Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3333, Task ID: 842

Task ID: 842 Risk Level: 10

Date Processed: 2016-05-18 10:45:11 (UTC)

Processing Time: 62.91 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\752d6fe81122349daf998a56f48e0b38.exe'

Sample ID: 3333 Type: basic Owner: admin

Label: 752d6fe81122349daf998a56f48e0b38 Date Added: 2016-05-18 10:30:52 (UTC)

File Type: PE32:win32:gui
File Size: 827904 bytes

MD5: 752d6fe81122349daf998a56f48e0b38

SHA256: e36aa66b3e7928b47f8c4beb0ab46a2e886f9f87ca6de7cf7fd05d8f5457b020

Description: None

Pattern Matching Results

6 Modifies registry autorun entries

3 Connects to local host

5 PE: Contains compressed section

10 Creates malicious events: Kelihos trojan 2 [Spam]

5 Adds autostart object

Static Events

Anomaly: PE: No DOS stub

Process/Thread Events

Creates process: C:\windows\temp\752d6fe81122349daf998a56f48e0b38.exe

["C:\windows\temp\752d6fe81122349daf998a56f48e0b38.exe"]

Loads service: ProtectedStorage [C:\Windows\system32\lsass.exe]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED
Creates event: \BaseNamedObjects\Svcctr1StartEvent_A3752DX
Creates event: \BaseNamedObjects\PS_SERVICE_STARTED

File System Events

 Creates:
 C:\Windows\Temp\tmp.exe

 Opens:
 C:\Windows\Prefetch\752D6FE81122349DAF998A56F48E0-CFEA67D2.pf

Opens: C:\Windows

 Opens:
 C:\Windows\System32\wow64.dll

 Opens:
 C:\Windows\System32\wow64win.dll

 Opens:
 C:\Windows\System32\wow64cpu.dll

 Opens:
 C:\Windows\system32\wow64log.dll

 Opens:
 C:\Windows\Sys\WOW64

Opens: C:\windows\temp\COMCAT.dll
Opens: C:\windows\sysWOW64\comcat.dll
Opens: C:\windows\temp\WMDMPS.dll
Opens: C:\windows\sysWOW64\wmdmps.dll
Opens: C:\windows\sysWOW64\sechost.dll
Opens: C:\windows\sysWOW64\temp\delta

Opens: C:\Windows\Temp\752d6fe81122349daf998a56f48e0b38.exe

Opens: C:\windows\temp\DNSAPI.dll C:\Windows\SysWOW64\dnsapi.dll Opens: Opens: C:\windows\temp\IPHLPAPI.DLL C:\Windows\SysWOW64\IPHLPAPI.DLL Opens: C:\windows\temp\WINNSI.DLL Opens: Opens: C:\Windows\SysWOW64\winnsi.dll Opens: C:\windows\temp\MSWSOCK.dll C:\Windows\SysWOW64\mswsock.dll Opens:

Opens: C:\Windows\Globalization\SortIng\SortDefault.nls

Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL

Opens: C:\Windows\Temp

Opens: C:\Windows\Temp\tmp.exe

Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui

Opens: C:\Windows\System32\C_1256.NLS Opens: C:\Windows\System32\C_1251.NLS Opens: C:\Windows\System32\C_950.NLS Opens: C:\Windows\System32\C_1250.NLS Opens: C:\Windows\System32\C_1253.NLS Opens: C:\Windows\System32\C_1255.NLS C:\Windows\System32\C_932.NLS Opens: C:\Windows\System32\C_949.NLS Opens:

