setminus wow6432 node \setminus clsid \setminus \{50d5107a-d278-4871-8989-f4ceaaf59cfc\} \setminus treatas
    Opens key
                                                                 HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
 f4ceaaf59cfc}\progid
                                                                 HKCR \setminus wow6432 node \\ clsid \setminus \{50d5107a-d278-4871-8989-f4ceaaf59cfc\} \setminus progid
    Opens key:
                                                                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
     Opens key:
    Opens key:
                                                                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
                                                                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
    Opens key:
f4ceaaf59cfc}\progid
                                                                 Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
    Opens key:
f4ceaaf59cfc}\inprocserver32
                                                                 HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989
    Opens key:
f4ceaaf59cfc}\inprocserver32
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler32
    Opens key:
                                                                 HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler32
                                                                 HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
    Opens key:
f4ceaaf59cfc}\inprochandler
    Opens key:
                                                                 HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler
                                                                 HKCU\software\policies\microsoft\internet explorer\control panel
    Opens key:
                                                                 HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_iedde_register_urlecho
    Opens key:
                                                                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature iedde register urlecho
                                                                 HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
    Opens key:
00aa00bbbb58}
    Opens key:
                                                                 HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
    Opens key:
                                                                 HKCR \setminus wow 6432 node \\ clsid \setminus \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \setminus treatas
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1
00aa00bbbb58}\progid
    Opens key:
                                                                 HKCR \setminus wow6432 node \\ clsid \setminus \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \setminus progid
    Opens key
                                                                 HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1
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\w
                                                                                      v6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler32
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler
     Opens key:
                                                                 HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler
    Opens key:
                                                                 HKLM\software\wow6432node\microsoft\windows script\features
    Opens key:
                                                                 HKLM\software\wow6432node\microsoft\com3
     Opens key:
HKCU \setminus software \\ \\ classes \\ appid \\ \\ 62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exeel \\ \\ classes \\ \\ appid \\ \\ bef0774b2baa23c901e164b0c7afbb.exeel \\ \\ classes \\ \\ appid \\ bef0774b2baa23c901e164b0c7afbb.exeel \\ \\ classes \\ \\ class
    Opens key:
HKCR\appid\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
    Opens key:
                                                                 HKLM\software\wow6432node\microsoft\ole\appcompat
    Opens key:
                                                                 HKLM\software\microsoft\ole\appcompat
    Opens key:
                                                                 HKLM\system\currentcontrolset\control\lsa
    Opens key:
HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} wow 6432 node \label{lem:hklm} icrosoft \label{lem:hklm} software \label{lem:hklm} wow 6432 node \label{lem:hklm} wow 6432 n
provider
                                                                 HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
    Opens key:
     Opens key:
{\tt HKLM} \verb|\system| current controlset| policies| microsoft| cryptography| configuration and the substitution of the substit
                                                                 HKLM\software\policies\microsoft\cryptography
    Opens key:
    Opens key:
                                                                 HKLM\software\microsoft\cryptography
                                                                 HKLM\software\wow6432node\microsoft\cryptography\offload
     Opens key:
    Opens key
                                                                 0000000000463
                                                                 HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
    Opens key:
                                                                 HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
00000000046}\proxystubclsid32
                                                                 HKCR\w
                                                                                     w6432node\interface\{00000134-0000-0000-c000-
    Opens key:
000000000046}\proxystubclsid32
    Opens key:
                                                                 HKLM\system\currentcontrolset\services\bfe
    Opens key:
                                                                 HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| internet explorer\\| recovery
                                                                 HKLM\software\policies\microsoft\internet explorer\recovery
    Opens kev:
                                                                 HKCU\software\microsoft\internet explorer\recovery
     Opens kev
                                                                 HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_scripturl_mitigation
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_scripturl_mitigation
    Opens key:
                                                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecor
                                                               ntrol\feature_block_lmz_img
    Opens key:
                                                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature behaviors
    Opens key:
                                                                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
    Opens key:
                                                                 HKLM\software\wow6432node\microsoft\internet explorer\default behaviors
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}
                                                                 HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{3050f4cf-98b5-11cf-bb82-00aa00bdce0b\}
    Opens key:
    Opens key:
                                                                 HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\treatas
                                                                 HKCR \verb|\wow6432| node \verb|\clsid| \{3050f4cf-98b5-11cf-bb82-00aa00bdce0b\} \verb|\treatas| node \verb|\clsid| \} treatas| for the substitution of the substit
    Opens key:
```

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

Opens key:

```
00aa00bdce0b}\progid
                                   HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid
  Opens key:
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82
00aa00bdce0b}
                                   er32
  Opens key:
                                   HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
                                   HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\inprochandler32
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
                                   HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}
                   \inprochandler
  Opens key:
                                   HKCU\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
                                   HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
  Opens key:
dc030521aabd3
                                   HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
  Opens kev:
  Opens key:
                                   HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{81397204 - f51a - 4571 - 8d7b - f51a -
dc030521aabd}\treatas
                                   HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd\\treatas
  Opens key:
  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\
                                               6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
                                   HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
  Opens key:
dc030521aabd}\inprochandler32
                                   HKCR\
                                                432node\clsid\{81397204-f51a-4571-8d7b
dc030521aabd}\inprochandler32
                                   HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
  Opens key:
dc030521aabd}\inprochandler
  Opens key:
                                   HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler
                                   HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
  Opens key:
3c8b00c100003
  Opens key:
                                   HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\treatas
  Opens key:
                                   \label{local-cond} $$HKCR\wow6432node\clsid\\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\\{treatas}
  Opens kev
                                   HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\progid
  Opens key:
                                   HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
  Opens key:
  Opens key
                                   HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
                                   HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a
  Opens kev:
3c8b00c10000}\progid
                                   HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid
  Opens key:
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32
                                   HKCR
                                              w6432node\clsid\{d1fe6762-fc48-11d0-883a
3c8b00c10000}\inprocserver32
  Opens key
                                   HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler32
  Opens key:
                                   HKCR\
                                               6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler32
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler
                                   HKCR
                                              v6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
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:
                                   HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas
  Opens kev
                                   HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\progid
  Opens key:
                                   HKCR \setminus wow6432 \\ node \\ clsid \\ \{4fd2a832-86c8-11d0-8fca-00c04fd9189d\} \\ \setminus progid
                                   HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
  Opens key:
  Opens key:
                                   HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
  Opens key:
                                   HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca
00c04fd9189d}\progid
                                   HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid
  Opens key:
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32
  Opens key:
                                   HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocse
                                   er32
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler32
  Opens key:
                                   HKCR\
                                                432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler32
  Opens key
                                   HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler
                                   HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\setup
  Opens key:
  Opens key:
                                   {\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus setup}
  Opens key:
                                   HKLM\software\wow6432node\microsoft\windows\currentversion
  Opens key:
                                   HKLM\hardware\devicemap\video
                                   HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-
  Opens key:
1e1a187c13e9}\0000
  Opens key:
HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
  Opens key:
9dd4432fa2e9}\0000
```

HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-

Opens key:

```
0d8e74595f78}\0000
                                                      HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
   Opens key:
8ed0c8eb59a8}\0000
   Opens key:
                                                      HKLM\software\wow6432node\microsoft\directdraw\compatibility
   Opens key:
                                                      HKLM\software\wow6432node\microsoft\directdraw\compatibilitv\bug!
   Opens key:
HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} Wow 6432 node \label{limits} in the limit \label{limits} If the limit \label{limits} If the limit \label{limits} is a simple constant \label{limits} If the limit \l
   Opens key:
                                                      Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus direct draw \setminus compatibility \setminus mortal kombat 3
   Opens key:
                                                      HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98
   Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibilitv\nhlpowerplay
   Opens key:
Opens key:
                                                      HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
squadron
   Opens key:
                                                      HKLM\software\wow6432node\microsoft\directdraw\compatibilitv\savage
   Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet
   Opens kev:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder
   Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100
   Opens key:
HKLM\softwa
                           e\wow6432node\microsoft\directdraw\compatibility\starcraft115
   Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo
                                                      HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide
   Opens key:
    Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension
   Opens key:
HKL\dot{M} \setminus soft \dot{w} are \setminus wow 6432 node \setminus microsoft \setminus direct draw \setminus compatibility \setminus ziff davis quality benchmark the following of the following of the following properties of the following of the following properties of the 
HKLM\software\wow6432node\microsoft\directdraw\compatibilitv\ziffdaviswinmarkbenchmark
                                                      HKLM\software\wow6432node\microsoft\directdraw\gammacalibrator
   Opens key:
                                                      HKLM\software\wow6432node\microsoft\directdraw
   Opens key:
   Opens key:
                                                      HKLM\software\wow6432node\microsoft\direct3d
   Opens key:
                                                      HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1
                                                      Opens key:
f941e9b7e1fe}
   Opens key:
                                                      HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
   Opens key:
                                                      HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\treatas
                                                      \label{local-cond} \begin{tabular}{ll} HKCR \wow6432 node \clsid \a7ee7f34-3bd1-427f-9231-f941e9b7e1fe} \label{local-cond} \end{tabular}
   Opens key:
   Opens key
                                                      f941e9b7e1fe}\progid
                                                      HKCR \setminus wow6432 \\ node \\ clsid \\ \{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe\} \\ \setminus progid
   Opens key:
   Opens key
                                                      HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32
                                                      HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
   Opens key
f941e9b7e1fe}\inprocserver32
                                                      HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
   Opens key:
f941e9b7e1fe}\inprochandler32
                                                      HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
   Opens key:
f941e9b7e1fe}\inprochandler32
   Opens key:
                                                      HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprochandler
                                                      HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
   Opens key:
f941e9b7e1fe}\inprochandler
   Opens key:
                                                      {\tt HKCU \setminus software \setminus classes \setminus dximage transform.microsoft.shadow}
   Opens key:
                                                      HKCR\dximagetransform.microsoft.shadow
   Opens key:
                                                      HKCU\software\classes\dximagetransform.microsoft.shadow\clsid
    Opens key:
                                                      HKCR\dximagetransform.microsoft.shadow\clsid
   Onens key
                                                      HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}
   Opens key:
                                                      HKCR \setminus wow6432 \\ node \\ \clsid \\ \{e71b4063-3e59-11d2-952a-00c04fa34f05\}
                                                      HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{e71b4063-3e59-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-952a-11d2-95000-95000-95000-95000-95000-95000-95000-95000-95000-95000-95000-95000-95000-95000-95000-
    Opens key
00c04fa34f05}\treatas
                                                      \label{local-eq:hkcrwow6432} HKCR\wow6432 node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\\\ \treat as
   Opens key:
    Opens key:
                                                      HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\progid
                                                      HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid
   Opens key:
                                                      HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a
   Opens key:
00c04fa34f05}\inprocserver32
   Opens key:
                                                      HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32
                                                      HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
   Opens key:
00c04fa34f05}\inprochandler32
   Opens key:
                                                      HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprochandler32
   Opens key:
                                                      HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprochandler
   Opens key:
                                                      HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprochandler
   Opens key
                                                      HKLM\software\wow6432node\microsoft\internet explorer\activex
compatibility
   Opens key
                                                      HKLM\software\wow6432node\microsoft\internet explorer\activex
compatibility\{e71b4063-3e59-11d2-952a-00c04fa34f05}
   Opens key
                                                      HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db3
                                                      HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
   Opens key:
   Opens key:
                                                      HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\treatas
   Opens key:
                                                      HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas
                                                      HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
   Opens key:
0000f87557db}\progid
                                                      Opens key:
   Opens key:
                                                      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\{4ch26c03-ff93-11d0-817e-0000f87557dh}\progid
                         HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
 Opens key:
0000f87557db}\inprocserver32
                         HKCR
                                  /6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32
                         HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
 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\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}
 Opens key:
                         HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
 Opens kev:
                         HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\treatas
                          HKCR \ wow 6432 node \ clsid \ \{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd\} \ treat as
 Opens key:
 Opens key:
                          HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
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
 Opens key:
                         HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
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
 Opens key
                         HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandler
 Opens key:
                         HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandler
                         HKCU\software\classes\typelib
 Opens key:
                         HKCR\typelib
 Opens key:
 Opens key:
                          HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
 Opens key:
                          HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
 Opens key:
                          HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
 Opens key:
 Opens key:
                          HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047
00aa003b6061}\1.1\409
                          HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409
 Opens key:
 Opens key:
                         HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\9
 Opens key:
                          HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9
 Opens key:
                         HKCU\software\classes\tvpelib\{5e77eb03-937c-11d1-b047-
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
                          HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32
 Opens key:
 Opens key:
                         \label{thm:hkcu} \begin{tabular}{ll} HKCU \software \classes \typelib \ \{54314d1d-35fe-11d1-81a1-0000f87557db\} \end{tabular}
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
 Opens key:
                          HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
 Opens key:
                          HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
  Opens key:
 Opens key:
                          0000f87557db}\1.1\409
                          HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\409
 Opens key:
                          HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
  Opens key:
0000f87557db3\1.1\9
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\9
 Opens key:
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
 Opens key:
0000f87557db}\1.1\0
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db\\1.1\0
 Opens key:
                         HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
 Opens key:
0000f87557db}\1.1\0\win32
 Opens key:
                         HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32
 Opens key:
                         HKCU\software\classes\mime\database\content type\image/png
 Opens key:
                          HKCR\mime\database\content type\image/png
 Opens key:
                          HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}
                          HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
 Opens key:
                          HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
 Opens key:
00aa006c1a01}\treatas
 Opens key:
                          HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
                          HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
                         HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
 Opens kev:
00aa006c1a01}\progid
                          HKCR \setminus wow6432 node \\ clsid \setminus \{30c3b080-30fb-11d0-b724-00aa006c1a01\} \setminus progid
 Opens key:
 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
 Opens key:
                          HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas
                          HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\progid
                          HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid
 Opens key:
 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\{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\{275c23e2-3747-11d0-9fea-
```