Opens: C:\dev\urandom

 Opens:
 C:\windows\temp\dhcpcsvc.DLL

 Opens:
 C:\Windows\SysWOW64\dhcpcsvc.dll

 Opens:
 C:\windows\temp\wpcap.dll

 Opens:
 C:\Windows\SysWOW64\wpcap.dll

```
C:\Windows\system\wpcap.dll
  Opens:
 Opens:
                         C:\Windows\wpcap.dll
 Opens:
                         C:\Windows\SysWOW64\Wbem\wpcap.dll
 Opens:
                         C:\Windows\SysWOW64\WindowsPowerShell\v1.0\wpcap.dll
 Opens:
                         C:\
                         C:\$Recycle.Bin
 Opens:
                         C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001
 Opens:
 Opens:
                         C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Roaming
                         C:\Users\Admin\AppData\Roaming\FlashFXP\3\Sites.dat
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\FlashFXP\3\Quick.dat
 Opens:
                         C:\Users\Admin\AppData\Roaming\FlashFXP\3\History.dat
                         C:\Users\Admin\AppData\Roaming\FlashFXP\4\Sites.dat
 Opens:
                         C:\Users\Admin\AppData\Roaming\FlashFXP\4\Quick.dat
 Opens:
                         C: \verb|\USers\Admin\AppData\Roaming\FlashFXP\A\History.dat|
 Opens:
 Opens:
                         C:\Documents and Settings\
 Opens:
                         C:\dump.pcap
 Opens:
                         C:\exception.log
                         C:\Users\Admin\AppData\Local
 Opens:
                         C:\Users\Admin\AppData\Local\BulletProof Software\BulletProof FTP Client
 Opens:
2009\sites\Bookmarks\
                         C:\Users\Admin\AppData\Roaming\BulletProof Software\BulletProof FTP
 Opens:
Client 2009\sites\Bookmarks\
 Opens:
                         C:\windows\temp\profapi.dll
                         C:\Windows\SysWOW64\profapi.dll
 Opens:
 Opens:
                         C:\ProgramData
 Opens:
                         C:\ProgramData\BulletProof Software\BulletProof FTP Client
2009\sites\Bookmarks\
                         C:\Users\Admin\AppData\Local\BulletProof Software\BulletProof FTP
Client\2010\sites\Bookmarks\
                         C:\Users\Admin\AppData\Roaming\BulletProof Software\BulletProof FTP
 Opens:
Client\2010\sites\Bookmarks\
                         C:\ProgramData\BulletProof Software\BulletProof FTP
 Opens:
Client\2010\sites\Bookmarks\
 Opens:
                         C:\pagefile.sys
 Opens:
                         C:\PerfLogs
 Opens:
                         C:\PerfLogs\Admin
 Opens:
                         C:\Program Files
 Opens:
                         C:\Program Files\Common Files
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink
                         C:\Program Files\Common Files\Microsoft Shared\ink\Alphabet.xml
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\BulletProof Software\BulletProof FTP Client
2009\Default.bps
 Opens:
                         C:\Users\Admin\AppData\Roaming\BulletProof Software\BulletProof FTP
Client 2009\Default.bps
                         C:\ProgramData\BulletProof Software\BulletProof FTP Client
 Opens:
2009\Default.bps
 Opens:
                         C:\Users\Admin\AppData\Local\BulletProof Software\BulletProof FTP
Client\2010\Default.bps
                         C:\Users\Admin\AppData\Roaming\BulletProof Software\BulletProof FTP
 Opens:
Client\2010\Default.bps
 Opens:
                         C:\ProgramData\BulletProof Software\BulletProof FTP
Client\2010\Default.bps
 Opens:
                         C:\Users\Admin\AppData\Roaming\TurboFTP\addrbk.dat
 Opens:
                         C:\Users\Admin\AppData\Roaming\GPSoftware\Directory
Opus\ConfigFiles\ftp.oxc
                         C:\Users\Admin\AppData\Roaming\GPSoftware\Directory
Opus\Layouts\System\default.oll
                         C:\Users\Admin\AppData\Local\GPSoftware\Directory
 Opens
Opus\ConfigFiles\ftp.oxc
                         C:\Users\Admin\AppData\Local\GPSoftware\Directory
 Opens:
Opus\Layouts\System\default.oll
 Opens:
                         C:\ProgramData\GPSoftware\Directory Opus\ConfigFiles\ftp.oxc
 Opens:
                         C:\ProgramData\GPSoftware\Directory Opus\Layouts\System\default.oll
 Opens:
                         C:\Windows\32BitFtp.ini
 Opens:
                         C:\Users\Admin\AppData\Roaming\VanDyke\Config\Sessions
                         C:\Users\Admin\AppData\Roaming\BitKinex\bitkinex.ds
 Opens:
                         C:\Users\Admin\AppData\Roaming\GlobalSCAPE\CuteFTP
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\GlobalSCAPE\CuteFTP Pro
 Opens:
                         C:\Users\Admin\AppData\Roaming\GlobalSCAPE\CuteFTP Lite
                         C:\ProgramData\GlobalSCAPE\CuteFTP
 Opens:
                         C:\ProgramData\GlobalSCAPE\CuteFTP Pro
 Opens:
 Opens:
                         C:\ProgramData\GlobalSCAPE\CuteFTP Lite
 Opens:
                         C:\Program Files (x86)
 Opens:
                         C:\Program Files (x86)\CuteFTF
 Opens:
                         C:\Windows\win.ini
 Opens:
                         C:\Program Files (x86)\Common Files
                         C:\Program Files (x86)\Common Files\Ipswitch\WS_FTP
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\Ipswitch\WS_FTP\Sites
                         C:\Users\Admin\AppData\Roaming\Ipswitch\WS_FTP Home\Sites
 Opens:
                         C:\ProgramData\Ipswitch\WS_FTP\Sites
 Opens:
                         C:\ProgramData\Ipswitch\WS_FTP Home\Sites
 Opens:
                         {\tt C:\Users\Admin\AppData\Local\Ipswitch\WS\_FTP\Sites}
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Ipswitch\WS_FTP Home\Sites
 Opens:
                         {\tt C:\Users\Admin\AppData\Roaming\NetDrive\NDSites.ini}
 Opens:
                         C:\ProgramData\NetDrive\NDSites.ini
                         C:\Users\Admin\AppData\Local\NetDrive\NDSites.ini
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\FileZilla\sitemanager.xml
```

```
Opens:
                         C:\Users\Admin\AppData\Roaming\FileZilla\recentservers.xml
                         C:\Users\Admin\AppData\Roaming\FTP Explorer\profiles.xml
 Opens:
                         C:\ProgramData\FTP Explorer\profiles.xml
 Opens:
                         C:\Users\Admin\AppData\Local\FTP Explorer\profiles.xml
 Opens:
                         C:\Users\Admin\AppData\Roaming\SmartFTP\Favorites.dat
 Opens:
                         C:\Users\Admin\AppData\Roaming\SmartFTP\Client
 Opens:
2.0\Favorites\Favorites.dat
                         C:\Users\Admin\AppData\Roaming\SmartFTP\History.dat
 Opens:
                         Opens:
 Opens:
                         C:\ProgramData\SmartFTP\Favorites.dat
 Opens:
                         C:\ProgramData\SmartFTP\Client 2.0\Favorites\Favorites.dat
                         C:\ProgramData\SmartFTP\History.dat
 Opens:
                         C:\ProgramData\SmartFTP\Client 2.0\Favorites\
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\FTPRush\RushSite.xml
 Opens:
                         C:\Users\Admin\AppData\Roaming\Frigate3\FtpSite.XML
 Opens:
                         C:\Users
 Opens:
                         C:\Users\All Users
                         C:\Users\Default User
 Opens:
 Opens:
                         C:\Users\Default
 Opens:
                         C:\Users\Admin\AppData\Roaming\Bitcoin\wallet.dat
 Opens:
                         C:\ProgramData\APPDATA\ROAMING\BITCOIN\WALLET.DAT
                         C:\Users\Default\AppData\Roaming\Bitcoin\wallet.dat
 Opens:
 Opens:
                         C:\Users\Public\AppData\Roaming\Bitcoin\wallet.dat
 Opens:
                         C:\Windows\wcx_ftp.ini
                         C:\Windows\Windows Commander\wcx_ftp.ini
 Opens:
 Opens:
                         C:\Windows\Total Commander\wcx_ftp.ini
 Opens:
                         C:\Users\Admin
                         C:\Users\Admin\wcx_ftp.ini
 Opens:
 Opens:
                         C:\Users\Admin\Windows Commander\wcx_ftp.ini
 Opens:
                         C:\Users\Admin\Total Commander\wcx_ftp.ini
 Opens:
                         C:\Program Files (x86)\wcx_ftp.ini
 Opens:
                         C:\Program Files (x86)\Windows Commander\wcx_ftp.ini
 Opens:
                         C:\Program Files (x86)\Total Commander\wcx_ftp.ini
 Opens:
                         C:\Users\Admin\AppData\Roaming\GHISLER\wcx_ftp.ini
 Opens:
                         C:\Users\Admin\AppData\Roaming\Windows Commander\GHISLER\wcx_ftp.ini
                         C:\Users\Admin\AppData\Roaming\Total Commander\GHISLER\wcx_ftp.ini
 Opens:
 Opens:
                         C:\ProgramData\GHISLER\wcx_ftp.ini
 Opens:
                         C:\ProgramData\Windows Commander\GHISLER\wcx_ftp.ini
 Opens:
                         C:\ProgramData\Total Commander\GHISLER\wcx_ftp.ini
 Opens:
                         C:\Users\Admin\AppData\Local\GHISLER\wcx_ftp.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Windows Commander\GHISLER\wcx_ftp.ini
                         C:\Users\Admin\AppData\Local\Total Commander\GHISLER\wcx_ftp.ini
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\AceBIT\
 Opens:
                         C:\ProgramData\AceBIT\
                         C:\Windows\SysWOW64\tzres.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\tzres.dll.mui
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\AceBIT\
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink\ar-SA
 Opens:
                         C:\windows\temp\pstorec.dll
 Opens:
                         C:\Windows\SysWOW64\pstorec.dll
                         C:\Program Files\Common Files\Microsoft Shared\ink\ar-SA\tipresx.dll.mui
 Opens:
 Opens:
                         C:\windows\temp\ATL.DLL
 Opens:
                         C:\Windows\SysWOW64\atl.dll
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink\bg-BG
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink\bg-BG\tipresx.dll.mui
                         C:\Program Files\Common Files\Microsoft Shared\ink\Content.xml
 Opens:
 Opens:
                         C:\Windows\SysWOW64\wship6.dll
                         C:\Program Files\Common Files\Microsoft Shared\ink\cs-CZ
 Opens:
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink\cs-CZ\tipresx.dll.mui
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink\da-DK
                         C:\Program Files\Common Files\Microsoft Shared\ink\da-DK\tipresx.dll.mui
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink\de-DE
 Opens:
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink\de-DE\tipresx.dll.mui
                         C:\Program Files\Common Files\Microsoft Shared\ink\el-GR
 Opens:
                         {\tt C:\Program\ Files\Common\ Files\Microsoft\ Shared\ink\el-GR\tipresx.dll.mui}
 Opens:
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink\en-US
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\FlickLearningWizard.exe.mui
                         C:\Program Files\Common Files\Microsoft Shared\ink\en-US\InkObj.dll.mui
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink\en-
 Opens:
US\InkWatson.exe.mui
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\InputPersonalization.exe.mui
                         C:\Program Files\Common Files\Microsoft Shared\ink\en-
 Opens:
{\tt US\backslash IPSEventLogMsg.dll.mui}
                         C:\Users\Admin\AppData\Roaming\Google\Chrome\
 Opens:
                         C:\Users\Admin\AppData\Local\Google\Chrome\
 Opens:
 Opens:
                         C:\ProgramData\Google\Chrome\
 Opens:
                         C:\Users\Admin\AppData\Roaming\Chromium\
                         C:\Users\Admin\AppData\Local\Chromium\
 Opens:
 Opens:
                         C:\ProgramData\Chromium\
 Opens:
                         C:\Users\Admin\AppData\Roaming\ChromePlus\
 Opens:
                         C:\Users\Admin\AppData\Local\ChromePlus\
                         C:\Program Files\Common Files\Microsoft Shared\ink\en-
 Opens:
US\IpsMigrationPlugin.dll.mui
 Opens:
                         C:\ProgramData\ChromePlus\
 Opens:
                         C:\Users\Admin\AppData\Roaming\Bromium\
 Opens:
                         C:\Users\Admin\AppData\Local\Bromium\
                         C:\ProgramData\Bromium\
 Opens:
                         C:\Users\Admin\AppData\Roaming\Nichrome\
 Opens:
```

```
Opens:
                                  C:\Users\Admin\AppData\Local\Nichrome\
  Opens:
                                  C:\Program Files\Common Files\Microsoft Shared\ink\en-US\micaut.dll.mui
                                  C:\ProgramData\Nichrome\
  Opens:
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Comodo\
  Opens:
                                  C:\Users\Admin\AppData\Local\Comodo\
                                  C:\ProgramData\Comodo\
  Opens:
  Opens:
                                  C:\Users\Admin\AppData\Roaming\RockMelt\
                                  C:\Users\Admin\AppData\Local\RockMelt\
  Opens:
                                  C:\ProgramData\RockMelt\
  Opens:
  Opens:
                                  C:\Users\Admin\AppData\Roaming\MapleStudio\ChromePlus\
  Opens:
                                  C:\Program Files\Common Files\Microsoft Shared\ink\en-US\mip.exe.mui
                                  C:\Users\Admin\AppData\Local\MapleStudio\ChromePlus\
  Opens:
                                  C:\ProgramData\MapleStudio\ChromePlus\
  Opens:
  Opens:
                                  C:\Users\Admin\AppData\Roaming\browser.yandex\
                                  C:\Users\Admin\AppData\Local\browser.yandex\
  Opens:
                                  C:\ProgramData\browser.yandex\
  Opens:
  Opens:
                                  C:\Users\Admin\Desktop
                                  \hbox{\tt C:\Users\Admin\AppData\Roaming\Adobe}\\
  Opens:
  Opens:
                                  Opens:
                                  C:\Users\Admin\AppData\Roaming\Adobe\Acrobat\9.0
                                  C:\Program Files\Common Files\Microsoft Shared\ink\en-
  Opens:
US\mshwLatin.dll.mui
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Adobe\Acrobat\9.0\Collab
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Adobe\Acrobat\9.0\Forms
                                  C:\Users\Admin\AppData\Roaming\Adobe\Acrobat\9.0\JavaScripts
  Opens:
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Identities
                                  C:\Users\Admin\AppData\Roaming\Identities\{9506AC1B-447F-4459-900E-
  Opens:
43BE84A098E7}
  Opens:
                                  {\tt C:\Program\ Files\Common\ Files\Microsoft\ Shared\ink\en-US\rtscom.dll.mui}
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Media Center Programs
                                  C:\Users\Admin\AppData\Roaming\Microsoft
  Opens:
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\AddIns
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Credentials
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Crypto
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Crypto\RSA
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-980053277-
  Opens:
1733835069-2361817685-1001
  Opens:
                                  C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\ShapeCollector.exe.mui
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick
  Opens:
Launch\User Pinned
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick
Launch\User Pinned\ImplicitAppShortcuts
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick
  Opens:
Launch\User Pinned\TaskBar
  Opens:
                                  C: \verb|\Users\Admin\AppData\Roaming\Microsoft\MMC| \\
  Opens:
                                  {\tt C: \V Sers \Admin \App Data \Roaming \Microsoft \Network}
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk\_hiddenPbk
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Office
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Office\Recent
  Opens:
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Protect
                                  Opens:
1733835069-2361817685-1001
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates
  Opens:
                                  C:\Program Files\Common Files\Microsoft Shared\ink\en-US\tabskb.dll.mui
                                  C:\Program Files\Common Files\Microsoft Shared\ink\en-US\TipBand.dll.mui
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My
  Opens:
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates
                                  C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Templates
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows
  Opens:
  Opens:
                                  {\tt C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies}
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache
  Opens:
                                  C:\Program Files\Common Files\Microsoft Shared\ink\en-US\TipRes.dll.mui
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache\Low
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
  Opens:
                                  C: \label{loss} C: \label{lo
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries
  Opens:
                                  {\tt C:\Windows\Network\ Shortcuts}
  Opens:
  Opens:
                                  {\tt C:\Program\ Files\Common\ Files\Microsoft\ Shared\ink\en-US\tipresx.dll.mui}
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE\Low
  Opens:
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
                                  {\tt C:\Program\ Files\Common\ Files\Microsoft\ Shared\ink\en-US\TipTsf.dll.mui}
  Opens:
  Opens:
Opens:
                                  C:\Program Files\Common Files\Microsoft Shared\ink\es-ES
                                  C:\Program Files\Common Files\Microsoft Shared\ink\es-ES\tipresx.dll.mui
  Opens:
                                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\SendTo
  Opens:
```

```
Opens:
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
  Opens:
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
  Opens:
Menu\Programs\Accessories\Accessibility
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
  Opens:
Menu\Programs\Accessories\System Tools
  Opens:
                                   {\tt C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start}
Menu\Programs\Administrative Tools
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Maintenance
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Templates
  Opens:
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Oracle
  Opens:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\et-EE
  Opens:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\et-EE\tipresx.dll.mui
  Opens:
                                   C:\Users\Admin\AppData\Roaming\Oracle\Java
                                   C:\Users\Admin\AppData\Roaming\Oracle\Java\Uninstall
  Opens:
                                   C:\Users\Admin\AppData\Local\Adobe
  Opens:
  Opens:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\fi-FI
  Opens:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\fi-FI\tipresx.dll.mui
  Opens:
                                   C:\Users\Admin\AppData\Local\Adobe\Acrobat
                                   C:\Users\Admin\AppData\Local\Adobe\Acrobat\9.0
  Opens:
                                   C:\Users\Admin\AppData\Local\Adobe\Acrobat\9.0\Cache
  Opens:
  Opens:
                                   C:\Users\Admin\AppData\Local\Adobe\Color
  Opens:
                                   C:\Users\Admin\AppData\Local\Adobe\Color\Profiles
  Opens:
                                   C:\Users\Admin\AppData\Local\Application Data\
                                   C:\Users\Admin\AppData\Local\History\
  Opens:
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Credentials
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Event Viewer
                                   C:\Users\Admin\AppData\Local\Microsoft\Event Viewer\Views
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Feeds
  Opens:
  Opens:
                                   {\tt C:\Users\Admin\AppData\Local\Microsoft\Feeds\Feeds\ for\ United\ States}^{\tt C:\Users\Admin\AppData\Local\Microsoft\Feeds\ for\ United\ States}^{\tt C:\Users\ for\ United\ States\ for\ Unite\ United\ States\ for\ Unite\ Un
  Opens:
                                   {\tt C:\Program\ Files\Common\ Files\Microsoft\ Shared\ink\fr-FR}
  Opens:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\fr-FR\tipresx.dll.mui
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Feeds\Microsoft Feeds~
  Opens:
                                   666AE6A92D3D}~
                                   C:\Users\Admin\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-
  Opens:
666AE6A92D3D}~\WebSlices~
                                   C:\Users\Admin\AppData\Local\Microsoft\Feeds Cache
  Opens:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions
  Opens:
  Opens:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\auxpad
  Opens:
                                   Opens:
                                   Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Feeds Cache\JH8KG3LN
                                   C:\Users\Admin\AppData\Local\Microsoft\Feeds Cache\Q0UWLZUG
  Opens:
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer
  Opens:
                                   C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\auxpad\auxbase.xml
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\DOMStore
  Opens:
  Onens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\2UWQWYVI
  Opens:
                                   C: \verb|\Users\Admin\AppData\Local\Microsoft\Internet|
Explorer\DOMStore\KOWHMEP2
                                   {\tt C:\Users\Admin\AppData\Local\Microsoft\Internet}
Explorer\DOMStore\NLN206FE
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\VU73CBGV
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\Recovery
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\Recovery\Active
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\Recovery\High
  Opens:
  Opens:
                                   C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\auxpad.xml
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Recovery\High\Active
                                   C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Recovery\High\Last Active
  Opens:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad
                                   C:\Program Files\Common Files\Microsoft
  Opens:
Shared \verb|\ink\fsdefinitions\keypad\ea.xml|
                                   C:\Program Files\Common Files\Microsoft
  Opens:
Shared \verb|\ink\fsdefinitions\keypad\keypadbase.xml|
  Opens:
                                   {\tt C:\Users\Admin\AppData\Local\Microsoft\Internet\ Explorer\Recovery\Last}
Active
                                   C:\Users\Admin\AppData\Local\Microsoft\Media Player
  Opens:
                                   C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\keypad\kor-kor.xml
                                   C:\Users\Admin\AppData\Local\Microsoft\Media Player\Sync Playlists
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Media Player\Sync Playlists\en-
  Opens
US\000207D6
  Opens:
                                   C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\keypad.xml
                                   C:\Users\Admin\AppData\Local\Microsoft\Office
  Opens:
                                   C:\Users\Admin\AppData\Local\Microsoft\Office\12.0
  Opens:
```

```
Opens:
                                        C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main
                                        C:\Users\Admin\AppData\Local\Microsoft\Office\14.0
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\TaskSchedulerConfig
  Opens:
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\1033
  Opens:
                                        C:\Program Files\Common Files\Microsoft
  Opens:
Shared\ink\fsdefinitions\main\hase.xml
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Burn
  Opens:
  Opens:
                                        C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\Burn\Burn|
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Explorer
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\GameExplorer
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Historv\Low
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5
  Opens:
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Ringtones
  Opens:
                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet\ Files}
  Opens:
                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\AntiPhishing
                                        \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet| \\
  Opens:
Files\Content.IE5
                                        \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet| \\
  Opens:
Files\Content.IE5\266VNL5S
                                        C:\Program Files\Common Files\Microsoft
  Opens:
Shared\ink\fsdefinitions\main\baseAltGr_rtl.xml
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\TZILKL9J
                                        C:\Program Files\Common Files\Microsoft
  Opens:
Shared\ink\fsdefinitions\main\base_altgr.xml
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\WM60WM90
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.MSO
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Low
  Opens:
                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Low\AntiPhishing
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5
                                        C:\Program Files\Common Files\Microsoft
  Opens:
Shared\ink\fsdefinitions\main\base_ca.xml
                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
  Opens:
Files\Low\Content.IE5\175TAOYU
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5\MJZKTK0Y
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5\QQSZX7PK
  Opens:
                                        C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base_heb.xml
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5\ZKONPR3Z
                                        C:\Program Files\Common Files\Microsoft
  Opens:
\dot{\text{Shared}} \ \dot{\text{
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized
  Opens:
                                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Virtualized\C
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized\C\Users
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized\C\Users\Admin
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
\dot{ \tt Files \Virtualized \C \Users \Admin \App Data}
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files \verb|\Virtualized\C\Users\Admin\AppData\Roaming\Microsoft
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized\C\Users\Admin\AppData\Roaming\Microsoft\Windows
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized\C\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\WER
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ReportArchive
                                        {\tt C: \Wers\Admin\AppData\Local\Microsoft\Windows\WER\Report\Queue}
  Opens:
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ReportQueue\NonCritical_VCRED000.EXE_8fab9a8aafb14ca3aa6b78edacd1d07896b1794_cab_088f7855
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Windows Anytime Upgrade
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows Mail
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows Mail\Backup
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows Mail\Backup\new
  Opens:
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows Mail\Stationery
  Opens:
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows Media
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows Media\12.0
  Opens:
```