```
00aa003f8646}\inprocserver32
                                                    HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
   Opens key:
00aa003f8646}\inprocserver32
                                                    Opens key
00aa006c1a01}\inprochandler32
                                                    HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
   Opens key:
00aa006c1a01}\inprochandler32
   Opens key:
                                                    HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
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}
   Opens key:
                                                     HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{275c23e2-3747-11d0-9fea-1864\} + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + (1996-1996) + 
00aa003f8646}\inprochandler32
   Opens key:
                                                    HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler32
                                                    HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
   Opens key:
00aa003f8646}\inprochandler
   Opens key:
                                                    HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler
    Opens key:
                                                    HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
   Opens key:
                                                    HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\treatas
   Opens key:
                                                    HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
    Opens key:
                                                     HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724
00aa006c1a01}\progid
                                                    HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid
   Opens key:
                                                     HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724
   Opens key
00aa006c1a01}\inprocser
                                                    er32
   Opens key:
                                                    HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
   Opens key:
                                                    00aa006c1a01}\inprochandler32
   Opens key:
                                                    HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler32
   Opens key:
                                                    00aa006c1a01}\inprochandler
                                                    HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
   Opens key:
00aa006c1a01}\inprochandler
    Opens key:
                                                    HKCU\software\classes\mime\database\content type
   Opens key
                                                     HKCR\mime\database\content type
   Opens key:
                                                    HKCU\software\classes\mime\database\content type\image/bmp\bits
   Opens key:
                                                     HKCR\mime\database\content type\image/bmp\bits
    Opens key:
                                                     HKCU\software\classes\mime\database\content type\image/gif\bits
   Opens key:
                                                     HKCR\mime\database\content type\image/gif\bits
                                                     HKCU\software\classes\mime\database\content type\image/jpeg\bits
   Opens key:
    Opens key:
                                                     HKCR\mime\database\content type\image/jpeg\bits
    Opens key:
                                                     HKCU\software\classes\mime\database\content type\image/pjpeg\bits
                                                    HKCR\mime\database\content type\image/pjpeg\bits
HKCU\software\classes\mime\database\content type\image/png\bits
   Opens key:
   Opens kev:
                                                     HKCR\mime\database\content type\image/png\bits
    Opens kev
   Opens key:
                                                     HKCU\software\classes\mime\database\content type\image/tiff\bits
   Opens key:
                                                    HKCR\mime\database\content type\image/tiff\bits
HKCU\software\classes\mime\database\content type\image/x-icon\bits
   Opens key:
    Opens key:
                                                     HKCR\mime\database\content type\image/x-icon\bits
   Opens key:
                                                     \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \simple \classes \mime \mime
   Opens key:
                                                     HKCR\mime\database\content type\image/x-jg\bits
                                                     HKCU\software\classes\mime\database\content type\image/x-png\bits
   Opens key:
                                                     HKCR\mime\database\content type\image/x-png\bits
    Opens key:
   Opens key:
                                                     \label{local-content} $$HKCU\software\classes\mbox{\sc mime}\database\content type\label{local-content} $$type\sc mime\database\content type\sc mime\datab
   Opens key:
                                                     HKCR\mime\database\content type\image/x-wmf\bits
                                                     HKCU\software\classes\mime\database\content type\image/x-png
   Opens key:
    Opens key:
                                                     {\tt HKCR\mime\database\content\ type\image/x-png}
   Opens key
                                                    HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}
   Opens key:
                                                     HKCR \setminus wow6432 \\ node \\ \clsid \\ \{a3ccedf7-2de2-11d0-86f4-00a0c913f750\}
                                                    Opens key
00a0c913f750}\treatas
                                                     HKCR \setminus wow6432 node \\ clsid \\ \{a3ccedf7-2de2-11d0-86f4-00a0c913f750\} \\ \\ treat as
   Opens key:
    Opens key:
                                                     HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\progid
                                                     HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid
   Opens key:
   Opens key:
                                                     HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4
00a0c913f750}\inprocserver32
   Opens key:
                                                    HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
                                                    HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
   Opens key:
00a0c913f750}\inprochandler32
   Opens key:
                                                    HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler32
   Opens key:
                                                     HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler
   Opens key:
                                                    HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\international\scripts\26
   Opens key:
                                                    HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefall back\simsun|
   Opens key:
                                                    HKCU\software\microsoft\internet
explorer\mai
                                                    trol\feature_binary_caller_service_provider
   Opens key:
                                                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
Opens key: HKCU\software\classes\wow6432node\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
   Opens key:
                                                    HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
   Opens key:
                                                     00c04fd90119}
   Opens key:
                                                     HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119}
                                                     HKCU\software\classes\wow6432node\interface\{332c4425-26cb-11d0-b483-
   Opens kev
00c04fd90119}\proxystubclsid32
                                                    HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-
   Opens key:
```

```
00c04fd90119}\proxystubclsid32
                                                                        HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
    Opens key:
000000000046}
                                                                        HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}
     Opens key:
     Opens key:
                                                                        HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\treatas
     Opens key:
                                                                        \label{locality} HKCR \land 00020424-0000-0000-c000-00000000046 \land treat as \\
     Opens key
                                                                        HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\progid
                                                                        \label{localization} \mbox{HKCR} $$ Wow6432 node\clsid\\ 00020424-0000-0000-c000-00000000046\\ \mbox{progid} $$ $$ \mbox{HKCR}$$ $$ Wow6432 node\clsid\\ \mbox{progid} $$ \mbox{HKCR}$$ $$ \mbox{progid} $$ $$ \mbox{HKCR}$$$ $$ \mbox{progid} $$ \mb
     Opens key:
                                                                        HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}
     Opens key:
     Opens key:
                                                                        HKCR\clsid\{00020424-0000-0000-c000-00000000046}
                                                                        HKCU\software\classes\clsid\{00020424-0000-0000-c000-
     Opens key:
000000000046}\progid
                                                                        Opens key:
     Opens key:
                                                                        HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32
     Opens key:
                                                                        HKCR\
                                                                                         wow6432node\clsid\{00020424-0000-0000-c000
00000000046}\inprocserver32
    Opens key:
                                                                        HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
     Opens key:
                                                                        HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
                                                                        HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
    Opens key:
000000000046}\inprochandler
                                                                        HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}\inprochandler
                                                                        HKCU\software\classes\mime\database\content type\image/gif
     Opens key:
                                                                        HKCR\mime\database\content type\image/gif
     Opens key:
     Opens key:
                                                                        HKCU\software\classes\mime\database\content type\application/javascript
     Opens key:
                                                                        {\tt HKCR\mbox{\tt mime}\database} \content\ type\application/javascript
                                                                        HKCU\software\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
                                                                        HKLM\software\wow6432node\microsoft\internet
     Opens key:
\verb|explorer\main\featurecontrol\feature\_custom\_image\_mime\_types\_kb910561| \\
                                                                        HKCU\software\microsoft\internet
    Opens key:
\verb|explorer\main\featurecontrol\feature\_cross\_domain\_redirect\_mitigation| \\
     Opens key:
                                                                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
                                                                        HKCU\software\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_block_lmz_script
     Opens key:
                                                                        HKLM\software\wow6432node\microsoft\internet
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 \verb|\software| \verb|\wow6432| node \verb|\microsoft| internet|
explorer\main\featurecontrol\feature activex inactivate mode removal revert
     Opens key:
                                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol
    Opens key:
                                                                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature use windowedselectcontrol
                                                                        HKCU\software\microsoft\internet explorer\new windows
     Opens key:
     Opens key:
                                                                        HKLM\software\wow6432node\microsoft\internet explorer\new windows
Opens key: HKCU\software\micro explorer\main\featurecontrol\feature_xmlhttp
                                                                        HKCU\software\microsoft\internet
                                                                        HKLM\software\wow6432node\microsoft\internet
     Opens key:
\verb|explorer\main\featurecontrol\feature\_xmlhttp| \\
    Opens key:
                                                                        HKCU\software\classes\shockwaveflash.shockwaveflash
     Opens key:
                                                                        HKCR\shockwaveflash.shockwaveflash
                                                                        HKCU\software\classes\shockwaveflash.shockwaveflash\clsid
     Opens key:
     Opens key:
                                                                        HKCR\shockwaveflash.shockwaveflash\clsid
                                                                        HKCU \setminus software \setminus classes \setminus wow 6432 \\ 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-
     Opens key:
 444553540000
     Opens key:
                                                                        HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
     Onens key
                                                                        HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\treatas
     Opens key:
                                                                        HKCR \verb|\wow6432| node \verb|\clsid| \{d27cdb6e-ae6d-11cf-96b8-444553540000\} \verb|\treatas| \} treatas |\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=\wid
                                                                        HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
     Opens key
444553540000}\progid
    Opens key:
                                                                        HKCR \verb|\wow6432| node \verb|\clsid| \{d27cdb6e-ae6d-11cf-96b8-444553540000\} \verb|\progid| \} where $d_1 = d_2 = d_2
     Opens key:
                                                                        HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8
444553540000}\inprocserver32
                                                                        HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
    Opens key:
444553540000}\inprocserver32
                                                                        HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler32
                                                                        HKCR\w
                                                                                              w6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
    Opens key:
444553540000}\inprochandler32
                                                                        HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
     Opens key:
444553540000}\inprochandler
                                                                        HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
     Opens kev:
444553540000}\inprochandler
                                                                        HKLM \verb|\hardware\description\system\central processor \verb|\lambda| 0
     Opens key:
     Opens key:
                                                                        HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001
     Opens key:
                                                                        HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}
     Opens key:
                                                                        \label{local-equation} $HKCR\times \frac{d27cdb6b-ae6d-11cf-96b8-444553540000}$ \\ HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444533540000}\tabularter{label-equation} $$1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1.0$ \\ $1
     Opens key:
                                                                        HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0
     Opens key:
     Opens key:
                                                                        HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\409
                                                                        HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\409
     Opens key:
     Opens key:
                                                                        HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\9
     Opens key:
                                                                        HKCR\tvpelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\9
                                                                        HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
     Opens key:
444553540000}\1.0\0
                                                                        Opens key:
     Opens kev:
                                                                        HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\0\win32
                                                                        HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32
     Opens key:
     Opens key:
                                                                        HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
```

```
HKCR\typelib\{00020430-0000-0000-c000-000000000046}
   Opens key:
                                             HKCU\software\classes\typelib\{00020430-0000-0000-c000-0000000046}\2.0
   Opens key:
   Opens key:
                                             HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0
                                             HKCU\software\classes\typelib\{00020430-0000-0000-c000-
   Opens key:
000000000046}\2.0\0
                                            HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0
   Opens key:
   Opens key:
                                             HKCU\software\classes\typelib\{00020430-0000-0000-c000
000000000046}\2.0\0\win32
                                             HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32
   Opens key:
                                             HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
   Opens key:
                                             HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
   Opens key:
   Opens key:
                                             HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
   Opens key:
   Opens key:
                                             HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
00c04fb6bfc4}\1.0\0
   Opens key:
                                             HKCR \verb|\typelib|{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4} \verb|\t,0|| 0
   Opens kev:
                                            HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
00c04fb6bfc4}\1.0\0\win32
                                             HKCR \ typelib \ \{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4\} \ 1.0 \ 0 \ win 32acconstant \ 1.0 
   Opens key:
   Opens key:
                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_domstorage
                                            HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_domstorage
                                            HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
  Opens key:
00c04fb6bfc4}
   Opens key:
                                             HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
   Opens key
                                            HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
                                             HKCR \ wow 6432 node \ clsid \ \{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4\} \ treat as
   Opens key:
                                             HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{7b8a2d94-0ac9-11d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-896c-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-8966-14d1-896
00c04fb6bfc4}\progid
                                             HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
   Opens key:
   Opens key:
                                             HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
                                             HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
   Opens key:
   Opens key:
                                             HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\progid
   Opens key:
                                             HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
   Opens key
                                            HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
                                            HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c
  Opens key:
00c04fb6bfc4}\inprocserver32
   Opens key
                                            HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
   Opens key:
                                            HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
   Opens key:
                                            HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler
   Opens key:
                                            HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler
                                             \label{localization} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\sc discovery}} \\
   Opens key:
                                             HKLM\software\wow6432node\microsoft\internet explorer\feed discovery
   Opens kev:
                                             HKCU\software\microsoft\ftp
   Opens kev
                                             HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_activex_repurposedetection
Opens key: HKLM\software\wow6432node\microsoft\internet
\verb|explorer'| \verb|main'| feature control'| feature active x_repurpose detection| \\
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activex compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
                                            HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_addon_management
   Opens key:
                                            HKLM \ software \ wow 6432 node \ microsoft \ internet
explorer\main\featurecontrol\feature addon management
   Opens key:
                                             HKCU\software\microsoft\internet
                                           ntrol\feature_alloweddomainlist
   Opens key:
                                            HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature alloweddomainlist
  Opens key:
                                            \label{lem:hklm} \verb+KKLM\software\wow6432node\microsoft\internet explorer\extension
compatibility\{d27cdb6e
                                            ae6d-11cf-96b8-444553540000}
                                            HKCU\software\classes\wow6432node\clsid\{aaf8c6ce-f972-11d0-97eb-
  Opens key:
00aa00615333}
   Opens key:
                                             HKCR \setminus wow 6432 \\ node \\ \clsid \\ \{aaf8c6ce-f972-11d0-97eb-00aa00615333\}
   Opens key:
                                             \label{lem:hkcu} \verb+KKCU\software\microsoft\code store database\distribution units
  Opens key:
                                            HKLM\software\wow6432node\microsoft\code store database\distribution
units
  Opens key:
                                             HKLM\software\wow6432node\microsoft\code store database\distribution
units\{d27cdb6e-ae6d-11cf-96b8-444553540000}
                                            HKCU\software\classes\wow6432node\clsid
  Opens key:
                                             HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\availableversion
  Opens key:
                                            HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\availableversion
   Opens key:
                                            HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\installedversion
   Opens key:
                                            HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\installedversion
   Opens key:
                                            HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\appid
                                            HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\appid
   Opens key:
   Opens key
                                             HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8
444553540000}\languagecheckperiod
  Opens key
                                            HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\languagecheckperiod
  Opens key:
                                             HKCU\software\microsoft\internet
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
                                            HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus
  Opens key:
                                            HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
   Opens key:
444553540000}\miscstatus\1
   Opens key:
                                            HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
```