 ${\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\ Sidebard}$

Opens:

```
Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows Sidebar\Gadgets
                         C:\Users\Admin\AppData\Local\Programs
 Opens:
                         C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base_kor.xml
                         C:\Users\Admin\AppData\Local\Programs\Common
 Opens:
                         C:\Users\Admin\AppData\Local\Temp
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\gen_py
 Onens:
                         C:\Program Files\Common Files\Microsoft
 Opens:
Shared\ink\fsdefinitions\main\base_rtl.xml
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\gen_py\2.7
 Opens:
                         {\tt C: \V Sers \Admin \App Data \Local \Temp \hsperfdata\_Admin}
                         C:\Users\Admin\AppData\Local\Temp\Low
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\Microsoft Visual C++ 2010 \times64
Redistributable Setup_10.0.30319
                         C:\Users\Admin\AppData\Local\Temp\Microsoft Visual C++ 2010 x86
 Opens:
Redistributable Setup_10.0.30319
                         C:\Users\Admin\AppData\Local\Temp\WPDNSE
 Opens:
                         Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Temporary Internet Files\
 Opens:
                         C:\Users\Admin\AppData\Local\VirtualStore
 Opens:
                         C:\ProgramData\Adobe
                         C:\ProgramData\Adobe\Acrobat
 Opens:
 Opens:
                         C:\ProgramData\Adobe\Acrobat\9.0
 Opens:
                         C:\ProgramData\Adobe\Acrobat\9.0\Replicate
                         C:\ProgramData\Adobe\Acrobat\9.0\Replicate\Security
 Opens:
 Opens:
                         C:\ProgramData\Adobe\Reader
                         C:\ProgramData\Adobe\Reader\9.3
 Opens:
                         C:\ProgramData\Adobe\Reader\9.3\ARM
 Opens:
 Opens:
                         C:\ProgramData\Adobe\Reader\9.3\ARM\26091
 Opens:
                         C:\ProgramData\Adobe\Updater6
                         C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\ja-jp.xml
 Opens:
                         C:\ProgramData\Application Data\
 Opens:
                         C:\ProgramData\Desktop\
 Opens:
                         C:\ProgramData\Documents\
                         C:\ProgramData\Favorites\
 Opens:
 Opens:
                         C:\ProgramData\Microsoft
 Opens:
                         C: \verb|\ProgramData\Microsoft\Assistance| \\
 Opens:
                         C:\ProgramData\Microsoft\Assistance\Client
 Opens:
                         C:\ProgramData\Microsoft\Assistance\Client\1.0
 Opens:
                         C:\ProgramData\Microsoft\Assistance\Client\1.0\en-US
                         C:\Program Files\Common Files\Microsoft
 Opens:
Shared\ink\fsdefinitions\main\ko-kr.xml
                         C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\zh-changjei.xml
                         C:\ProgramData\Microsoft\Crypto
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\Crypto\DSS
                         C:\ProgramData\Microsoft\Crypto\DSS\MachineKeys
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\Crypto\Keys
 Opens:
                         C:\ProgramData\Microsoft\Crypto\RSA
                         C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
 Opens:
                         C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\Device Stage
                         C:\ProgramData\Microsoft\Device Stage\Device
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-
97838f1b04b03
                         \label{lem:c:programDataMicrosoftDevice StageDevice} C: \ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-6484}.
 Opens:
4d3decd87120}
 Opens:
                         C:\ProgramData\Microsoft\Device Stage\Task
                         C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-
 Opens:
d8f2cf8722c9}
 Opens:
                         C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\zh-dayi.xml
                         C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-
 Opens:
d8f2cf8722c9}\en-US
                         C:\ProgramData\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-
 Opens:
1775fb1a7a42}
 Opens:
                         C:\ProgramData\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-
1775fb1a7a42}\en-US
                         C:\ProgramData\Microsoft\DeviceSync
 Opens:
                         C:\ProgramData\Microsoft\DRM
 Opens:
                         C:\ProgramData\Microsoft\DRM\Server
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\eHome
                         C:\ProgramData\Microsoft\eHome\logs
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\Event Viewer
 Opens:
                         C:\ProgramData\Microsoft\Event Viewer\Views
                         C:\ProgramData\Microsoft\Event Views\ApplicationViewsRootNode
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\Event Viewer\Windows Logs
 Opens:
                         C:\ProgramData\Microsoft\IdentityCRL
 Opens:
                         C:\ProgramData\Microsoft\IlsCache
                         C:\ProgramData\Microsoft\Media Player
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\MF
 Opens:
                         C:\ProgramData\Microsoft\Network
                         C:\ProgramData\Microsoft\Network\Connections
 Opens:
                         C:\ProgramData\Microsoft\Network\Downloader
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\PlayReady
 Opens:
                         {\tt C:\ProgramData\Microsoft\RAC}
 Opens:
                         C: \verb|\ProgramData\Microsoft\RAC\Outbound| \\
                          C:\ProgramData\Microsoft\RAC\PublishedData
 Opens:
                         C:\ProgramData\Microsoft\RAC\StateData
 Opens:
```

```
Opens:
                                               C:\ProgramData\Microsoft\RAC\Temp
                                               C:\Program Files\Common Files\Microsoft
   Opens:
Shared\ink\fsdefinitions\main\zh-phonetic.xml
   Opens:
                                               C:\ProgramData\Microsoft\Search
                                               C:\ProgramData\Microsoft\Search\Data
   Opens:
                                               C:\ProgramData\Microsoft\Search\Data\Applications
   Opens:
   Opens:
                                               C:\ProgramData\Microsoft\Search\Data\Applications\Windows
                                               C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Config
   Opens:
   Opens:
                                               Opens:
\label{lem:condition} C: \Program Data \Microsoft \Search \Data \Applications \Windows \Gather Logs \System Index \Applications \Windows \Gather \Ga
                                               C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects
   Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex
   Opens:
                                               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main.xml
   Opens:
{\tt C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\IndexerReserved} \\
   Opens:
C: \PogramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\PropMap
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\SecStore
   Opens:
                                               C:\ProgramData\Microsoft\Search\Data\Temp
                                               C:\ProgramData\Microsoft\User Account Pictures
   Opens:
                                               C:\ProgramData\Microsoft\User Account Pictures\Default Pictures
   Opens:
                                               C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\numbers
   Opens:
   Opens:
                                               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\numbers\numbase.xml
                                               C:\ProgramData\Microsoft\Vault
   Opens:
   Opens:
                                               C:\ProgramData\Microsoft\Windows
   Opens:
                                               C:\ProgramData\Microsoft\Windows\AIT
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Caches
   Opens:
                                               C:\ProgramData\Microsoft\Windows\DeviceMetadataStore
                                               C:\ProgramData\Microsoft\Windows\DeviceMetadataStore\en-US
   Opens:
   Opens:
                                               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\numbers.xml
   Opens:
                                                C:\ProgramData\Microsoft\Windows\DRM
   Opens:
                                               C:\ProgramData\Microsoft\Windows\DRM\Cache
   Opens:
                                               C:\ProgramData\Microsoft\Windows\GameExplorer
                                               C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics
   Opens:
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Ringtones
   Opens:
                                               C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskmenu
                                               C:\Program Files\Common Files\Microsoft
   Opens:
Shared\ink\fsdefinitions\oskmenu\oskmenubase.xml
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Sqm
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Sqm\Manifest
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Sqm\Sessions
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Sqm\Upload
                                               C:\ProgramData\Microsoft\Windows\Start Menu
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Start Menu\Programs
   Opens:
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories
                                               C:\ProgramData\Microsoft\Windows\Start
   Opens:
Menu\Programs\Accessories\Accessibility
                                               C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\System
   Onens:
Tools
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Tablet
PC
   Opens:
                                               \verb| C: \P o and \P o an
PowerShell
   Opens:
                                               \verb|C:\ProgramData\Microsoft\Windows\Start\ Menu\Programs\Administrative|\\
Tools
                                               C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Games
   Opens:
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance
                                               C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Python 2.7
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
   Opens:
   Opens:
                                               C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Tablet PC
                                               C:\Program Files\Common Files\Microsoft
   Opens:
Shared\ink\fsdefinitions\oskmenu.xml
                                               C:\ProgramData\Microsoft\Windows\Templates
   Opens:
                                               C:\ProgramData\Microsoft\Windows\WER
   Opens:
   Opens:
                                               C:\ProgramData\Microsoft\Windows\WER\ReportArchive
                                               C:\ProgramData\Microsoft\Windows\WER\ReportQueue
   Opens:
   Opens:
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_x64_5d5d8b7c1982ab7c66cf747e7b18b39e2441a_cab_07106987
   Opens:
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_x64_d473a376adfb18a7b165c5e3c26de43cd8bccb_cab_07e86b1d
   Opens:
                                                C:\ProgramData\Microsoft\Windows Defender
                                               C:\ProgramData\Microsoft\Windows Defender\Definition Updates
   Opens:
   Opens:
                                               C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Backup
   Opens:
                                               C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Updates
   Opens:
                                               C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{D2B0B133-
42ED-44D3-809A-46EBB62BA863}
                                               C:\ProgramData\Microsoft\Windows Defender\LocalCopy
   Opens:
   Opens:
                                               C:\ProgramData\Microsoft\Windows Defender\Quarantine
   Opens:
                                               C:\ProgramData\Microsoft\Windows Defender\Scans
   Opens:
                                               C:\ProgramData\Microsoft\Windows Defender\Scans\History
                                               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\osknumpad
```

```
Opens:
                                   C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\osknumpad\osknumpadbase.xml
                                    C:\ProgramData\Microsoft\Windows Defender\Scans\History\CacheManager
  Opens:
                                    C:\ProgramData\Microsoft\Windows Defender\Scans\History\Results
  Opens:
                                   C:\ProgramData\Microsoft\Windows Defender\Scans\History\Service
  Opens:
                                    C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store
  Opens:
                                    C:\ProgramData\Microsoft\Windows Defender\Support
                                    C:\ProgramData\Microsoft\Windows NT
  Opens:
  Opens:
                                    {\tt C: \normalize{C: \normali
  Opens:
                                    C:\ProgramData\Microsoft\Windows NT\MSFax\ActivityLog
  Opens:
                                    C:\ProgramData\Microsoft\Windows NT\MSFax\Common Coverpages
                                    C:\ProgramData\Microsoft\Windows NT\MSFax\Common Coverpages\en-US
  Opens:
  Opens:
                                    C:\ProgramData\Microsoft\Windows NT\MSFax\Inbox
  Opens:
                                    C:\ProgramData\Microsoft\Windows NT\MSFax\Queue
  Opens:
                                   C:\ProgramData\Microsoft\Windows NT\MSFax\SentItems
                                    C:\ProgramData\Microsoft\Windows NT\MSFax\VirtualInbox
  Opens:
                                   C:\ProgramData\Microsoft\Windows NT\MSFax\VirtualInbox\en-US
  Opens:
                                    C:\ProgramData\Microsoft\Windows NT\MSScan
  Opens:
  Opens:
                                   C:\ProgramData\Microsoft\WwanSvc
  Opens:
                                    C:\ProgramData\Microsoft\WwanSvc\Profiles
  Opens:
                                    C:\ProgramData\Start Menu\
                                    C:\ProgramData\Sun
  Opens:
  Opens:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\osknumpad.xml
                                   C:\ProgramData\Sun\Java
  Opens:
  Opens:
                                   C:\ProgramData\Sun\Java\Java Update
  Opens:
                                   C:\ProgramData\Templates\
                                   C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskpred
  Opens:
  Opens:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\oskpred\oskpredbase.xml
                                    C:\Program Files (x86)\Whisper Technology\FTP Surfer\
  Opens:
  Opens:
                                    C:\Users\Admin\AppData\Roaming\FTPGetter
  Opens:
                                   C:\ProgramData\FTPGetter\
  Opens:
                                    C:\Users\Admin\AppData\Local\FTPGetter\
                                   C:\Users\Admin\AppData\Roaming\Estsoft\ALFTP\
  Opens:
  Opens:
                                    C:\ProgramData\Estsoft\ALFTP\
  Opens:
                                   C:\Users\Admin\AppData\Local\Estsoft\ALFTP\
  Opens:
                                   C:\Users\Admin\AppData\Roaming\BlazeFtp\
  Opens:
                                   C:\ProgramData\BlazeFtp\
  Opens:
                                    C:\Users\Admin\AppData\Local\BlazeFtp\
  Opens:
                                    C:\Users\Admin\AppData\Roaming\3D-FTP\
  Opens:
                                    C:\ProgramData\3D-FTP\
  Opens:
                                    C:\Users\Admin\AppData\Local\3D-FTP\
                                   C:\Users\Admin\AppData\Roaming\SiteDesigner\
  Opens:
                                   C:\ProgramData\SiteDesigner\
  Opens:
                                   C:\Users\Admin\AppData\Local\SiteDesigner\
  Opens:
  Opens:
                                   C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\oskpred.xml
  Opens:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols
  Opens:
                                   C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\symbols\ea-sym.xml
                                   C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\symbols\ja-jp-sym.xml
                                   C:\Program Files\Common Files\Microsoft
  Opens:
Shared\ink\fsdefinitions\symbols\symbase.xml
                                   C:\Program Files\Common Files\Microsoft
  Onens:
Shared\ink\fsdefinitions\symbols.xml
                                   {\tt C:\Program\ Files\Common\ Files\Microsoft\ Shared\ink\fsdefinitions\web}
  Opens:
  Opens:
                                   C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\web\webbase.xml
                                    C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\web.xml
  Opens:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\he-IL
  Opens:
  Opens:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\he-IL\tipresx.dll.mui
  Opens:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\hr-HR
                                    C:\Program Files\Common Files\Microsoft Shared\ink\hr-HR\tipresx.dll.mui
  Opens:
  Opens:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\hu-HU
                                    C:\Program Files\Common Files\Microsoft Shared\ink\hu-HU\tipresx.dll.mui
  Opens:
  Opens:
                                   {\tt C:\Program\ Files\Common\ Files\Microsoft\ Shared\ink\hwrcommonlm.dat}
  Opens:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\HWRCustomization
  Opens:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\hwrenalm.dat
  Reads from:
                                    C:\Windows\Temp\752d6fe81122349daf998a56f48e0b38.exe
                                    C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
  Reads from:
1001\desktop.ini
  Reads from:
                                    C:\exception.log
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\Alphabet.xml
  Reads from:
                                    C:\Windows\win.ini
                                    C:\Program Files\Common Files\Microsoft Shared\ink\ar-SA\tipresx.dll.mui
  Reads from:
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\bg-BG\tipresx.dll.mui
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\Content.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\cs-CZ\tipresx.dll.mui
                                    C:\Program Files\Common Files\Microsoft Shared\ink\da-DK\tipresx.dll.mui
  Reads from:
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\de-DE\tipresx.dll.mui
  Reads from:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\el-GR\tipresx.dll.mui
                                   C:\Program Files\Common Files\Microsoft Shared\ink\en-
  Reads from:
US\FlickLearningWizard.exe.mui
                                   C:\Program Files\Common Files\Microsoft Shared\ink\en-US\InkObi.dll.mui
  Reads from:
  Reads from:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\InkWatson.exe.mui
  Reads from:
                                   C:\Program Files\Common Files\Microsoft Shared\ink\en-
```