```
444553540000}\miscstatus\1
                                   HKLM\software\wow6432node\microsoft\windows\tablet pc\
  Opens key:
  Opens key:
                                   HKCU\software\classes\mime\database\content type\application/x-
shockwave-flash
  Opens kev:
                                   HKCR\mime\database\content type\application/x-shockwaye-flash
                                   HKCU\software\classes\protocols\filter\application/x-shockwave-flash
  Opens key:
  Opens key:
                                   HKCR \verb|\protocols| filter \verb|\application| / x-shockwave-flash
  Opens key
                                   HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}
                                   HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
  Opens key:
00c04f983e60}\treatas
                                   HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\treatas
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
  Opens key:
00c04f983e60}\progid
  Opens key:
                                   HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid
                                   HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e
  Opens kev:
00c04f983e60}\inprocserver32
                                   HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
  Opens key:
00c04f983e60}\inprocserver32
                                   HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
  Opens kev:
00c04f983e60}\inprochandler32
  Opens key:
                                   HKCR\
                                              w6432node\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
                                   HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| msxml30
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata
                                   HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32
  Opens key:
  Opens key:
\label{lem:hkcu} \verb|HKCU| system| current control set \verb|control| media properties \verb|private properties| joystick \verb|winm| in the system control set \verb|control| media properties \verb|private properties| joystick \verb|winm| in the system control set \verb|control| media properties \verb|private properties| joystick \verb|winm| in the system control set \verb|control| media properties \verb|private properties| joystick \verb|winm| in the system control set \verb|control| media properties | joystick \verb|winm| in the system control set \verb|control| media properties | joystick \verb|winm| in the system control set | joystick | joystick
                                   Opens key:
  Opens key:
                                   HKLM\system\currentcontrolset\control\securityproviders
  Opens key:
  Opens key:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache
  Opens key:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
  Opens key:
                                   HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
                                   HKCU\software\microsoft\internet explorer\domstorage\baidu.com
  Opens key:
  Opens key:
                                   HKCU\software\microsoft\internet explorer\domstorage\total
                                   HKLM\software\wow6432node\policies\microsoft\internet explorer\services HKLM\software\policies\microsoft\internet explorer\services
  Opens key:
  Opens key:
  Opens key:
                                   HKCU\software\microsoft\internet explorer\services
  Opens key:
                                   {\tt HKLM \ } software \verb|\ wow 6432 node \verb|\ policies \verb|\ microsoft \verb|\ internet| \\
explorer\activities
  Opens key:
                                   HKLM\software\policies\microsoft\internet explorer\activities
  Opens key:
                                   HKCU\software\microsoft\internet explorer\activities
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet explorer\activities
                                   HKLM\software\wow6432node\policies\microsoft\internet
  Opens kev:
explorer\infodelivery\restrictions
                                   HKLM\software\policies\microsoft\internet
  Opens key:
explorer\infodelivery\restrictions
                                   HKCU\software\policies\microsoft\internet
  Opens key:
explorer\infodelivery\restrictions
  Opens key:
                                   \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM\software\wow6432node\policies\microsoft\internet\ explorer\suggested \end{tabular}
sites
  Opens key:
                                   HKLM\software\policies\microsoft\internet explorer\suggested sites
  Opens key:
                                   HKCU\software\microsoft\internet explorer\suggested sites
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\system
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
  Opens key:
                                   HKLM\software\microsoft\windows\currentversion\policies\system
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Opens key:
08002b30309d}\shellfolder
Opens key: 00a0c90a8f39}
                                   HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
  Opens key:
                                   HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\treatas
                                   HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas
  Opens key:
  Opens key:
                                   HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\progid
  Opens key:
                                   HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
                                   HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
  Opens key:
                                   HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
  Opens key:
                                   HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
  Opens key:
00a0c90a8f39}\progid
                                   HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
  Opens kev:
                                   HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
  Opens kev
00a0c90a8f39}\inprocser
                                   er32
  Opens key:
                                   HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserver32
                                   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
                                   HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
  Opens key:
00a0c90a8f39}\inprochandler
  Opens key:
                                   HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee853
  Opens key:
                                   HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
  Opens key:
                                   HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
  Opens key:
                                   HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
```

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

```
Opens key:
a2d8-08002b30309d}\shellfolder
                                  HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
  Opens key:
0080c7f4ee85}\forward
  Opens key:
                                  HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
  Opens key:
                                  HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
                                  HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
  Opens key:
  Opens key:
Opens kev:
11e3-a68e-806e6f6e6963}\
  Opens key:
                                  HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\tvpelib
  Opens key:
                                  HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib
  Opens key:
                                  HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
                                  HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
  Opens kev:
                                  HKCU\software\classes\drive\shellex\folderextensions
  Opens key:
  Opens key:
                                  HKCR\drive\shellex\folderextensions
Opens key:
4442-804e-409d6c4515e9}
                                  HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
  Opens key:
                                  HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e93
  Opens key:
11e3-a68e-806e6f6e6963}\
  Opens key:
                                  HKCU \setminus software \setminus classes \setminus typelib \setminus \{eab22ac0-30c1-11cf-a7eb-0000c05bae0b\} \setminus 1.1
                                  HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
  Opens key:
  Opens key:
                                  HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0
  Opens key:
                                  HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
  Opens key:
                                  HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0\win32
  Opens key:
                                  HKCR \ typelib \ \{eab22ac0-30c1-11cf-a7eb-0000c05bae0b\} \ 1.1 \ 1.0 \ win 32ac0-30c1-11cf-a7eb-0000c05bae0b\} \ 1.1 \ 1.0 \ win 32ac0-30c1-11cf-a7eb-0000c05bae0b\} \ 1.0 \ win 32ac0-30c1-11cf-a7eb-0000c05bae0b\} \ 1.0 \ win 32ac0-30c1-11cf-a7eb-0000c05bae0b
                                  HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Opens key:
b8dc300d9f9d}
                                  HKCR \\ wow 6432 \\ 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 \setminus wow6432 \\ node \\ clsid \\ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\} \\ \\ treatas
                                  HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\progid
                                  HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
  Opens key:
  Opens key:
                                  HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
                                  HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
  Opens key:
  Opens key:
                                  HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\progid
                                  HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
  Opens key:
  Opens key:
                                  HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
                                  HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Opens key:
b8dc300d9f9d}\inprocserver32
  Opens key:
                                  HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-
0000000000463
                                  HKCR\wow6432node\interface\{00020400-0000-0000-c000-00000000046}
  Opens key:
  Opens key
                                  HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:
                                  HKCR\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
                                  0000000000463
                                  HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Opens key:
b8dc300d9f9d}\inprochandler32
                                  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
                                  HKCR\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}
  Opens key:
                                  HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
  Opens key:
000000000046}\treatas
                                  HKCR\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}\treatas
  Opens key:
                                  HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c0000-
  Opens kev
000000000046}\progid
                                  HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\progid
  Opens key:
                                  HKCU\software\classes\clsid\{00020420-0000-0000-c000-00000000046}
  Opens kev:
                                  HKCR\clsid\{00020420-0000-0000-c000-00000000046}
  Opens key:
                                  HKCU\software\classes\clsid\{00020420-0000-0000-c000-
  Opens key:
000000000046}\progid
  Opens key:
                                  HKCR\clsid\{00020420-0000-0000-c000-00000000046}\progid
  Opens key:
                                  HKCU\software\microsoft\windows\currentversion\explorer
  Opens key
                                  HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:
                                  HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocser
                                 er32
  Opens key
                                  HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
                                  HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
  Opens key:
00000000046}\inprochandler32
  Opens key:
                                  HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
00000000046}\inprochandler
  Opens key:
                                  HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
00000000046}\inprochandler
  Opens key:
HKLM \label{thm:loss} which is a fixed by the statement of the statement
HKCU \ software \ microsoft \ windows \ shell \ associations \ urlassociations \ directory
```

```
Opens key:
                                                                                  HKCU\software\classes\directorv
     Opens key:
                                                                                  HKCR\directory
      Opens key:
                                                                                  HKCU\software\classes\directory\curver
      Opens key:
                                                                                  HKCR\directory\curve
                                                                                  HKCR\directory\
     Opens key:
                                                                                 HKCU\software\classes\directory\shellex\iconhandler
     Opens key:
      Opens key:
                                                                                  HKCR\directory\shellex\iconhandler
     Opens key:
                                                                                  HKCU\software\classes\folder
                                                                                 HKCR\folder
     Opens key:
                                                                                  HKCU\software\classes\folder\shellex\iconhandler
     Opens key:
                                                                                  HKCR\folder\shellex\iconhandler
      Opens key:
     Opens key:
                                                                                  HKCU\software\classes\allfilesystemobjects
                                                                                 HKCR\allfilesystemobjects
HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
     Opens key:
     Opens key:
                                                                                  HKCR\allfilesystemobjects\shellex\iconhandler
     Opens key:
     Opens key:
                                                                                  {\tt HKCU \ } software \verb|\ classes \verb|\ directory \verb|\ docobject|
     Opens kev:
                                                                                  HKCR\directorv\docobiect
      Opens key:
                                                                                  HKCU\software\classes\folder\docobject
                                                                                  HKCR\folder\docobject
     Opens key:
     Opens key:
                                                                                  HKCU\software\classes\allfilesystemobjects\docobject
                                                                                  HKCR\allfilesvstemobjects\docobject
     Opens kev:
                                                                                  HKCU\software\classes\directory\browseinplace
      Opens key:
     Opens key:
                                                                                  HKCR\directory\browseinplace
     Opens key:
                                                                                  HKCU\software\classes\folder\browseinplace
                                                                                  HKCR\folder\browseinplace
     Opens key:
      Opens key:
                                                                                  HKCU\software\classes\allfilesystemobjects\browseinplace
     Opens key:
                                                                                  {\tt HKCR\ leftle systemobjects\ browsein place}
                                                                                  HKCU\software\classes\directory\clsid
     Opens key:
                                                                                  HKCR\directory\clsid
     Opens key:
      Opens key:
                                                                                  HKCU\software\classes\folder\clsid
     Opens key:
                                                                                  HKCR\folder\clsid
                                                                                  HKCU\software\classes\allfilesystemobjects\clsid
     Opens key:
     Opens key:
                                                                                  HKCR\allfilesystemobjects\clsid
                                                                                  HKCU\software\classes\wow6432node\interface\{6d5140c1-7436-11ce-8034-
     Opens key
00aa006009fa3
     Opens key:
                                                                                  HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}
     Opens key
                                                                                  HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus interface \setminus \{6d5140c1-7436-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11ce-8034-11c
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}
     Opens key:
                                                                                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
     Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\treatas
     Opens key:
                                                                                  HKCR\wow6432 node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treat as
     Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\progid
                                                                                  HKCR\wow6432 node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid
     Opens key:
                                                                                 HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
     Opens key:
     Opens kev:
                                                                                  HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
      Opens kev
e4fddd701cba}\progid
                                                                                 Opens key:
     Opens key:
444553540000}
     Opens key:
                                                                                 HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
                                                                                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
     Opens key
e4fddd701cba}\inprocserver32
     Opens key:
                                                                                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32
     Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32
                                                                                 HKCR'
                                                                                                           w6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32
                                                                                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
     Opens key:
e4fddd701cba}\inprochandler32
                                                                                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
     Opens key
e4fddd701cba}\inprochandler32
                                                                                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
     Opens key:
e4fddd701cba}\inprochandler
     Opens key
                                                                                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler
                                                                                 HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c1as + 
     Opens key:
444553540000}\shellfolder
     Opens key:
                                                                                 HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\shellfolder
     Opens key:
                                                                                 HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c2a7 -
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
                                                                                  \label{local-cond} $$HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\ \progid $$
     Opens key:
     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
                                                                                 HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
     Opens key:
                                                                                  HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
      Opens key:
444553540000}\inprochandler32
                                                                                 HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
     Opens key
444553540000}\inprochandler32
                                                                                 HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{ff393560-c2a7-11cf-bff4-c1ases\} \setminus \{ff39560-c2a7-11cf-bff4-c1ases\} \setminus \{ff39560-c2a7-11cf-bff4-c1ases\} \setminus \{ff39560-c2a7-11cf-bff4-c1ases\} \setminus \{ff39600-c2a7-11cf-bff4-c1ases\} \setminus \{ff39600-c2a7-11cf-bff4-c1ases\} \setminus \{ff39600-c2a7-11cf-bff4-c1ases\} \setminus \{ff39600-c2a7-11cf-bff4-c1ases\} \setminus \{ff39600-c2a7-11cf-bff4-c1ases\} \setminus \{ff39600-c2a7-11cf-bff4-c1ases\} \setminus \{ff39600-c2a7-a1ases\} \setminus \{ff396000-c2a7-a1ases\} \setminus \{ff396000-c2a7-a1ases\} \setminus \{ff396000-c2a7-a1ases\} \setminus \{ff396000-c2a7-a1ases\} \setminus \{ff396000-c2a7-a1ases\} \setminus \{ff3960000-c2a7-a1ases\} \setminus \{ff396000-c2a7-a1ases\} \setminus \{ff39600000-c2a7-a1ases\} \setminus \{ff396000000000000
     Opens key:
444553540000}\inprochandler
     Opens key:
                                                                                 HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler
     Opens key:
HKLM \label{lem:hklm} KLM \label{lem:hklm} Which is the last of the lemma to the last of the last of
c2a7-11cf-bff4-444553540000}
                                                                                 HKCU\software\classes\wow6432node\interface\{00020404-0000-0000-c000-
     Opens key:
000000000046}
     Opens key:
                                                                                  HKCR\wow6432node\interface\{00020404-0000-0000-c000-00000000046}
```