US\InputPersonalization.exe.mui

```
Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\IPSEventLogMsg.dll.mui
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\IpsMigrationPlugin.dll.mui
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-US\micaut.dll.mui
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-US\mip.exe.mui
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-
  Reads from:
US\mshwLatin.dll.mui
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-US\rtscom.dll.mui
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\ShapeCollector.exe.mui
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-US\tabskb.dll.mui
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-US\TipBand.dll.mui
  Reads from:
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-US\TipRes.dll.mui
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-US\tipresx.dll.mui
  Reads from:
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\en-US\TipTsf.dll.mui
                                    C:\Program Files\Common Files\Microsoft Shared\ink\es-ES\tipresx.dll.mui
  Reads from:
                                    {\tt C:\Program\ Files\Common\ Files\Microsoft\ Shared\ink\et-EE\tipresx.dll.mui}
  Reads from:
  Reads from:
                                     C: \ Files \ Common \ Files \ Microsoft \ Shared \ ink \ fi-FI \ tipresx. dll. mui \ Normal \ Files \ Microsoft \ Shared \ Normal \ Microsoft \ Microsoft \ Normal \ Microsoft \ Normal \ Microsoft \ 
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\fr-FR\tipresx.dll.mui
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared\ink\fsdefinitions\auxpad\auxbase.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\auxpad.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\keypad\ea.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared \verb|\ink\fsdefinitions\keypad\keypadbase.xml|
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\keypad\kor-kor.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared\ink\fsdefinitions\keypad.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared\ink\fsdefinitions\main\base.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared \verb|\ink\fsdefinitions\main\baseAltGr\_rtl.xml|
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared \verb|\ink\fsdefinitions\main\base_altgr.xml|
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base_ca.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base_heb.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared\ink\fsdefinitions\main\base_jpn.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared\ink\fsdefinitions\main\base kor.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared \verb|\ink\fsdefinitions\main\base\_rtl.xml|
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\ja-jp.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\ko-kr.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\zh-changjei.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared\ink\fsdefinitions\main\zh-dayi.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared \verb|\ink\fsdefinitions\main\zh-phonetic.xml|
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main.xml
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\numbers\numbase.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\numbers.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared\ink\fsdefinitions\oskmenu\oskmenubase.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\oskmenu.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared\ink\fsdefinitions\osknumpad\osknumpadbase.xml
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\osknumpad.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\oskpred\oskpredbase.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared\ink\fsdefinitions\oskpred.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft
Shared \verb|\ink\fsdefinitions\symbols\ea-sym.xml|
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared \verb|\ink\fsdefinitions\symbols\ja-jp-sym.xml|
                                    C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\symbols\symbase.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared\ink\fsdefinitions\symbols.xml
                                    C:\Program Files\Common Files\Microsoft
  Reads from:
Shared\ink\fsdefinitions\web\webbase.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\web.xml
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\he-IL\tipresx.dll.mui
  Reads from:
                                    C:\Program Files\Common Files\Microsoft Shared\ink\hr-HR\tipresx.dll.mui
```