```
Onens key
                                                                   HKCU\software\classes\wow6432node\interface\{00020404-0000-0000-c000-
000000000046}\proxystubclsid32
    Opens key:
                                                                   HKCR\wow6432node\interface\{00020404-0000-0000-c000-
00000000046}\proxystubclsid32
                                                                  HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
    Opens key:
000000000046}
    Opens key:
                                                                   HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}
    Opens key
                                                                   \label{local-cond} \mbox{HKCU\software\classes\wow6432} node\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\cls
000000000046}\treatas
                                                                   \label{localization} \mbox{HKCR} $$ Wow6432 node \clsid \end{0.0020421-0000-0000-c000-000000000046} \treat as $$ \mbox{Treat} $$ $$ A substitution of the context of the 
    Opens key:
     Opens key:
                                                                   HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\progid
                                                                   HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\progid
    Opens key:
                                                                   HKCU\software\classes\clsid\{00020421-0000-0000-c000-000000000046}
     Opens key:
                                                                   HKCR\clsid\{00020421-0000-0000-c000-00000000046}
     Opens key:
    Opens key:
                                                                   HKCU\software\classes\clsid\{00020421-0000-0000-c000-
000000000046}\progid
                                                                   HKCR\clsid\{00020421-0000-0000-c000-00000000046}\progid
    Opens key:
                                                                   HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\5.0\cache\extensible cache\mshist012016040820160409
                                                                  HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
    Opens key
000000000046}\inprocserver32
    Opens key
                                                                  HKCR
                                                                                        w6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32
    Opens key:
                                                                  00000000046}\inprochandler32
                                                                  HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
    Opens key
000000000046}\inprochandler32
                                                                  Opens key:
00000000046}\inprochandler
    Opens key:
                                                                  HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
00000000046}\inprochandler
                                                                  HKCU\software\microsoft\windows\currentversion\app
    Opens key:
paths\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
    Opens key:
                                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
                                                                  HKLM\software\microsoft\windows\currentversion\app
paths\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
Opens key: HKC
3aea-1069-a2d8-08002b30309d}
                                                                  HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
    Opens key:
Opens key:
                                                                  HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}
    Opens key:
                                                                   HKCR \setminus wow6432 node \\ clsid \\ \{20d04fe0-3aea-1069-a2d8-08002b30309d\}
    Opens key:
                                                                  HKCU\software\microsoft\internet explorer\main\windowssearch HKLM\software\policies\microsoft\internet explorer\feeds
    Opens key:
     Opens key:
                                                                   HKCU\software\microsoft\internet explorer\feeds
                                                                  HKLM\software\wow6432node\microsoft\internet explorer\feeds
     Opens key:
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
68ad-4d8a-87bd-30b759fa33dd}
    Opens key:
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}\propertybag
    Opens key:
                                                                   HKLM\software\wow6432node\microsoft\windows search
    Opens key:
                                                                   HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe2213
                                                                   HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}
    Opens key:
     Opens key:
                                                                   HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\treatas
                                                                  HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\treatas
    Opens key:
    Opens key:
                                                                  HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\progid
    Opens key:
                                                                  HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid
                                                                  HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
    Opens key:
0000f81fe221}\inprocserver32
                                                                  HKCR\\
                                                                                     ow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32
                                                                  HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
    Opens key:
0000f81fe221}\inprochandler32
                                                                  HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
    Opens key
0000f81fe221}\inprochandler32
                                                                  HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{f5078f35-c551-11d3-89b9-14432 node \setminus clsid \setminus \{f5078f35-c551-11d3-89b-14442 node \setminus clsid \setminus cl
    Opens key:
0000f81fe221}\inprochandler
    Opens key:
                                                                  HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprochandler
                                                                  HKCU\software\classes\shockwaveflash.shockwaveflash.7
    Opens key:
                                                                   HKCR\shockwaveflash.shockwaveflash.7
     Opens key:
    Opens key:
                                                                   HKCU\software\classes\shockwaveflash.shockwaveflash.7\clsid
    Opens kev:
                                                                   HKCR\shockwaveflash.shockwaveflash.7\clsid
     Opens kev
                                                                   HKCU\software\classes\mime\database\content type\image/x-icon
                                                                   HKCR\mime\database\content type\image/x-icon
    Opens key:
    Opens key:
                                                                   HKCU\software\classes\protocols\filter\image/x-icon
                                                                   HKCR\protocols\filter\image/x-icon
    Opens key:
     Opens key:
                                                                   HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_mime\_treat\_image\_as\_authoritative| \\
    Opens key:
                                                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
     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\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd\\treatas
                                                                  HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
    Opens key:
fd2b31b3eefd}\progid
                                                                  Opens key:
    Opens key:
                                                                   HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
    Opens key:
     Opens key:
                                                                   HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
```

fd2b31b3eefd}\progid

```
Opens key:
                                     HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\progid
                                    HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
  Opens key:
fd2b31b3eefd}\inprocserver32
                                    HKCR
                                                 /6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
  Opens key:
fd2b31b3eefd}\inprochandler32
                                    Opens key:
fd2b31b3eefd}\inprochandler32
                                    HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
  Opens key:
fd2b31b3eefd}\inprochandler
  Opens key:
                                    HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandler
  Queries value
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
  Queries value:
                                    HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \verb|\policies| microsoft \end{tabular} windows \end{tabular} safer \end{tabular} code identifiers [transparentenabled]
                                    HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Queries value:
                                    HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
  Queries value:
                                     HKCU\control panel\desktop[preferreduilanguages]
  Oueries value:
                                    HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Oueries value:
\label{local-prop} \begin{tabular}{ll} HKLM \end{tabular} Software \wow 6432 node \microsoft \windows \current version \side by side [prefer external manifest] \end{tabular}
  Queries value:
                                     Oueries value
                                     HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
                                     HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\gre_initialize[disablemetafiles]
                                     HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows
  Queries value:
nt \verb|\currentversion| compatibility 32[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb]| and the sum of the sum o
                                    HKLM\software\wow6432node\microsoft\windows
  Queries value:
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
settings[disableimprovedzonecheck]
  Oueries value:
                                    HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\windows\windows error
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]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\language groups[1]
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
Queries value: HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane1]|
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2] Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
                                     HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane5]|
  Oueries value:
                                     HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane6]|
  Queries value:
                                    HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane7]|
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
                                     HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane9]|
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
                                     HKLM\software\microsoft\windows
nt\current version\language pack\surrogatefall back[plane 11]
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                                     HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane13]|
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane14]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries 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:
  Oueries value
                                     HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
                                    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]
  Queries value:
                                    HKLM\software\microsoft\ole[maxsxshashcount]
```

```
Queries value:
\label{thm:local_computername} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ is the local computername (computername) $$ is the local 
                                                      HKLM\system\setup[oobeinprogress]
   Queries value:
    Oueries value:
                                                      HKLM\system\setup[systemsetupinprogress]
                                                     HKLM\software\microsoft\sqmclient\windows[ceipenable]
   Queries value:
    Queries value:
                                                      HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be18 - be
Oueries value:
                                                     HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
                                                      HKLM\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[createuricachesize]
   Queries value:
                                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
   Queries value
                                                     HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[createuricachesize]
   Oueries value
                                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
   Queries value:
                                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunvcode]
   Queries value:
                                                      HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
   Oueries value:
                                                     HKLM\software\wow6432node\microsoft\internet
explorer\\ \verb|main| featurecontrol| feature_http_username\_password\_disable[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
    Queries value:
                                                      HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_http\_username\_password\_disable[*]
   Queries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension] \end{tabular}
    Queries value:
                                                      {\tt HKLM \ } system \verb| `current control set \verb| services \verb| ldap[ldapclient integrity]| \\
   Oueries value
                                                      HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
                                                      HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
   Queries value:
   Queries value:
                                                      HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
                                                      \label{thm:condition} \begin{tabular}{ll} HKCU \software \mbox{$\stackrel{\cdot}{$}$ internet explorer $$ ietld[ietlddllversionhigh] $$ \end{tabular}
    Queries value:
   Oueries value
                                                      \label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\ietld[ietldversionlow]}}
                                                      HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
   Queries value:
    Queries value:
                                                      HKCU\software\microsoft\internet explorer\main[frametabwindow]
   Queries value:
                                                      HKLM\software\wow6432node\microsoft\internet
explorer\main[frametabwindow]
   Queries value:
                                                     HKCU\software\microsoft\internet explorer\main[framemerging]
                                                      HKLM\software\wow6432node\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]
    Queries value:
                                                      HKCU\software\microsoft\internet explorer\main[admintabprocs]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\internet
explorer\main[admintabprocs]
    Oueries value:
                                                     HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
                                                      HKLM\software\wow6432node\microsoft\internet
    Queries value:
explorer\main[tabprocgrowth]
                                                     HKLM\software\wow6432node\microsoft\internet
   Oueries 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 software \ microsoft \ windows \ current version \ policies \ explorer \ [no properties recyclebin] \ described \
   Queries 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[noco
   Oueries value
                                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[attributes]
   Queries value:
                                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[callforattributes]
                                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
   Queries value:
                                                      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-
08002b30309d}\shellfolder[usedrophandler]
                                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[wantsforparsing]
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value
08002b30309d \verb|\shellfolder[wantsparsedisplayname]|
                                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[queryforoverlay]
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value
08002b30309d}\shellfolder[mapnetdriveverbs]
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\shellfolder[queryforinfotip]
   Queries value:
                                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hideinwebview]
   Queries value:
                                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hideondesktopperuser]
   Oueries value
                                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsaliasednotifications]
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d \verb|\shellfolder[wantsuniversaldelegate]|
   Oueries value
                                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[nofilefolderjunction]
   Queries value:
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[pintonamespacetree]
                                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[hasnavigationenum]
```

42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]

Oueries value:

HKLM\software\microsoft\rpc[maxrpcsize]

```
Oueries value
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-
08002b30309d}1
                           HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
 Queries value
08002b30309d}\inprocserver32[1
 Queries value:
                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-0000000000046}
0xffff]
 Queries value:
                           HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
 Queries value:
                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[inprocserver32]
                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
 Queries value:
08002b30309d}\inprocserver32[threadingmodel]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
                          HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
 Oueries value:
                          \textbf{HKCU} \\ \textbf{software} \\ \textbf{microsoft} \\ \textbf{windows} \\ \textbf{currentversion} \\ \dot{\textbf{internet}} \\
 Queries value:
settings[urlencoding]
                          HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer \verb|\main| featurecontrol | feature\_unc\_saved filecheck [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature unc savedfilecheck[*]
 Queries value:
                           HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
 Queries value:
                          \label{thm:local_hammon_hammon} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet}} \ .
settings\zones\1[flags]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
 Queries value:
                           \label{thm:local_equation} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc 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\main\featurecontrol\feature localmachine lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
 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]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[fromcachetimeout]
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[secureprotocols]
 Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[secureprotocols]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablekeepalive]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disab]epassport]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\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]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings[enablehttp1_1]
 Oueries value:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyhttp1.1]
 Queries value
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablebasicoverclearchannel]
                          HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[category]
```

Queries value:

```
33be-4251-ba85-6007caedcf9d}[name]
        Queries value:
HKLM\software\w
                                                                                       v6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[parentfolder]
        Queries value:
 HKLM \label{lem:hklm} White the latest and the la
33be-4251-ba85-6007caedcf9d}[description]
        Oueries value:
```

 $HKLM \label{lem:hklm} In the latest and the lates$ 33be-4251-ba85-6007caedcf9d}[relativepath]

Queries value:

33be-4251-ba85-6007caedcf9d}[parsingname]

33be-4251-ba85-6007caedcf9d}[infotip] Oueries value: $HKLM \label{lem:hklm} In the latest and the lates$

33be-4251-ba85-6007caedcf9d}[localizedname]

Oueries value:

33be-4251-ba85-6007caedcf9d}[icon]

Oueries value:

33be-4251-ba85-6007caedcf9d}[security]

Oueries value:

 $HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} H$ 33be-4251-ba85-6007caedcf9d}[streamresource]

33be-4251-ba85-6007caedcf9d}[streamresourcetype]

Queries value:

33be-4251-ba85-6007caedcf9d}[localredirectonly]

Queries value:

33be-4251-ba85-6007caedcf9d}[roamable]

Oueries value:

 $HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} HK$ 33be-4251-ba85-6007caedcf9d}[precreate]

Queries value:

33be-4251-ba85-6007caedcf9d}[stream]

33be-4251-ba85-6007caedcf9d}[publishexpandedpath]

Oueries value:

 $HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} Which \label{li$ $33 be-4251-ba85-6007 caedcf9d \} [attributes] \\$

Oueries value:

33be-4251-ba85-6007caedcf9d}[foldertypeid]

Oueries value:

 $HK \dot{L} M \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{352481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-16481e8-1648168-$ 33be-4251-ba85-6007caedcf9d}[initfolderhandler]

Queries value:

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

folders[cache]

Queries value:

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

 $\label{thm:hklm} HKL^{M} software \verb|\wow6432node\microsoft\windows\currentversion\end{|linearize} explorer \verb|\folderdescriptions\fill{|linearize} folderdescriptions\fill{|linearize} folderdescriptions\fill{|l$

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

6fba-4fcf-9d55-7b8e7f157091}[parentfolder]

Queries value: 6fba-4fcf-9d55-7b8e7f157091}[description]

Queries value:

6fba-4fcf-9d55-7b8e7f157091}[relativepath]

Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-$ 6fba-4fcf-9d55-7b8e7f157091}[parsingname]

Oueries value:

 $HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} H$ 6fba-4fcf-9d55-7b8e7f157091}[infotip]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localizedname]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \ fflb 32785-respectively. \\$ 6fba-4fcf-9d55-7b8e7f157091}[icon]

Queries value:

6fba-4fcf-9d55-7b8e7f157091}[security]

Queries value:

 $HKLM \label{lem:hkkm} HKLM \label{lem:hkkm} HKLM \label{lem:hkkm} White \$ $6 fba-4 fcf-9 d55-7 b8 e7 f157091 \} [stream resource] \\$

Oueries value:

 $\label{thm:hamman} HKL^{M} software \\ \windows \\ \current version \\ \ext{explorer} folder descriptions \\ \ext{f1b32785-pt.} folder descriptions \\ \ext{f1b32785-pt.} folder descriptions \\ \ext{f2b32785-pt.} folder descriptions \\ \ext{f2b32785-pt.} folder descriptions \\ \ext{f3b32785-pt.} folder descriptions \\ \ext{f3b3278$ 6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]

Oueries value:

6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]

Queries value:

6fba-4fcf-9d55-7b8e7f157091}[roamable]