C:\Program Files\Common Files\Microsoft Shared\ink\hu-HU\tipresx.dll.mui

Reads from:

C:\Program Files\Common Files\Microsoft Shared\ink\hwrcommonlm.dat
C:\Program Files\Common Files\Microsoft Shared\ink\hwrenalm.dat
C:\Windows\Temp\tmp.exe Reads from: Reads from:

Deletes:

Network Events

Connects to:	127.0.0.1:49160 93.79.131.49:80	
Connects to: Connects to:	127.0.0.1:49163	
Connects to:	95.56.1.35:80	
Connects to:	127.0.0.1:49166	
Connects to:	178.137.28.35:80	
Connects to:	127.0.0.1:49169	
Connects to:	159.148.43.126:80	
Connects to:	127.0.0.1:49172	
Connects to:	178.184.111.126:80	
Connects to:	127.0.0.1:49175	
Connects to:	46.35.160.125:80	
Connects to:	127.0.0.1:49178	
Connects to:	111.248.89.74:80	
Connects to:	127.0.0.1:49181	
Connects to:	183.82.136.221:80	
Connects to:	127.0.0.1:49184	
Connects to:	128.74.134.221:80	
Connects to:	127.0.0.1:49187	
Connects to:	46.250.2.3:80	
Connects to:	127.0.0.1:49190	
Connects to:	46.146.22.4:80	
Connects to:	127.0.0.1:49193	
Connects to:	94.153.6.5:80	
Connects to:	127.0.0.1:49196	
Connects to:	178.89.51.244:80	
Connects to:		
Connects to:	127.0.0.1:49199 95.59.44.244:80	
Connects to:	127.0.0.1:49202	
Connects to:	37.150.17.12:80	
Connects to:	127.0.0.1:49205	
Connects to:	1.203.248.12:80	
Connects to:	127.0.0.1:49208	
Connects to:	178.89.127.0:80	
Connects to:	127.0.0.1:49211	
Connects to:	114.38.242.22:80	
Connects to:	127.0.0.1:49214	
Connects to:	109.229.168.23:80	
Connects to:	127.0.0.1:49217	
Connects to:	37.57.15.7:80	
Connects to:	212.8.43.26:80	
Sends data to:	127.0.0.1:49160	
Sends data to:	93.79.131.49:80	
Sends data to:	127.0.0.1:49163	
Sends data to:	95.56.1.35:80	
Sends data to:	127.0.0.1:49166	
Sends data to:	178.137.28.35:80	
Sends data to:	127.0.0.1:49169	
Sends data to:	159.148.43.126:80	
Sends data to:	127.0.0.1:49172	
Sends data to:	178.184.111.126:80	
Sends data to:	127.0.0.1:49175	
Sends data to:	46.35.160.125:80	
Sends data to:	127.0.0.1:49178	
Sends data to:	111.248.89.74:80	
Sends data to:	127.0.0.1:49181	
Sends data to:	183.82.136.221:80	
Sends data to:	127.0.0.1:49184	
Sends data to:	128.74.134.221:80	
Sends data to:	127.0.0.1:49187	
Sends data to:	46.250.2.3:80	
Sends data to:	127.0.0.1:49190	
Sends data to:	46.146.22.4:80	
Sends data to:	127.0.0.1:49193	
Sends data to:	94.153.6.5:80	
Sends data to:	127.0.0.1:49196	
Sends data to:	178.89.51.244:80	
Sends data to:	127.0.0.1:49199	
Sends data to:	95.59.44.244:80	
Sends data to:	127.0.0.1:49202	
Sends data to:	37.150.17.12:80	
Sends data to:	127.0.0.1:49205	
Sends data to:	1.203.248.12:80	
Sends data to:	127.0.0.1:49208	
Sends data to:	178.89.127.0:80	
Sends data to:	127.0.0.1:49211	
Sends data to:	114.38.242.22:80	
Sends data to:	127.0.0.1:49214	
Sends data to:	109.229.168.23:80	
Sends data to:	127.0.0.1:49217	
Sends data to:	37.57.15.7:80	
Sends data to:	212.8.43.26:80	
Receives data from:	127.0.0.1:49161	

Receives data from: 127.0.0.1:49164 Receives data from: 95.56.1.35:80 Receives data from: 127.0.0.1:49167 Receives data from: 178.137.28.35:80 Receives data from: 127.0.0.1:49170 Receives data from: 159.148.43.126:80 Receives data from: 127.0.0.1:49173 Receives data from: 178.184.111.126:80 Receives data from: 127.0.0.1:49176 Receives data from: 46.35.160.125:80 Receives data from: 127.0.0.1:49179 Receives data from: 111.248.89.74:80 Receives data from: 127.0.0.1:49182 Receives data from: 183.82.136.221:80 Receives data from: 127.0.0.1:49185 Receives data from: 128.74.134.221:80 Receives data from: 127.0.0.1:49188 Receives data from: 46.250.2.3:80 Receives data from: 127.0.0.1:49191 Receives data from: 46.146.22.4:80 Receives data from: 127.0.0.1:49194 Receives data from: 94.153.6.5:80 Receives data from: 127.0.0.1:49197 Receives data from: 178.89.51.244:80 Receives data from: 127.0.0.1:49200 Receives data from: 95.59.44.244:80 Receives data from: 127.0.0.1:49203 Receives data from: 37.150.17.12:80 Receives data from: 127.0.0.1:49206 Receives data from: 1.203.248.12:80 Receives data from: 127.0.0.1:49209 Receives data from: 178.89.127.0:80 Receives data from: 127.0.0.1:49212 Receives data from: 114.38.242.22:80 Receives data from: 127.0.0.1:49215 Receives data from: 109,229,168,23:80 Receives data from: 127.0.0.1:49218 Receives data from: 37.57.15.7:80

Windows Registry Events

Creates key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current \vee ersion \setminus ime \setminus imtc70$ Creates key: HKLM\software\wow6432node\microsoft\windows\currentversion\run Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options Opens key: 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\terminal server Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: ${\tt HKLM \ } system \verb|\ current control \ \\ srp \verb|\ gp \ \\ dll$ Opens key: $HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$ HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens kev: Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\language Opens kev: HKLM\svstem\currentcontrolset\control\mui\uilanguages Opens kev: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete Opens key: $HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| mui\\| settings$ Opens key: HKLM\software\policies\microsoft\mui\settings Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens kev: Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration Opens key: HKCU\software\policies\microsoft\control panel\desktop HKCU\control panel\desktop\languageconfiguration Opens key: Opens key: HKCU\control panel\desktop HKCU\control panel\desktop\muicached Opens kev: $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| side by side \\| microsoft\\| windows\\| current version\\| windows\\| win$ Opens key: Opens key: $\label{lem:hklm} \verb+Kklm \+ system \+ control \+ ls \+ sorting \+ versions$ Opens key: HKLM\ HKLM\software\wow6432node\microsoft\windows Opens key: nt\currentversion\diagnostics Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\gre_initialize HKLM\software\wow6432node\microsoft\windows Opens kev: nt\currentversion\compatibility32 HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime Opens kev: compatibility Opens key:

HKLM\software\wow6432node\microsoft\ole HKLM\software\wow6432node\microsoft\ole\tracing

HKLM\software\wow6432node\microsoft\oleaut

HKLM\system\currentcontrolset\services\crypt32

HKLM\software\wow6432node\microsoft\windows\currentversion\internet

HKLM\software\microsoft\ole\tracing

Opens key: settings Opens kev:

Opens key:

Opens key: Opens kev:

Opens key:

```
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
                  HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings
 Opens key:
                  HKLM\software\policies\microsoft\sqmclient\windows
 Opens key:
                  HKLM\software\microsoft\sqmclient\windows
 Opens key:
                  HKLM\system\currentcontrolset\services\winsock2\parameters
                  HKLM\svstem\currentcontrolset\control\nls\extendedlocale
 Opens kev:
 Opens key:
                  HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\397ab6e2
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries
 Opens kev:
Opens key:
Opens key:
Opens kev:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000000
 Opens kev:
Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
Opens kev:
Opens key:
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006
                  HKLM\svstem\currentcontrolset\services\winsock\parameters
 Opens kev:
 Opens key:
                  HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
 Opens key:
                  HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
 Opens key:
                  \label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ winsock \+ setup migration \+ providers
 Opens key:
                  HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
                  HKLM\system\currentcontrolset\control\cmf\config
 Opens kev:
 Opens key:
                   HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
 Opens key:
                  HKLM\system\currentcontrolset\control\nls\locale
 Opens key:
                  HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
 Opens key:
                  \label{lem:hklm} \verb+Kklm \+ system \+ control \+ language groups \\
 Opens kev:
                  HKCU\software
 Opens key:
                  HKCU\software\adobe
 Opens key:
                  HKCU\software\adobe\acrobat reader
 Opens key:
                  HKCU\software\adobe\acrobat reader\9.0
 Opens key:
                  HKCU\software\adobe\acrobat reader\9.0\adobeviewer
                   HKCU\software\adobe\acrobat reader\9.0\annots
 Opens kev:
 Opens key:
                   \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \adobe \acrobat reader \9.0 \annots \cannots \end{tabular}
 Opens key:
                  HKCU\software\adobe\acrobat reader\9.0\annots\cannot
 Opens kev:
                  HKCU\software\adobe\acrobat reader\9.0\avconversionfrompdf
 Opens key:
                  HKCU\software\adobe\acrobat reader\9.0\avconversionfrompdf\csettings
 Opens kev:
                  HKCU\software\adobe\acrobat reader\9.0\avconversiontopdf
 Opens key:
                  HKCU\software\adobe\acrobat reader\9.0\avconversiontopdf\csettings
 Opens key:
                  HKCU\software\adobe\acrobat reader\9.0\avdisplay
 Opens key:
                  HKCU\software\adobe\acrobat reader\9.0\avgeneral
                   HKCU\software\adobe\acrobat reader\9.0\avgeneral\cdockables
 Opens key:
 Opens key:
                  HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars
 Opens key:
                  HKCU\software\adobe\acrobat
reader\9.0\avgeneral\ctoolbars\cadvcommenting
                  HKCU\software\adobe\acrobat
 Opens kev:
reader\9.0\avgeneral\ctoolbars\cbasiccommenting
                  HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars\ccommenting
 Opens key:
 Opens key:
                  HKCU\software\adobe\acrobat reader\9.0\avtracker
 Opens key:
                  HKCU\software\adobe\acrobat reader\9.0\collab
                  HKCU\software\adobe\acrobat reader\9.0\collab\cdocumentcenter
 Opens key:
```