```
6fba-4fcf-9d55-7b8e7f157091}[precreate]
         Queries value:
 6fba-4fcf-9d55-7b8e7f157091}[stream]
         Oueries value:
6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
         Queries value:
6fba-4fcf-9d55-7b8e7f157091}[attributes]
6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
        Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-b12785-
6fba-4fcf-9d55-7b8e7f157091\} [initfolder handler]\\
        Oueries value:
                                                                                                                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders[local appdata]
         Queries value:
0e22-4760-9afe-ea3317b67173}[category]
         Queries value:
0e22-4760-9afe-ea3317b67173}[name]
         Queries value:
 HKLM \label{lem:hklm} While the latest and the la
0e22-4760-9afe-ea3317b67173}[parentfolder]
        Oueries value:
0e22-4760-9afe-ea3317b67173}[description]
         Oueries value:
HKLM \label{lem:hkk} Which was a function when the sum of the su
0e22-4760-9afe-ea3317b67173}[relativepath]
         Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[parsingname]
         Queries value:
0e22-4760-9afe-ea3317b67173}[infotip]
         Queries value:
 HKLM \label{lem:hklm} White the latest and the la
0e22-4760-9afe-ea3317b67173}[localizedname]
         Oueries value:
 HK LM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-market \ properties \ proper
 0e22-4760-9afe-ea3317b67173}[icon]
         Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{5e6c858f-microsoft\} \ descriptions \ \ descriptions \ \ descriptions 
0e22-4760-9afe-ea3317b67173}[security]
0e22-4760-9afe-ea3317b67173}[streamresource]
         Oueries value:
HKLM \label{lem:hklm} In the latest and the lates
0e22-4760-9afe-ea3317b67173}[streamresourcetype]
        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\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[precreate]
         Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[stream]
         Queries value:
0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
        Queries value:
 HKLM \label{lem:hklm} White the latest and the la
0e22-4760-9afe-ea3317b67173}[attributes]
        Oueries value:
 HK LM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-market \ properties \ proper
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-
980053277-1733835069-2361817685-1001[profileimagepath]
        Oueries value:
                                                                                                                                      HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\content[cacheprefix]
                                                                                                                                      HKCU\software\microsoft\windows\currentversion\internet
        Queries value:
settings\5.0\cache\content[cachelimit]
                                                                                                                                      HKCU\software\microsoft\windows\currentversion\internet
        Queries value:
 settings\5.0\cache\cookies[peruseritem]
        Queries value:
                                                                                                                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
        Queries value:
HKLM \label{limits} IN Most ware \verb|\wow6432| node \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| (2b0f765d-100) and the second s
 c0e9-4171-908e-08a611b84ff6}[category]
        Oueries value:
 \label{thm:hklm} HKL^{M} software \verb|\wow6432| node \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| \{2b0f765d-16b] and the statement of the statement 
c0e9-4171-908e-08a611b84ff6}[name]
         Oueries value:
c0e9-4171-908e-08a611b84ff6}[parentfolder]
         Queries value:
c0e9-4171-908e-08a611b84ff6}[description]
```

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

Queries value:

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]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:hklm} HKL^{M} software \verb|\wow6432| node \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| \{2b0f765d-16b] and the statement of the statement$ c0e9-4171-908e-08a611b84ff6}[stream]

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

folders[cookies]

Queries value:

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

Oueries value:

 $HKLM \label{lem:hklm} Software \label{lem:hklm} Which is the last of the last convex plane and the last convex plane and$ 65f9-4cf6-a03a-e3ef65729f3d}[name] Queries value:

 $HKLM \label{lem:hklm} Software \label{lem:hklm} Which is a few and the latest a$ 65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[description] Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-

65f9-4cf6-a03a-e3ef65729f3d}[relativepath] Queries value:

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

Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (3eb685db-10eb) \ descr$

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

Queries value:

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

Oueries value: $HK LM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{3eb685db-explorer\} \ begin{picture}(1,0) \put(0,0) \put(0$

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]

Oueries value:

 $65f9-4cf6-a03a-e3ef65729f3d \} [streamresource type] \\$

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value 65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\cookies[cacheprefix] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\history[peruseritem] HKLM\software\wow6432node\microsoft\windows\currentversion\internet ${\tt settings \ 1.0 \ cache \ history [peruseritem]}$ Oueries value: $HKLM \label{lem:hklm} In the latest and the lates$ b784-432e-a781-5a1130a75963}[category] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[name] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[parentfolder] b784-432e-a781-5a1130a75963}[description] Queries value: b784-432e-a781-5a1130a75963}[relativepath] Queries value: $\label{thm:hklm} HKL^{\tt Mklm} software \verb|\wow6432| node \verb|\windows\currentversion\explorer| folder descriptions \verb|\dgdc8a3b-equal to the content of the co$ b784-432e-a781-5a1130a75963}[parsingname] Oueries value: $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[infotip] Queries value: b784-432e-a781-5a1130a75963}[localizedname] Queries value: b784-432e-a781-5a1130a75963}[icon] Queries value: b784-432e-a781-5a1130a75963}[security] Oueries value: $HKLM \label{lem:hklm} In the latest and the lates$ b784-432e-a781-5a1130a75963}[streamresource] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[streamresourcetype] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[localredirectonly] b784-432e-a781-5a1130a75963}[roamable] Queries value: b784-432e-a781-5a1130a75963}[precreate] Oueries value: $\label{thm:hklm} HKL^{\tt Mklm} software \verb|\wow6432| node \verb|\windows\currentversion\explorer| folder descriptions \verb|\dgdc8a3b-equal to the content of the co$ b784-432e-a781-5a1130a75963}[stream] Oueries value: b784-432e-a781-5a1130a75963}[publishexpandedpath] Queries value: b784-432e-a781-5a1130a75963}[attributes] Queries value: b784-432e-a781-5a1130a75963}[foldertypeid] Queries value: b784-432e-a781-5a1130a75963}[initfolderhandler] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[history] Queries value: HKCU\software\microsoft\windows\currentversion\internet ${\tt settings\5.0\cache\history[cacheprefix]}$ Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\extensible cache\domstore[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cachepath] Queries value: $\label{thm:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \\$ 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\5.0\cache\extensible cache\feedplat[cacherepair] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cachepath] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cacheprefix] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cachelimit] HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cacheoptions]

```
Oueries value
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
  Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
                                            sible cache\iecompat[cachepath]
settings\5.0\ca
   Oueries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
   Queries value:
                                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
  Oueries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                                            \label{local-constraint} \begin{tabular}{ll} HKCU \end{tabular} in cross of the local constraint of 
   Queries value
settings\5.0\cache\extensible cache\ietld[cacherepair]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
  Oueries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
                                            Queries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
  Queries value
                                            \label{thm:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \\
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
   Queries value
                                            \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
                                            sible cache\privacie:[cacheoptions]
settings\5.0\cache
  Oueries value
                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
  Queries value:
                                            HKCU\software\policies\microsoft\windows\currentversion\internet
                                            wnloadfailureui]
settings[displayscriptde
  Oueries value
                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
   Queries value:
                                            \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \normalisation \part that the lemma is a simple of the lemma is
settings[mbcsapiforcrack]
                                            HKCU\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[utf8servernameres]
                                            HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[disableworkerthreadhibernation]
   Oueries value:
                                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
   Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[socketsendbufferlength]
                                            HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[socketreceivebufferlength]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[keepal
  Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxconnectionsperserver]
  Queries value:
                                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                                            HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[maxcor
                                           er1_0server]
  Oueries value:
                                            HKI M\software\
                                                                        ow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1 Oserver]
  Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxco
                                            erproxy]
   Oueries value
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Queries value:
                                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[connecttimeout]
  Oueries value:
                                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
   Queries value:
                                            \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings[connectretries]
  Oueries value:
                                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
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]
                                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[receivetimeout]
                                            \label{local-observation} \mbox{HKCU\software\mbox{\sc windows\currentversion\internet}} \\
  Queries value:
{\tt settings[disablentlmpreauth]}
                                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[scavengecachelo
                                            werbound]
   Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
  Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scave
                                            ngecachefilelifetime]
  Oueries value
                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Oueries value:
                                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
   Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpi
                                            rytimesecs]
  Oueries value
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                                            HKLM\software\wow6432node\microsoft\internet
explorer\\ \verb|main| featurecontrol| feature_disable\_unicode\_handle\_closing\_callback [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\
```

```
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]
  Queries value
                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
 Oueries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
{\tt settings[wpadsearchall domains]}
 Oueries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocacl
                             hecheck1
                              Queries value:
settings[bypasshttpnocachecheck]
                              HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocach
                             echeck]
 Queries value:
                              \label{thm:local_microsoft} \begin{tabular}{ll} HKLM \begin{tabular}{ll} software \begin{tabular}{ll} wow 6432 node \begin{tabular}{ll} microsoft \begin{tabular}{ll} windows \begin{tabular}{ll} current version \begin{tabular}{ll} internet \begin{tabular}{ll} current \begin{tabular}{ll} wow 6432 node \begin{tabular}{ll} microsoft \begin{tabular}{ll} wow 6432 node \begin{tabula
settings[bypasssslnocachecheck]
                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttptrace]
 Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodia
                              override]
 Oueries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
 Oueries value:
                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                              \label{lem:hkcu} \verb+kkcu's of tware \verb+micros of twindows \verb+current version \verb+internet+ \\
  Queries value:
settings[mimeexclusionlistforcache]
 Oueries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
                              \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \internet} \\ \end{tabular}
 Queries value:
settings[dnscacheenabled]
 Oueries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
 Oueries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                              HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonzonecross
                              ing]
                              HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonbadcertrecving]
                              HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpostr
 Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                              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\cur
                   rentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Oueries value:
Queries value:
Oueries value:
Oueries value:
Queries value:
HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries \code 000000000004 \[packed catalogitem] \end{subarray} \label{lem:hklm}
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000008[packedcatalogitem]
  Queries value:
Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Oueries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace\_catalog 5 [num\_catalog\_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
  Oueries value:
HKLM \\ system \\ current control set \\ services \\ winsock \\ 2 \\ parameters \\ namespace\_catalog \\ S \\ catalog\_entries \\ 0000000000001 \\ [displaystring]
```

Oueries value

Oueries value:

 $HKLM \ system \ current controls et \ services \ \ winsock \ 2 \ parameters \ names pace_catalog5 \ \ catalog_entries \ \ 000000000001 \ [address family]$ Queries value:

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

Queries value:

Oueries value:

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

Oueries value:

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

Oueries value:

Queries value:

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

Queries value:

Queries value:

Oueries value:

Queries value:

Oueries value:

Queries value:

Oueries value:

Queries value:

Oueries value:

Queries value:

Oueries value:

Queries value:

Oueries value: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog5 \ (catalog_entries \ 0000000000004 \ [displaystring]$

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

Queries value:

Queries value:

Queries value:

Oueries value

Queries value:

HKLM\system\cur rentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[storesserviceclassinfo] Oueries value:

 $HKLM \ system \ \ current control set \ services \ \ winsock 2 \ parameters \ \ namespace_catalog5 \ \ \ catalog_entries \ \ \ 0000000000004 \ [providerinfo]$ Queries value:

Oueries value:

 $HKL\\ M (system) current control set (services) win sock 2 parameters (name space_catalog5 (catalog_entries) (000000000005 [displaystring]) (displaystring) ($

Queries value:

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

Oueries value:

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

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

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

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring] Queries value:

Oueries value:

 $HKLM \ system \ current controls et \ services \ \ winsock \ 2 \ parameters \ namespace_catalog \ 5 \ catalog_entries \ \ 0000000000006 \ [address family]$ Queries value:

Oueries value:

Queries value:

Oueries value:

Queries value:

Oueries value:

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]
    Queries value:
                                                                    HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
    Oueries value:
                                                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disablebranchcache]
    Queries value:
                                                                    HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| tracing[enable consoletracing]
    Queries value:
                                                                    HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| tracing\\| rasapi 32[enable file tracing]|
                                                                    HKLM\software\wow6432node\microsoft\tracing\rasapi32[filetracingmask]
    Oueries value:
     Oueries value:
\label{local-observation} HKLM \software \wow 6432 node \microsoft \tracing \rasapi 32 [enable consoletracing]
    Queries value:
                                                                    HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus rasapi32 [consoletracing mask]
                                                                    HKLM\software\wow6432node\microsoft\tracing\rasapi32[maxfilesize]
    Oueries value:
                                                                    HKLM\software\wow6432node\microsoft\tracing\rasapi32[filedirectory]
     Queries value:
    Queries value:
                                                                    HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus tracing \setminus rasmancs [enable file tracing]
    Oueries value:
                                                                    HKLM\software\wow6432node\microsoft\tracing\rasmancs[filetracingmask]
    Queries value:
\label{local-prop} \mbox{HKLM\software\wow6432} node\mbox{\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware
                                                                    \label{thm:hklm:software} HKLM \software \swow6432 node \swicrosoft \tracing \rasmancs [consoletracing mask] \\ HKLM \software \swow6432 node \swicrosoft \tracing \rasmancs [maxfilesize] \\
    Queries value:
    Oueries value:
                                                                    HKLM\software\wow6432node\microsoft\tracing\rasmancs[filedirectory]
     Queries value:
     Queries value:
                                                                    HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
                                                                    HKLM\software\microsoft\sqmclient\windows\disabledprocesses[2ac077a7]
    Queries value:
     Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
    Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
    Queries value:
                                                                    HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
    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[proxyoverride]
    Oueries value:
                                                                    HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
    Queries value:
                                                                    HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacvsettings]
                                                                    HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings\connections[defaultconnectionsettings]
    Queries value:
                                                                    HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
                                                                    HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings\zonemap[autodetect]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
    Queries value:
{\tt HKLM \ } system \verb| current control set \verb| services \verb| tcpip \verb| parameters [disable adapter domain name] | the system \verb| current control set \verb| services \verb| tcpip \verb| parameters [disable adapter domain name] | the system \verb| current control set \verb| services \verb| tcpip \verb| parameters [disable adapter domain name] | the system \verb| current control set \verb| services \verb| tcpip \verb| parameters [disable adapter domain name] | the system \verb| current control set \verb| services \verb| tcpip \verb| parameters [disable adapter domain name] | the system \verb| tcpip \verb| parameters [disable adapter domain name] | the system \verb| tcpip \verb| parameters [disable adapter domain name] | the system \verb| tcpip \verb| tcpip \verb| parameters [disable adapter domain name] | the system \verb| tcpip tc
    Oueries value
HKLM\svstem\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
    Oueries value
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
    Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]
    Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} a prioritize record data \end{tabular} $$ a prioritize record
    Queries value:
HKLM \verb|\system| current controlset \verb|\services| dns cache \verb|\parameters[allow unqualified query]|
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [append to multilabel name]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
    Queries value:
Oueries 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]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
    Queries value:
                                                                    {\tt HKLM \ } \dot{s} {\tt ystem \ } \dot{s} {\tt ervices \ } dnscache \ | \ parameters [useedns]
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
    Oueries value:
\label{thm:local_control} \begin{tabular}{ll} HKLM \end{tabular} Aksign $$ \arrowvert $$ \arrowver
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
    Queries value:
                                                                    HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration enabled]
```

```
Oueries value
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
   Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
   Queries value:
Oueries 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]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters \texttt{[registration refreshinterval]}
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
   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:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
Oueries value:
\label{thm:local_thm} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]]{thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:local_thm:
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
  Queries value:
Queries value:
                                            \label{lem:hklmsystem} \verb| HKLM \rangle is stem \verb| current control set \verb| services \verb| dns cache \verb| parameters [dns test]| | \\
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
  Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$ KLM \end{tabular} $$ AKLM \end{tab
   Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[resolverregistration]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [resolver registration only]
   Queries 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]|
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
  Queries 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]
   Oueries value:
                                            HKLM\software\wow6432node\microsoft\internet
explorer\\ \verb|main| featurecontrol| feature\_mime\_handling[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
  Queries value:
                                            HKLM\software\wow6432node\microsoft\internet
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[]
   Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
                                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[compatible]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\user agent[version]
                                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\user agent[version]
  Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet settings[user
agent]
   Queries value:
                                            \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{microsoft} \windows \current version} \end{tabular} \label{thm:local_hammon_hammon}
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:
explorer\\ \verb|main| featurecontrol| feature\_browser\_emulation [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                                                     HKLM\software\wow6432node\microsoft\internet
    Queries value:
explorer\main\featurecontrol\feature_browser_emulation[*]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\\ \verb|main| featurecontrol| feature_maxconnections perserver [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] \\
    Queries value:
                                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
    .
Queries value:
                                                     HKLM\software\wow6432node\microsoft\internet
explorer\\ \verb|main| featurecontrol| feature\_maxconnectionsper1\_0server\\ [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
    Queries value:
                                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
                                                     HKLM\system\currentcontrolset\services\winsock\parameters[transports]
    .
Queries value:
{\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ tcpip6 \verb|\ parameters \verb|\ winsock[mapping]|
                                                     HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
   Oueries value:
                                                     HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
\label{thm:local_equation} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} a winsock [maxsock addrlength] $$ \end{tabular} $$ HKLM \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$$ \end{tabular} $$$ \end{tabular} $$$ \end{ta
   Queries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed elayed acceptance] \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} N in sock [used elayed elay
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
   Queries value:
                                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableutf8]
    Queries value:
                                                     \label{thm:linear} \mbox{HKCU\software\mbox{$\mbox{$m$icrosoft\internet}$ explorer\international[acceptlanguage]} \label{thm:linear}
    Oueries value:
                                                     HKLM\software\wow6432node\microsoft\internet
explorer\\ \verb|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]
    Queries value:
                                                     {\tt HKLM \ } system \verb|\  current control set \verb|\  services \verb|\  winsock \verb|\  setup| \\
migration\providers\tcpip6[winsock 2.0 provider id]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
   Oueries value:
\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constraint of the constr
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[a]ways use tabl
                                                     HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
    Queries value:
                                                     HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
    Queries value:
00c04fd7d062}\inprocserver32[inprocserver32]
                                                     HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
   Oueries value:
00c04fd7d062}\inprocserver32[]
    Queries value:
                                                     HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}[]
    Queries value:
                                                     HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32[inprocserver32]
                                                     HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
    Oueries value:
9fe3c77a297a}\inprocserver32[]
    Queries value:
                                                     HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32[threadingmodel]
                                                     HKCU\software\microsoft\windows\currentversion\explorer\runmru[mrulist]
    Oueries value:
    Queries value:
                                                     HKCU\software\microsoft\windows\currentversion\explorer\runmru[a]
                                                     HKCU\software\microsoft\windows\currentversion\explorer\runmru[d]
    Queries value:
    Queries value:
                                                     HKCU\software\microsoft\windows\currentversion\explorer\runmru[c]
                                                     HKCU\software\microsoft\windows\currentversion\explorer\runmru[b]
    Oueries value:
                                                     HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}[]
    Oueries value:
                                                     HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
    Queries value:
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}[]
                                                     HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                                     HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
   Oueries value:
00c04fd7d062}\inprocserver32[]
    Queries value:
                                                     HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
                                                     HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
   Oueries value:
00aa005b4383}\inprocserver32[]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client[]
                                                     HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]
   Queries value:
    Queries value:
                                                     HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
                                                     HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
    Queries value:
b61bb7cdd997}\inprocserver32[inprocserver32]
                                                     HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
    Queries value:
b61bb7cdd997}\inprocserver32[]
```

HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

Queries value:

b61bb7cdd997}\inprocserver32[threadingmodel] HKLM\software\microsoft\rpc\extensions[ndroleextdll] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Oueries value: HKCU\control panel\desktop[smoothscroll] Queries value: $\label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ explorer \+ advanced \+ [enable balloon tips]$ Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect] Queries value: $\label{like} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{listviews} adow] \end{tabular}$ Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle] $\tt HKLM \colors \colo$ e1e01c1f69b5}[searchlist] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[enabledhcp] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[registrationenabled] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[registeradaptername] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[domain] Queries value: e1e01c1f69b5}[dhcpdomain] Queries value: e1e01c1f69b5}[dhcpv6domain] Oueries value: e1e01c1f69b5}[nameserver] Queries value: e1e01c1f69b5}[nameserver] Queries value: e1e01c1f69b5}[dhcpnameserver] Queries value: 806e6f6e6963}[enabledhcp] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[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: 806e6f6e6963}[dhcpdomain] Queries value: 806e6f6e6963}[nameserver] Queries value: 806e6f6e6963}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Oueries value: Queries value: e1e01c1f69b5}[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[disableadapterdomainname] Queries value: e1e01c1f69b5}[registrationmaxaddresscount] Queries value: e1e01c1f69b5}[maxnumberofaddressestoregister] Oueries value: $\verb|e1e01c1f69b5|| [enable multicast]|$ Queries value:

806e6f6e6963}[queryadaptername]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disableadapterdomainname] Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disabledynamicupdate]

Queries value:

806e6f6e6963}[enableadapterdomainnameregistration] Queries value:

806e6f6e6963}[registrationmaxaddresscount] Oueries value:

806e6f6e6963}[maxnumberofaddressestoregister]

```
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enablemulticast]
                                           HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
   Queries value:
   Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
                                           HKCR\mime\database\content type\text/html[extension]
   Oueries value:
                                           HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer \verb|\main| feature control| feature \_mime\_sniffing [62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe] | the substitution of the substitut
   Queries value:
                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
                                           HKCU\software\microsoft\windows\currentversion\internet
   .
Queries value:
settings[istextplainhonored]
Queries value: HKLM\software\wow6432 node\microsoft\internet explorer\main\feature\_feeds[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
   Oueries value:
                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_feeds[*]
   Queries value:
                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                           HKLM\software\wow6432node\microsoft\internet
   Queries value:
\verb|explorer\main\featurecontrol\feature\_safe\_bindtoobject[*]|
                                           HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
   Queries value:
   Queries value:
                                           HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]
                                           HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[inprocserver32]
                                           HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
   Oueries value:
00aa00686f13}\inprocserver32[]
   Queries value:
                                           HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[threadingmodel]
                                           HKLM\software\wow6432node\microsoft\internet
   Queries value:
Queries value:
                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]

Queries value: HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| feature control \verb|\feature_object_caching[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
   Queries value:
                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]
   .
Queries value:
                                           HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
   Queries value:
                                           91a2-7b624e0e72441
                                           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]
                                           HKCU\software\microsoft\windows
   Queries value:
nt\currentversion\windows[dragscrolldelay]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
                                           HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_restrict_filedownload[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
                                           HKCR\protocols\handler\about[clsid]
HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[]
   Queries value:
   Oueries 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]
   Oueries value:
                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
   Queries value:
                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\3[2106]
   Queries value:
                                           {\tt HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus zoom[zoomdisabled]}
   Queries value:
                                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\url history[daystokeep]
Queries value: HKLM\so
                                           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]
   Oueries value:
   Queries value:
                                           HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
                                           HKCU\software\microsoft\internet explorer\main[anchor underline] HKCU\software\microsoft\internet explorer\main[css_compat]
   Queries value:
   Oueries value:
                                           HKCU\software\microsoft\internet explorer\main[expand alt text]
   Oueries value:
   Queries value:
                                           HKCU\software\microsoft\internet explorer\main[display inline images]
   Queries value:
Queries value:
                                           HKCU\software\microsoft\internet explorer\main[display inline videos]
HKLM\software\wow6432node\microsoft\internet explorer\main[display
inline videos]
   Queries value:
                                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\internet explorer\mbox{\tt main[play\_background\_sounds]}} \\
                                           HKCU\software\microsoft\internet explorer\main[play_animations] HKCU\software\microsoft\internet explorer\main[print_background]
   Oueries value:
   Queries value:
   Queries value:
                                           HKCU\software\microsoft\internet explorer\main[use stylesheets]
   Oueries value:
                                           \label{local-continuous} \mbox{HKCU\software\mbox{$\mbox{$\mbox{microsoft\internet}$ explorer\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox
                                           HKCU\software\microsoft\internet explorer\main[xmlhttp]
HKCU\software\microsoft\internet explorer\main[xmlhttp]
   Queries value:
   Queries value:
   Queries value:
                                           HKCU\software\microsoft\internet explorer\main[disable script debugger]
   Oueries value:
                                           HKCU\software\microsoft\internet explorer\main[move system caret]
   Queries value:
   Queries value:
                                           HKCU\software\microsoft\internet explorer\main[force offscreen
 composition]
                                           HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
   Oueries value:
   Queries value:
                                           HKCU\software\microsoft\internet explorer\main[usethemes]
                                           HKCU\software\microsoft\internet explorer\main[usehr]
   Queries value:
   Queries value:
                                           HKCU\software\microsoft\internet explorer\main[q300829]
```

```
Oueries value:
                                    HKCU\software\microsoft\internet explorer\main[cleanup htcs]
                                    HKCU\software\microsoft\internet explorer\main[xdomainrequest]
  Queries value:
  Queries value:
                                    HKLM\software\wow6432node\microsoft\internet
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:
  Queries value:
                                    HKCU\software\microsoft\internet explorer\settings[anchor color visited]
                                   HKCU\software\microsoft\internet explorer\settings[anchor color hover]
  Oueries value:
  Queries value:
                                    HKCU\software\microsoft\internet explorer\settings[always use my colors]
                                    HKCU\software\microsoft\internet explorer\settings[always use my font
  Queries value:
size]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\settings[always use my font
face]
  Queries value:
                                    HKCU\software\microsoft\internet explorer\settings[disable visited
hyperlinks]
                                   HKCU\software\microsoft\internet explorer\settings[use anchor hover
  Oueries value:
color]
  Queries value:
                                   \label{local-observation} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\sc miscflags]}}
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\policies[allow
programmatic cut_copy_paste]
                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]

Oueries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                                    HKCU\software\microsoft\internet explorer\pagesetup[print_background]
  Queries value:
  Oueries value
                                   HKLM\system\currentcontrolset\control\nls\codepage[950]
                                   HKCU\software\microsoft\internet
  Queries value:
explorer\international\scripts\3[iefontsize]
                                   HKCU\software\microsoft\internet
  Queries value:
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\iefixedfontname1
                                   HKLM\software\wow6432node\microsoft\internet explorer\version
  Queries value:
vector[vml]
  Queries value:
                                    HKLM\software\wow6432node\microsoft\internet explorer\version vector[ie]
  Oueries value:
                                   HKLM\software\wow6432node\microsoft\internet explorer\version
vector[windowsedition]
                                    HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
  Queries value:
explorer \verb|\main| feature control \verb|\feature| zone_elevation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                                   HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_zone_elevation[*]
                                    HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer \verb|\main| featurecontrol| feature_xssfilter[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                                   HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecom
                                   trol\feature_xssfilter[*]
  Queries value:
                                   \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$m$icrosoft \windows \current version \internet} \end{tabular}
settings\zones[securitysafe]
Queries value: HKC
                                    \label{local-equation} \begin{tabular}{ll} HKCU \software \mbox{$^{\circ}$ internet explorer $$ main[no protected mode banner]$ \end{tabular}
                                    HKLM\software\wow6432node\microsoft\internet explorer\low
  Queries value:
\verb|rights[protected mode off for all zones]|\\
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[icon]
  Queries value:
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\0[minlevel]
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
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 model in the context of 
settings\zones\1[minlevel]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\1[recomm
                                   ndedlevel]
  Queries value:
                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ 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]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[icon]
  Queries value:
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\2[minlevel]
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
                                   ndedlevel]
settings\zones\2[recomm
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
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]
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\3[minlevel]
                                    Queries value:
settings\zones\3[recomm
                                   ndedlevel1
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\3[currentlevel]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2500]
  Queries value:
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
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 model in the context of 
settings\zones\4[recomm
                                                         ndedlevel1
                                                          HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\4[currentlevel]
   Queries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[2500]
                                                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} Software \end{tabular} wow 6432 node \end{tabular} in terms to the local property of the loc
   Queries value:
settings\zones\4[2500]
   Queries value:
                                                          HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
explorer\main\featurecontrol\feature mshtml autoload ieframe[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
                                                          HKLM\software\wow6432node\microsoft\internet
    Queries value:
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[*]
   Queries value:
                                                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} on the constraint \end{tabular} in the constraint \end{tabular} on the constraint \end{tabular
settings[cointernetcombineiuricachesize]
    Oueries value
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
   Queries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
                                                          HKLM\software\wo
    Queries value:
                                                                                                   /6432node\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
   Queries value:
                                                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
    Queries value:
                                                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[*]
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[securityidiuricachesize]
    Queries value:
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
   Queries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
                                                          HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| windows \verb|\currentversion\\| internet model in the context of 
    Queries value:
settings[securityidiuricachesize]
                                                          HKLM\software\wow6432node\microsoft\internet
   Queries value:
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:
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
   Queries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
    Queries value:
                                                          HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[]
    Oueries value:
                                                          HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                                                          HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
    Queries value:
f4ceaaf59cfc}\inprocserver32[]
                                                          HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
   Oueries value:
 f4ceaaf59cfc}\inprocser
                                                        ver32[threadingmodel]
    Queries value:
                                                          HKCR \ wow 6432 node \ clsid \ \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \ progid[]
    Queries value:
                                                          HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[]
                                                          HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
    Queries value:
00aa00bbbb58}\inprocserver32[inprocserver32]
    Queries value:
                                                          HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[1
                                                          HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
    Queries value:
00aa00bbbb58}\inprocserver32[threadingmodel]
    Queries value:
                                                          HKLM \setminus software \setminus microsoft \setminus ole \setminus appcompat[raise default authnlevel]
    Queries value:
                                                          HKLM\software\microsoft\ole[defau]taccesspermission]
                                                          HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
    Queries value:
    Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
    Queries value:
provider[image path]
   Queries value:
                                                          HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
    Queries value:
                                                          Oueries value:
                                                          HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
                                                          HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
    Queries value:
HKLM \verb|\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]|
                                                          HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
    Oueries value:
                                                          HKLM\software\microsoft\cryptography[machineguid]
    Oueries value:
                                                          HKCR\wow6432node\interface\{00000134-0000-0000-c000-
    Queries value
00000000046}\proxystubclsid32[]
                                                          HKLM\software\microsoft\rpc\extensions[remoterpcdll]
    Oueries value:
                                                          HKCU\software\microsoft\internet explorer\recovery[autorecover]
    Oueries value:
                                                          HKLM \setminus software \setminus wow 6432 node \setminus internet
    Queries value:
explorer\\ \verb|main| featurecontrol| feature\_block\_lmz\_img[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
    Queries value:
                                                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[*]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecom
                                                         trol\feature_behaviors[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
    Oueries value:
                                                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature behaviors[*]
    Queries value:
                                                          HKLM\software\wow6432node\microsoft\internet explorer\default
behaviors[homepage]
    Queries value:
                                                          HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid[]
                                                          HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[]
    Queries value:
    Queries value:
                                                          HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocser
                                                         er32[inprocserver32]
                                                          HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
   Oueries value:
00aa00bdce0b}\inprocserver32[]
                                                          HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
```

```
Oueries value:
                                                                                                                          HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid[]
                                                                                                                          HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[]
        Queries value:
                                                                                                                          HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
        Queries value:
 dc030521aabd}\inpr
                                                                                                                          er32[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}\inprocsery
                                                                                                                       er32[inprocserver32]
       Queries value:
                                                                                                                         HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32[]
                                                                                                                         HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
        Queries value
3c8b00c10000}\inprocserver32[threadingmodel]
       Queries value:
                                                                                                                         HKLM\software\wow6432node\microsoft\internet explorer\default
behaviors[dxtfilterbehavior]
                                                                                                                         HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[]
        Oueries value:
                                                                                                                          HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
        Queries value
00c04fd9189d}\inprocserver32[inprocserver32]
                                                                                                                         HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
       Oueries value:
00c04fd9189d}\inprocserver32[]
        Queries value
                                                                                                                         HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[threadingmodel]
   Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
         Queries value:
                                                                                                                          HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
        Oueries value:
                                                                                                                          {\tt HKLM} \verb|\hardware\\ \verb|\devicemap\\ \verb|\video[maxobjectnumber]|
                                                                                                                         HKLM\hardware\devicemap\video[\device\video3]
        Oueries value:
                                                                                                                          HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-
        Queries value:
  1e1a187c13e9}\0000[pruningmode]
        Oueries value:
                                                                                                                          HKLM\hardware\devicemap\video[\device\video0]
                                                                                                                         HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
        Queries value:
 9dd4432fa2e9}\0000[pruningmode]
                                                                                                                           HKLM\hardware\devicemap\video[\device\video1]
        Queries value:
        Oueries value
                                                                                                                         HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[pruningmode]
        Queries value:
                                                                                                                          HKLM\hardware\devicemap\video[\device\video2]
        Queries value:
                                                                                                                         8ed0c8eb59a8}\0000[pruningmode]
                                                                                                                          HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![name]
        Queries value:
         Queries value:
                                                                                                                          Queries value:
        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} LKLM \label{limits} HKLM \label{limits} White \label{limits} White \label{limits} HKLM \label{limits} White \label{limits} White \label{limits} White \label{limits} White \label{limits} White \label{limits} HKLM \label{limits} White \label
        Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[name]
       Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[flags]
        Queries value:
                                                                                                                         HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus direct draw \setminus compatibility \setminus diablo[id]
        Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[name]
HKLM \label{limit} \label{limit} HKLM \label{limit} HKLM \label{limit} Wow 6432 node \mbox{$\mathbb{N}$ irrors of the compatibility \mbox{$\mathbb{N}$ irrors of the compa
       Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} software \wow 6432 node \end{tabular} node \aligned \begin{tabular}{ll} high \end{tabular} id] \\ \end{tabular}
        Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[name]
       Queries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \software \wow 6432 node \microsoft \direct draw \compatibility \mbox{$M$ software} \end{tabular} \begin{tabular}{ll} HKLM \software \wow 6432 node \microsoft \direct draw \compatibility \mbox{$M$ software} \end{tabular} \begin{tabular}{ll} HKLM \software \wow 6432 node \microsoft \direct draw \compatibility \mbox{$M$ software} \end{tabular} \begin{tabular}{ll} HKLM \software \wow 6432 node \microsoft \direct draw \compatibility \mbox{$M$ software} \end{tabular} \begin{tabular}{ll} HKLM \software \wow 6432 node \microsoft \mbox{$M$ software} \mbox{$M$ software}
        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] |
        Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[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:
Queries value:
HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} If the limits of the lim
        Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[id]
                                                                                                                          HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
        Queries value:
 squadron[name]
       Queries value:
                                                                                                                          HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
 squadron[flags]
        Oueries value
                                                                                                                          HKLM\software\wow6432node\microsoft\directdraw\compatibilitv\rogue
 squadron[id]
        Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[name]
         Queries value:
\label{local-observation} HKLM \label{local-observation} IKLM \label{local-observation} HKLM \label{local-observation} Software \label{local-observation} Which is a substitution of the local content of the local conte
        Oueries value:
                                                                                                                         HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[id]
        Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[name]
        Oueries value:
HKLM \verb|\software| \verb|\wow6432| node| \verb|\microsoft| directdraw| compatibility| \verb|\scorchedplanet| [flags]| \\
        Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[id]
        Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[name]
        Queries value:
HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} If the limits of the lim
       Oueries value:
HKLM \label{limits} \label{limits} HKLM \label{limits} KLM \label{limits} Software \label{limits} Wow 6432 node \label{limits} wow 6432 node \label{limits} \label{limits} Wow 6432 node \label{limits} \label{limits} \label{limits} HKLM \label{limits} \label{limits} Software \label{limits} \label{limits} Wow 6432 node \label{limits} \label{limits} \label{limits} Wow 6432 node \label{limits} \label{limits} \label{limits} \label{limits} \label{limits} Wow 6432 node \label{limits} \label{limits} \label{limits} Wow 6432 node \label{limits} \label{limits} \label{limits} \label{limits} \label{limits} \label{limits} \label{limits} \label{limits} Wow 6432 node \label{limits} \labell{limits} \labell{limits} \labell{limits} \labell{limits} \lab
HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} If the limit \label{limit} If the \labell{limit} If the \labell{limit}
```

```
Oueries value
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[flags]
  Queries value:
                       w6432node\microsoft\directdraw\compatibility\starcraft100[id]
HKLM\software\v
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[name]
  Queries value:
Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[id]
HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| direct draw\\| compatibility\\| starcraft demo[name]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[flags]
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[id]
  Oueries value:
HKLM \label{limit} \begin{tabular}{ll} HKLM \label{limit} Wow6432 node \microsoft \directdraw \compatibility \terracide[name] \end{tabular}
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide[flags]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide[id]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[name]
  Oueries value:
HKLM \ software \ \ wow 6432 node \ \ \ icrosoft \ \ \ directdraw \ \ compatibility \ \ third dimension [flags]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[id]
  Queries value:
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:
                        6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
HKLM\software\v
  Oueries value
Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ direct draw \ compatibility \ viff daviswin mark benchmark \ [flags]
  Oueries value:
HKLM \label{limit} MkLM \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} Software \label{limit} \label{limit} White \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} HKLM \label{limit} \label{limit} HKLM \label{limi
  Queries value:
                                   HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus directdraw [modexonly]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\directdraw[emulationonly]
  Oueries value:
                                   HKLM\software\wow6432node\microsoft\directdraw[showframerate]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\directdraw[enableprintscreen]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\directdraw[forceagpsupport]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\directdraw[disableagpsupport]
                                   HKLM\software\wow6432node\microsoft\directdraw[disablemmx]
  Oueries value:
  Oueries value:
                                   HKLM\software\wow6432node\microsoft\directdraw[disableddscapsinddsd]
                                   HKLM\software\wow6432node\microsoft\directdraw[disablewidersurfaces]
  Queries value:
  Queries value:
                                   HKLM\software\wow6432node\microsoft\directdraw[usenonlocalvidmem]
                                   HKLM\software\wow6432node\microsoft\directdraw[forcerefreshrate]
  Oueries value:
                                   HKLM\software\wow6432node\microsoft\direct3d[flipnovsync]
  Oueries value:
  Queries value:
                                  HKLM\software\wow6432node\microsoft\directdraw[owndc]
                                   HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid[]
  Oueries value:
                                   HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[]
  Queries value:
                                   HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
  Queries value
f941e9b7e1fe}\inprocserver32[inprocserver32]
                                  HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
  Queries value:
f941e9b7e1fe}\inprocserver32[]
                                  HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
  Queries value:
f941e9b7e1fe}\inprocserver32[threadingmodel]
  Oueries value:
                                  HKCR\dximagetransform.microsoft.shadow\clsid[]
  Queries value:
                                   HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid[]
  Queries value:
                                   HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}[]
  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 \setminus wow6432 \\ node \\ clsid \\ \{4cb26c03-ff93-11d0-817e-0000f87557db\}[]
  Queries value:
                                  HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[inprocserver32]
                                  HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
  Queries value:
0000f87557db}\inprocserver32[]
  Queries value:
                                  HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[threadingmodel]
  Queries value:
                                   HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid[]
                                   HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}[]
  Queries value:
  Queries value:
                                  HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[inprocserver32]
                                  HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Oueries value:
f4fc1e6ca1bd}\inprocserver32[]
                                  HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Oueries value:
f4fc1e6ca1bd}\inprocserver32[threadingmodel]
                                   HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]
  Queries value:
  Queries value:
                                  HKCR\mime\database\content type\image/png[extension]
HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]
  Oueries value:
  Queries value:
                                   HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid[]
  Queries value:
                                   HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[]
  Oueries value:
                                  HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
                                   HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
  Queries value:
00aa006c1a01}\inprocserver32[]
  Oueries value:
                                  HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
  Queries value:
                                   HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[]
                                   HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
  Queries value:
00aa003f8646}\inprocserver32[inprocserver32]
                                  HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
  Queries value:
00aa003f8646}\inprocserver32[]
  Queries value:
                                  HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
```

```
HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid[]
   Queries value:
   Queries value:
                                              HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[]
                                              HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
   Queries value
00aa006c1a01}\inprocserver32[inprocserver32]
                                             HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
   Queries value:
00aa006c1a01}\inprocserver32[]
   Queries value:
                                             HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
                                             HKCR\mime\database\content type\image/bmp\bits[0]
   Queries value:
                                              HKCR\mime\database\content type\image/gif\bits[0]
   Queries value
   Queries value:
                                              HKCR\mime\database\content type\image/jpeg\bits[0]
                                             HKCR\mime\database\content type\image/pjpeg\bits[0] HKCR\mime\database\content type\image/png\bits[0]
   Oueries value:
   Queries value:
                                              HKCR\mime\database\content type\image/x-png\bits[0]
   Queries value:
   Queries value:
                                              \label{localization} HKCR\mbox{\sc mime} \mbox{\sc database} \mbox{\sc content type} \mbox{\sc image/$x-wmf} \mbox{\sc bits} \mbox{\sc bits} \mbox{\sc ontent} \mbox{\sc ont
                                             Oueries value:
   Oueries value:
                                              HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[]
   Queries value:
   Queries value:
                                             HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[inprocserver32]
                                              HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
   Queries value
00a0c913f750}\inprocserver32[]
                                             HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
   Oueries value:
00a0c913f750}\inprocserver32[threadingmodel]
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\codepage[1250]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\nls\codepage[1253]
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\codepage[1254]
   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:
                                              HKLM\system\currentcontrolset\control\nls\codepage[874]
   Queries value:
                                             HKLM\system\currentcontrolset\control\nls\codepage[932] HKLM\system\currentcontrolset\control\nls\codepage[936]
   Oueries value
   Queries value:
                                              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]
                                              HKCU\software\microsoft\internet
   Queries value:
explorer\international\scripts\26[iefontsizeprivate]
   Oueries value:
                                             HKCU\software\microsoft\internet
explorer\international\scripts\26[iepropfontname]
   Queries value:
                                              HKCU\software\microsoft\internet
{\tt explorer} \verb|\international\scripts\26[iefixed fontname]|\\
                                             HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane1]
                                              HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane2]|
                                             HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane3]
                                              HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane4]
Queries value: HKLM\software\microsoft\windows
\verb|nt\currentversion| language pack \verb|surrogatefallback \verb|simsun[plane5]| \\
   Queries value:
                                             HKLM\software\microsoft\windows
\label{local-problem} $$ nt`currentversion\anguagepack\surrogatefallback\simsun[plane6] $$ Queries value: $$ HKLM\software\microsoft\windows $$ $$
\verb| ``times | current version \verb| language pack \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| language pack \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| language pack \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| language pack \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| language pack \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| language pack \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| language pack \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| language pack \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| surrogate fall back \verb| simsun[plane 7]| | current version \verb| surrogate fall back \verb| surrogate 
  Oueries value:
                                             HKLM\software\microsoft\window
nt\currentversion\languagepack\surrogatefallback\simsun[plane8]
                                              HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane9]
   Oueries value
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane10]
   Queries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane11]
  Oueries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane12]
                                              HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane13]|
                                             HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane14]
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane15]|
                                             HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane16]
                                              HKCU\software\microsoft\windows script\settings[jitdebug]
   Queries value:
   Queries value:
                                              HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c
00aa00389b71}\proxystubclsid32[]
   Oueries value:
                                              HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-
00c04fd90119}\proxystubclsid32[]
   Queries value:
                                              HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}[]
   Queries value:
                                              HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
   Queries value:
                                             HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[]
  Queries value:
                                             HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocse
                                             er32[threadingmodel]
   Queries value:
                                              {\tt HKCR} \verb|\mime| database \verb|\content| type \verb|\image/gif[extension]| \\
                                              HKLM\software\wow6432node\microsoft\direct3d[disab]emmx]
   Oueries value:
   Queries value:
                                              HKLM\software\wow6432node\microsoft\direct3d[disablex3d]
                                              HKLM\software\wow6432node\microsoft\direct3d[fewvertices]
   Queries value:
   Oueries value:
                                              HKLM\software\wow6432node\microsoft\direct3d[disablevidmemvbs]
                                             HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\\ \verb|main| featurecontrol| feature\_block\_lmz\_script[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
                                             HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_block_lmz_script[*]
                                             HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\\ \verb|main| featurecontrol| feature\_use\_windowedselectcontrol[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
   Queries value:
                                             HKLM\software\wow6432node\microsoft\internet
```

00aa003f8646}\inprocserver32[threadingmodel]

```
explorer\main\featurecontrol\feature use windowedselectcontrol[*1
                          HKCU\software\microsoft\internet explorer\new
 Queries value:
windows[accuserinitonclick]
 Queries value:
                          HKCR\shockwaveflash.shockwaveflash\clsid[]
                          HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid[]
  Oueries value:
                          HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}[]
 Queries value:
                          HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
  Queries value:
444553540000}\inprocserver32[inprocserver32]
                          HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
 Oueries value:
444553540000}\inprocserver32[]
                          HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32[threadingmodel]
                          HKLM\system\currentcontrolset\control\wmi\security[12e1ddac-7ebb-434f-
 Oueries value:
bc58-54c27d745f8f]
 Queries value
                          HKLM\system\currentcontrolset\control\wmi\security[d53270e3-c8cf-4707-
958a-dad20c90073c1
 Oueries value:
                          HKLM\hardware\description\svstem\centralprocessor\0[~mhz]
  Oueries value
                          HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001[name]
 Queries value:
                          HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32[]
                          HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[]
  Oueries value:
                          HKLM\software\wow6432node\microsoft\internet explorer\default
  Queries value:
behaviors[userdata]
 Oueries value:
                          HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
  Queries value:
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c
00c04fb6bfc4}\inprocserv
                         er32[inprocserver32]
 Queries value:
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[]
  Queries value:
                          HKCR\w
                                  ow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[2000]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet explorer\feed
discovery[sound]
                          HKCU\software\microsoft\ftp[use web based ftp]
 Queries value:
  Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol \verb|\feature_activex_repurposedetection[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
 Oueries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection[*]
                          HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer \\ \verb|main| feature \\ control \\ \verb|feature_addon_management[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
 Oueries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_addon_management[*]
  Queries value:
                          HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8
444553540000}\miscstatus\1[]
                          HKLM\software\wow6432node\microsoft\windows\tablet pc[istabletpc]
 Oueries value:
  Queries value:
                          HKCR\mime\database\content type\application/x-shockwave-flash[extension]
                          HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid[]
  Queries value:
 Queries value:
                          HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}[]
                          HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
 Oueries value:
00c04f983e60}\inprocser
                         er32[inprocserver32]
 Queries value:
                          HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[]
                          HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-
 Queries value:
00c04f983e60}\inprocserver32[threadingmodel]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1606]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings \verb|\5.0| cache \verb|\extensible| cache \verb|\userdata[cacherepair]|
 Oueries value
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\userdata[cacheprefix]
 Oueries value
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachelimit]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache\extensible cache\userdata[cacheoptions]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave]
                          HKLM\software\wow6432node\microsoft\windows
 Queries value:
nt\currentversion\drivers32[wave1]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave2]
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave3]
                          HKLM\software\wow6432node\microsoft\windows
 Oueries value:
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]
                          HKLM\software\wow6432node\microsoft\windows
 Queries value:
nt\currentversion\drivers32[wave71
                          HKLM\software\wow6432node\microsoft\windows
 Queries value:
nt\currentversion\drivers32[wave8]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave9]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi1]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi2]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi3]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi4]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi5]
                          HKLM\software\wow6432node\microsoft\windows
```

nt\currentversion\drivers32[midi6]

```
Oueries value:
                                                                      HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi7]
     Queries value:
                                                                      HKLM\software\wow6432node\microsoft\windows
                                                                     s32[midi8]
 nt\currentversion\drive
     Oueries value:
                                                                      HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi9]
     Queries value:
Oueries value:
HKLM \label{limits} \label{limits} HKLM \label{limits} Which is a substitution of the limits of th
     Queries value:
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]
                                                                       HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
     Queries value:
     Queries value:
                                                                      HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
                                                                      HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
     Oueries value:
      Queries value:
\label{lem:hklm} \verb+Kklm/system/currentcontrolset/control/lsa/sspicache/credssp.dll[tokensize]+ \\
     Oueries value:
 HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlockcount]
\label{lem:hklm} \verb+Kklm \+ system \+ current control \+ security providers \+ schannel \+ [user context list count]
     Oueries value:
                                                                      HKCU\software\microsoft\internet explorer\domstorage\total[]
                                                                       HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
      Queries value:
      Queries value:
                                                                       HKCU\software\microsoft\internet
 explorer\services[selectionactivitybuttondisable]
                                                                      HKCU\software\microsoft\internet explorer\suggested sites[enabled]
     Queries value:
      Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constraint of the constrain
     Oueries value:
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Queries value:
08002b30309d \} \verb|\shellfolder[callforattributes]|
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
                                                                      Queries value:
08002b30309d}\shellfolder[wantsfordisplay]
     Oueries value:
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 08002b30309d}\shellfolder[hidefolderverbs]
     Queries value:
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
     Oueries value:
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Queries value:
08002b30309d \verb|\shellfolder[wantsparsedisplayname]|
                                                                      HKCU\software\macromedia\flashplayer[flashplayerversion]
     Oueries value:
                                                                       HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]
      Oueries value:
     Queries value:
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d \} \verb|\shellfolder[mapnetdriveverbs]|
     Queries value
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
                                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Queries value:
08002b30309d}\shellfolder[hideinwebview]
     Oueries value
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideondesktopperuser]
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Queries value:
08002b30309d \} \verb|\shellfolder[wantsaliased notifications]|
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Oueries value
08002b30309d}\shellfolder[wantsuniversaldelegate]
     Queries value:
                                                                      HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32[]
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Oueries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
                                                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Oueries value:
 08002b30309d}\shellfolder[hasnavigationenum]
     Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4060-a2d8-4069-a2d8-4069-a2d8
08002b30309d}1
     Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{8063a3d4-8213-42444, and a substitution \ and \ and
 11e3-a68e-806e6f6e6963}[data]
     Oueries value:
                                                                      HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
 0080c7f4ee85}\typelib[]
                                                                      HKCR \verb+\wow6432+ node \verb+\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-4d95-960c-4d95-960c-4d95-960c-4d95-960c-4d95-960c-4d95-960c-4d95-960c-4d95-960c-4d95-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c
     Queries value:
0080c7f4ee85}\typelib[version]
     Queries value:
 11e3-a68e-806e6f6e6963}[generation]
     Queries value:
11e3-a68e-806e6f6e6963}[data]
     Oueries value:
11e3-a68e-806e6f6e6963}[generation]
                                                                       HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
     Queries value:
     Oueries value:
                                                                      HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
 409d6c4515e9}[drivemask]
     Queries value:
                                                                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\[]
                                                                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
      Queries value:
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                                                      HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
     Queries value:
 b8dc300d9f9d}\inprocserver32[]
     Queries value:
                                                                      HKLM\software\microsoft\rpc[udtalignmentpolicy]
```

```
Oueries value:
                                              HKCR\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32[]
   Queries value:
                                              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
                                              HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Queries value:
   Queries value:
                                              HKCR\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}[]
                                              HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
   Oueries value:
00000000046}\inprocserver32[inprocserver32]
                                              HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
   Queries value:
000000000046}\inprocserver32[]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
HKLM \label{lem:hklm} LKLM \label{lkklm} HKLM \label{lkklm} If the last constant \label{lkklm} HKLM \label{lkklm} If the last \label{lkklm} LKLM \label{lkklm} If the last \label{lkklm} If the last \label{lkklm} If the last \label{lkklm} If the last \label{lkklm} LKLM \label{lkklm} If the last \label{lkklm} If the last \label{lkklm} If the last \label{lkklm} If the lkklm \labell \label{lkklm} If the lkklm \labell \labell{lkklm} If the lkklm \labell{lkklm} If the lkklm \labell \labell \labell \labell \
                                              HKCR\wow6432node\clsid\{00020420-0000-0000-c000
  Oueries value:
00000000046}\inprocserver32[threadingmodel]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Oueries value:
\label{local_equation} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced[hidefileext]$} \end{tabular}
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
  Queries value:
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
   Queries value:
                                              HKCR\directory[docobject]
   Oueries value:
                                              HKCR\folder[docobject]
                                              HKCR\allfilesystemobjects[docobject]
   Queries value:
                                              HKCR\directory[browseinplace]
   Queries value:
   Queries value:
                                              HKCR\folder[browseinplace]
                                              HKCR\allfilesvstemobjects[browseinplace]
   Oueries value:
                                              HKCR\directory[isshortcut]
   Queries value:
                                              HKCR\folder[isshortcut]
   Queries value:
   Oueries value:
                                              {\tt HKCR} \verb|\| all file system objects[is short cut] \\
                                              HKCR\directory[alwaysshowext]
   Oueries value:
                                              HKCR\directory[nevershowext]
   Queries value:
   Queries value:
                                              HKCR\folder[nevershowext]
                                              HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-
   Oueries value:
00aa006009fa}\proxystubclsid32[]
   Queries value:
                                              HKCR\allfilesystemobjects[nevershowext]
   Queries value:
                                              HKCR \setminus wow 6432 \\ node \\ clsid \\ \{a4a1a128-768f-41e0-bf75-e4fddd701cba\}[]
                                              HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
   Oueries value:
e4fddd701cba}\inprocserver32[inprocserver32]
                                              HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
   Queries value:
444553540000}\inprocserver32[]
                                              HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
  Oueries value:
444553540000}\inprocserver32[loadwithoutcom]
                                              HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
   Queries value:
e4fddd701cba}\inprocserver32[]
                                              HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
  Oueries value:
e4fddd701cba}\inprocserver32[threadingmodel]
                                              HKCU\software\microsoft\windows\currentversion\shell
   Queries value:
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {000214e6-0000-0000-c000-000000000046}
0xffff1
                                              HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[]
   Queries value
   Queries value:
                                              HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[inprocserver32]
                                              HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
  Queries value:
444553540000}\inprocserver32[threadingmodel]
   Queries value:
                                              HKCR\wow6432node\interface\{00020404-0000-0000-c000-
00000000046}\proxystubclsid32[]
   Queries value:
                                              HKCR\wow6432node\clsid\{00020421-0000-0000-c000-00000000046}[]
   Queries value:
                                              HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                                              HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
  Oueries value:
000000000046}\inprocserver32[]
                                              HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
   Queries value
 000000000046 \} \\ inprocserver 32 [threading model] \\ Queries value: HKCU \\ software \\ microsoft \\ windows \\ current version \\ internet \\
settings\5.0\cache\extensible cache\mshist012016040820160409[cacherepair]
  Queries value:
                                              \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
settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012016040820160409[ cachepath]|
                                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheprefix]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\5.0\cache\extensible cache\mshist012016040820160409[cachelimit]
                                                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheoptions]
                                                                                   HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (20d04fe0-d1) = (20d04fe0-d1) + (20d04fe0-d1) = (20d04fe0-d1) + (20d04fe0-d1) = (20d04fe0-d1) + (20d04fe0-d1) = (20d04f
      Queries value:
3aea-1069-a2d8-08002b30309d}[1
                                                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Queries value:
08002b30309d}[localizedstring]
      Queries value:
                                                                                   HKCU\software\microsoft\internet
explorer\main\windowssearch[enabledscopes]
      Queries value:
68ad-4d8a-87bd-30b759fa33dd}[category]
     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}[name]
     Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
68ad-4d8a-87bd-30b759fa33dd}[parentfolder]
      Queries value:
68ad-4d8a-87bd-30b759fa33dd}[description]
HKLM \label{lem:hklm} Software \label{lem:hklm} Which is a few and the latest a
68ad-4d8a-87bd-30b759fa33dd}[relativepath]
     Oueries value:
68ad-4d8a-87bd-30b759fa33dd\} \hbox{\tt [parsing name]}
     Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[infotip]
      Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[localizedname]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
68ad-4d8a-87bd-30b759fa33dd}[icon]
      Queries value:
68ad-4d8a-87bd-30b759fa33dd}[security]
      Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[streamresource]
     Oueries value:
HK LM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1777f761-market \ market 
68ad-4d8a-87bd-30b759fa33dd}[streamresourcetype]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
68ad-4d8a-87bd-30b759fa33dd}[localredirectonlv]
68ad-4d8a-87bd-30b759fa33dd}[roamable]
HKLM \label{lem:hklm} Software \label{lem:hklm} Which is a few and the latest a
68ad-4d8a-87bd-30b759fa33dd}[precreate]
     Queries value:
68ad-4d8a-87bd-30b759fa33dd}[stream]
     Queries value:
68ad-4d8a-87bd-30b759fa33dd}[publishexpandedpath]
      Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
68ad-4d8a-87bd-30b759fa33dd}[attributes]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
68ad-4d8a-87bd-30b759fa33dd}[foldertypeid]
      Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1777f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f761-177f7
68ad-4d8a-87bd-30b759fa33dd}[initfolderhandler]
                                                                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
      Queries value:
 folders[favorites]
      Queries value:
                                                                                   HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus windows \ search[current version]
      Oueries value:
                                                                                    HKLM\software\wow6432node\microsoft\downloadmanager[cacheok]
                                                                                    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[]
      Queries value:
                                                                                   HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32[threadingmodel]
                                                                                    HKCR\shockwaveflash.shockwaveflash.7\clsid[]
      Oueries value:
                                                                                   HKCR\mime\database\content type\image/x-icon[extension]
      Queries value:
      Queries value:
                                                                                   HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}[]
      Queries value:
                                                                                   HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
 fd2b31b3eefd}\inprocserver32[inprocserver32]
      Queries value:
                                                                                   HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[]
      Queries value:
                                                                                   HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocser
                                                                                 ver32[threadingmodel]
     Sets/Creates value:
                                                                                   HKLM\software\wow6432node\microsoft\internet
explorer\\ \verb|main| featurecontrol| feature\_scripturl\_mitigation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]|
      Sets/Creates value:
                                                                                    HKLM\software\wow6432node\microsoft\tracing\rasapi32[enablefiletracing]
      Sets/Creates value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus rasapi 32 [enable consolet racing]
                                                                                   HKLM\software\wow6432node\microsoft\tracing\rasapi32[filetracingmask]
      Sets/Creates value:
      Sets/Creates value:
                                                                                    HKLM\software\wow6432node\microsoft\tracing\rasapi32[consoletracingmask]
      Sets/Creates value:
                                                                                    HKLM \label{lem:hklm} In the last of the
      Sets/Creates value:
                                                                                   HKLM\software\wow6432node\microsoft\tracing\rasapi32[filedirectory]
                                                                                    HKLM\software\wow6432node\microsoft\tracing\rasmancs[enablefiletracing]
      Sets/Creates value:
```

HKLM\software\wow6432node\microsoft\tracing\rasmancs[enableconsoletracing]

 $HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| tracing \verb|\rasmancs[filetracing mask]|$ Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[consoletracingmask] Sets/Creates value: Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[maxfilesize] Sets/Creates value: $HKLM \label{lem:hklm} \begin{tabular}{ll} HKLM \label{lem:hklm} software \wow6432 node \microsoft \tracing \rasmancs [filedirectory] \end{tabular}$ Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\userdata[cachepath] HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\5.0\cache\extensible cache\userdata[cacheprefix] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\userdata[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\5.0\cache\extensible cache\userdata[cacheoptions] HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\5.0\cache\e sible cache\userdata[cacherepair] Sets/Creates value: HKCU\software\microsoft\internet explorer\domstorage\baidu.com[] HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: 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: $settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012016040820160409[cache options]|$ Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016040820160409[cacherepair] Value changes: HKCU\software\microsoft\internet explorer\main[disable script debugger] Value changes: $\label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ internet$ settings\zonemap[uncasintranet] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable] Value changes: $\label{thm:local_HKCU} \begin{tabular}{ll} HKCU \software \mbox{\mathbb{N} internet} \end{tabular}$ settings\connections[savedlegacysettings] Value changes: HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication[name] HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication[id] Value changes: Value changes:

HKCU\software\microsoft\windows\currentversion\internet

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

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

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