HKCU\software\adobe\acrobat reader\9.0\collab\cdocumentcenter\csettings

```
Opens key:
                                                HKCU\software\adobe\acrobat reader\9.0\collab\cemaildistribution
   Opens kev:
                                                HKCU\software\adobe\acrobat
reader\9.0\collab\cemaildistribution\csettings
   Opens key:
                                                HKCU\software\adobe\acrobat
reader\9.0\collab\cinitiationwizardfirstlaunch
   Opens key:
                                                HKCU\software\adobe\acrobat reader\9.0\collab\cserversettings
   Opens key:
                                                HKCU\software\adobe\acrobat reader\9.0\installer
   Opens key:
                                                HKCU\software\adobe\acrobat reader\9.0\installer\migrated
   Opens key:
                                                \label{lem:hkcu} \verb+KKCU \software \adobe \acrobat reader \9.0 \nstall path
   Opens key:
                                                HKCU\software\adobe\acrobat reader\9.0\language
   Opens key:
                                                HKCU\software\adobe\acrobat reader\9.0\language\current
   Opens key:
                                                HKCU\software\adobe\acrobat reader\9.0\language\next
   Opens key:
                                                HKCU\software\adobe\acrobat reader\9.0\multimedia
   Opens key:
                                                HKCU\software\adobe\acrobat reader\9.0\multimedia\ccolorandborder
   Opens kev:
                                                HKCU\software\adobe\acrobat reader\9.0\originals
   Opens key:
                                                HKCU\software\adobe\acrobat reader\9.0\prefsdialog
   Opens kev:
                                                HKCU\software\adobe\acrobat reader\9.0\sdi
   Opens key:
                                                HKCU \ software \ adobe\ acrobat\ reader \ \ 9.0 \ selection
   Opens key:
                                                HKCU\software\adobe\acrobat reader\9.0\usagemeasurement
   Opens key:
                                                HKCU\software\adobe\adobe acrobat
   Opens key:
                                                HKCU\software\adobe\adobe acrobat\9.0
                                                HKCU\software\adobe\adobe acrobat\9.0\diskcabs
   Opens kev:
   Opens key:
                                                HKCU\software\adobe\adobe arm
   Opens key:
                                                HKCU\software\adobe\adobe arm\1.0
                                                HKCU\software\adobe\adobe arm\1.0\arm
   Opens kev:
   Opens key:
                                                HKCU\software\adobe\adobe synchronizer
                                                HKCU\software\adobe\adobe synchronizer\9.0
   Opens key:
                                                HKCU\software\adobe\adobe synchronizer\9.0\acrobat.com
   Opens key:
   Opens key:
                                                HKCU\software\adobe\commonfiles
   Opens key:
                                                HKCU\software\adobe\commonfiles\usage
                                                HKCU\software\adobe\commonfiles\usage\reader 9
   Opens key:
   Opens key:
                                                HKCU\software\appdatalow
   Opens key:
                                                HKCU\software\appdatalow\software
   Opens key:
                                                HKCU\software\appdatalow\software\microsoft
   Opens kev:
                                                HKCU\software\appdatalow\software\microsoft\internet explorer
   Opens key:
                                                HKCU\software\appdatalow\software\microsoft\internet explorer\security
                                                HKCU\software\appdatalow\software\microsoft\internet
   Opens kev:
explorer\security\antiphishing
   Opens key:
                                                HKCU\software\javasoft
   Opens key:
                                                HKCU\software\javasoft\java update
   Opens key:
                                                HKCU\software\javasoft\java update\policy
                                                HKCU\software\javasoft\java update\policy\javafx
   Opens key:
   Opens key:
                                                HKCU\software\macromedia
   Opens key:
                                                HKCU\software\macromedia\flashplayer
   Opens kev:
                                                HKCU\software\microsoft
   Opens key:
                                                HKCU\software\microsoft\active setup
   Opens key:
                                                HKCU\software\microsoft\active setup\declined install on demand iev5
   Opens key:
                                                HKCU\software\microsoft\active setup\installed components
   Opens key:
                                                HKCU\software\microsoft\active setup\installed components\>{26923b43-
4d38-484f-9b9e-de460746276c}
   Opens key:
                                                HKCU\software\microsoft\active setup\installed components\>{60b49e34-
c7cc-11d0-8953-00a0c90347ff}
   Opens key:
                                                HKCU\software\microsoft\active setup\installed components\{2c7339cf-
2b09-4501-b3f3-f3508c9228ed}
                                                HKCU\software\microsoft\active setup\installed components\{44bba840-
   Opens kev:
cc51-11cf-aafa-00aa00b6015c}
                                                \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{$microsoft$ active setup$ installed components$ \end{tabular} $$ $$ $46652a52-4000 $$$ $46652a52-4000 $$$$ $46652a52-4000 $$$$ $46652a52-4000 $$$ $46652a52-4000 $$$$ $46652a52-4000 $$$$ $46652a52-4000 $$$$ $46652a52-4000 $$$$ $46652a52-40000 $$$$ $46652a52-40000 $$$$ $46652a52-40000 $$$$ $46652a52-40000 $$$$ $46652a52-40000 $$$$ $466
   Opens key:
394a-11d3-b153-00c04f79faa6}
   Opens key:
                                                HKCU\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4340}
   Opens kev:
                                                HKCU\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4383}
   Opens key:
                                                HKCU\software\microsoft\active setup\installed components\{89b4c1cd-
b018-4511-b0a1-5476dbf70820}
   Opens key:
                                                HKCU\software\microsoft\activemovie
                                                HKCU\software\microsoft\activemovie\devenum 64-bit
   Opens kev:
   Opens key:
                                                HKCU\software\microsoft\activemovie\devenum 64-bit\{4efe2452-168a-11d1-
bc76-00c04fb9453b}
                                                HKCU\software\microsoft\activemovie\devenum 64-bit\{4efe2452-168a-11d1-
   Opens key:
bc76-00c04fb9453b}\default midiout device
                                                HKCU\software\microsoft\activemovie\devenum 64-bit\{e0f158e1-cb04-11d0-
   Opens key:
bd4e-00a0c911ce86}
   Opens key:
                                                HKCU\software\microsoft\activemovie\devenum 64-bit\{e0f158e1-cb04-11d0-
bd4e-00a0c911ce86}\default directsound device
   Opens key:
                                                HKCU\software\microsoft\assistance
                                                HKCU\software\microsoft\assistance\client
   Opens kev:
   Opens key:
                                                HKCU\software\microsoft\assistance\client\1.0
   Opens key:
                                                HKCU\software\microsoft\assistance\client\1.0\settings
   Opens key:
                                                HKCU\software\microsoft\command processor
                                                HKCU\software\microsoft\ctf
   Opens key:
                                                HKCU\software\microsoft\ctf\assemblies
   Opens key:
   Opens key:
                                                HKCU \setminus software \setminus microsoft \setminus ctf \setminus assemblies \setminus 0x00000409
   Opens key:
                                                HKCU \setminus software \setminus microsoft \setminus ctf \setminus ssemblies \setminus 0x00000409 \setminus \{34745c63-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f0-4784-b2f
8b67-5e12c8701a31}
   Opens key:
                                                HKCU\software\microsoft\ctf\directswitchhotkevs
                                                HKCU\software\microsoft\ctf\hiddendummylayouts
   Opens key:
```

Opens key: HKCU\software\microsoft\ctf\sortorder\language
Opens key: HKCU\software\microsoft\ctf\tip

HKCU\software\microsoft\ctf\msutb

HKCU\software\microsoft\ctf\sortorder

Opens key:

Opens key: HKCU\software\microsoft\direct3d

Opens key: HKCU\software\microsoft\direct3d\mostrecentapplication

Opens key: HKCU\software\microsoft\eventsystem

Opens key: HKCU\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-

00805fc79216}

Opens key: HKCU\software\microsoft\fax

Opens key: HKCU\software\microsoft\fax\fxsclnt\archive
Opens key: HKCU\software\microsoft\fax\fxsclnt\confirm

Opens key: HKCU\software\microsoft\fax\setup
Opens key: HKCU\software\microsoft\fax\userinfo
Opens key: HKCU\software\microsoft\feeds
Opens key: HKCU\software\microsoft\ftp
Opens key: HKCU\software\microsoft\gdiplus
Opens key: HKCU\software\microsoft\jam
Opens key: HKCU\software\microsoft\jam
Opens key: HKCU\software\microsoft\jam

Opens key: HKCU\software\microsoft\iam\accounts\active directory gc

Opens key: HKCU\software\microsoft\iam\accounts\active directory gc\windows mail

account id

Opens key:

Opens key:

Opens key:

Opens key: HKCU\software\microsoft\iam\accounts\verisign

Opens key: HKCU\software\microsoft\iam\accounts\verisign\windows mail account id

Opens key: HKCU\software\microsoft\ime
Opens key: HKCU\software\microsoft\ime\imesc
Opens key: HKCU\software\microsoft\ime\imesc\5.0
Opens key: HKCU\software\microsoft\imejp
Opens key: HKCU\software\microsoft\imejp\10.0

Opens key: HKCU\software\microsoft\imejp\10.0\dictionaries
Opens key: HKCU\software\microsoft\imejp\10.0\manage
Opens key: HKCU\software\microsoft\imejp\10.0\msime

Opens key: HKCU\software\microsoft\imejp\10.0\msime\autocharwidth

Opens key: HKCU\software\microsoft\imejp\10.0\romadef Opens key: HKCU\software\microsoft\imejp\10.0\romadef\ms-ime Opens key: HKCU\software\microsoft\imejp\10.0\stylelist Opens key: HKCU\software\microsoft\imejp\10.0\stylelist\atok Opens key: $HKCU \setminus software \setminus microsoft \setminus imejp \setminus 10.0 \setminus stylelist \setminus atok \setminus color$ Opens key: HKCU\software\microsoft\imejp\10.0\stylelist\ms-ime2000 Opens key: $HKCU \ software \ microsoft \ imejp \ 10.0 \ stylelist \ ms-ime2000 \ color \ mathematical and the software \ microsoft \ mejp \ mathematical and the software \ microsoft \ mejp \ mathematical and the software \ microsoft \ mejp \ mathematical and the software \ microsoft \ mejp \ mathematical and the software \ microsoft \ mejp \ mathematical and the software \ microsoft \ mejp \ mathematical and the software \ microsoft \ mejp \ mathematical and the software \ microsoft \ mejp \ mathematical and the software \ microsoft \ mejp \ mathematical and the software \ microsoft \ mejp \ mathematical and the software \ microsoft \ mejp \ mathematical and the software \ microsoft \ mejp \ mathematical \ mejp \ mejp \ mathematical \ mejp \ mejp \ mejp \ mejp \ mathematical \ mejp \$ Opens key: HKCU\software\microsoft\imejp\10.0\stylelist\natural

Opens key: HKCU\software\microsoft\imejp\10.0\stylelist\natural\color Opens key: HKCU\software\microsoft\imejp\10.0\stylelist\vje
Opens key: HKCU\software\microsoft\imejp\10.0\stylelist\vje\color Opens key: HKCU\software\microsoft\imejp\10.0\stylelist\wx
Opens key: HKCU\software\microsoft\imejp\10.0\stylelist\wx
Opens key: HKCU\software\microsoft\imejp\10.0\stylelist\wx\color Opens key: HKCU\software\microsoft\imejp\10.0\window

Opens key: HKCU\software\microsoft\imejp\10.0\window

Opens key: HKCU\software\microsoft\imejp\10.0\window\pltsmall

Opens key: HKCU\software\microsoft\imejp\10.0\window\plttiny
Opens key: HKCU\software\microsoft\imejp\10.1
Opens key: HKCU\software\microsoft\imejp\10.1
HKCU\software\microsoft\internet connection wizard

Opens key: HKCU\software\microsoft\internet explorer

Opens key: HKCU\software\microsoft\internet explorer\browseremulation
Opens key: HKCU\software\microsoft\internet explorer\browseremulation\lowmic

Opens key: HKCU\software\microsoft\internet explorer\caretbrowsing
Opens key: HKCU\software\microsoft\internet explorer\desktop

Opens key: HKCU\software\microsoft\internet explorer\desktop\general
Opens key: HKCU\software\microsoft\internet explorer\desktop\general
Opens key: HKCU\software\microsoft\internet explorer\domstorage
Opens key: HKCU\software\microsoft\internet explorer\domstorage
Opens key: HKCU\software\microsoft\internet explorer\domstorage\total

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

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

Opens key: HKCU\software\microsoft\internet explorer\help_menu_icrosoft\internet explorer\help_menu_urls

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

Opens key: HKCU\software\microsoft\internet explorer\ietlu\lowmic
Opens key: HKCU\software\microsoft\internet explorer\ietlu\lowmic
Opens key: HKCU\software\microsoft\internet explorer\interliforms
Opens key: HKCU\software\microsoft\internet explorer\international

Opens key: HKCU\software\microsoft\internet explorer\international\scripts Opens key: HKCU\software\microsoft\internet explorer\international\scripts\10 $HKCU \ software \ microsoft \ internet\ explorer \ international \ scripts \ \ 11$ Opens key: Opens key: Opens key: HKCU\software\microsoft\internet explorer\international\scripts\13 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\14 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\15 HKCU\software\microsoft\internet explorer\international\scripts\16 Opens key: Opens key: HKCU\software\microsoft\internet explorer\international\scripts\17 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\18 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\19 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\20 HKCU\software\microsoft\internet explorer\international\scripts\21 Opens key: Opens key: Opens key: HKCU\software\microsoft\internet explorer\international\scripts\23 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\24 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\25 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\26 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\27 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\28 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\29 Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3 $\label{local-condition} \mbox{HKCU\software\mbox{\sc internet explorer\international\sc ripts\sc 30}} \\$ Opens key:

 $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc ripts\34}} \\$

HKCU\software\microsoft\internet explorer\international\scripts\35

HKCU\software\microsoft\internet explorer\international\scripts\37

```
Opens key:
                                                     HKCU\software\microsoft\internet explorer\international\scripts\38
    Opens key:
                                                     HKCU\software\microsoft\internet explorer\international\scripts\39
                                                     HKCU\software\microsoft\internet explorer\international\scripts\4
    Opens key:
                                                     HKCU\software\microsoft\internet explorer\international\scripts\5
   Opens key:
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\international\scripts\6
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\international\scripts\7
                                                     HKCU\software\microsoft\internet explorer\international\scripts\8
   Opens kev:
                                                    HKCU\software\microsoft\internet explorer\international\scripts\9
   Opens key:
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\internetregistry
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\linksbar
   Opens key:
                                                     \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\linksbar\itemcache}} \\
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\linksbar\itemcache\0
                                                     HKCU\software\microsoft\internet explorer\linksbar\itemcache\1
   Opens key:
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\lowregistry
                                                    HKCU\software\microsoft\internet explorer\lowregistry\domstorage
   Opens kev:
                                                     \label{thm:lower} \begin{tabular}{ll} HKCU \software \microsoft \internet explorer \label{thm:lower} \end{tabular} \begin{tabular}{ll} explorer \software \microsoft \internet explorer \software \microsoft \m
   Opens key:
   Opens kev:
                                                    HKCU\software\microsoft\internet
explorer\lowregistry\dontshowmethisdialogagain
                                                    HKCU\software\microsoft\internet explorer\lowregistry\shell extensions
   Opens key:
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\lowregistry\shell
extensions\cached
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\main
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\main\default feeds
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\main\default feeds\{5adc2714-
2975-4245-b68a-3721298c1e70}
   Opens key:
                                                    50c0-4a2a-b9a6-951f2355feb2}
                                                    Opens key:
e349-461a-b4f5-b4674114d3a6}
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\main\featurecontrol
                                                    HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
   Opens key:
                                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown\settings
   Opens kev:
                                                    HKCU\software\microsoft\internet explorer\main\windowssearch
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\new windows
                                                    HKCU\software\microsoft\internet explorer\pagesetup
   Opens key:
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\phishingfilter
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\privacy
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\recovery
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\recovery\active
                                                     HKCU\software\microsoft\internet explorer\recovery\adminactive
   Opens key:
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\searchscopes
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\searchurl
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\security
                                                    HKCU\software\microsoft\internet explorer\security\antiphishing
   Opens key:
   Opens key:
                                                    HKCU\software\microsoft\internet
explorer\security\antiphishing\2cedbfbc-dba8-43aa-b1fd-cc8e6316e3e2
                                                    HKCU\software\microsoft\internet explorer\services
   Opens kev:
                                                     HKCU\software\microsoft\internet explorer\settings
   Opens key:
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\setup
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\sqm
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\suggested sites
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\tabbedbrowsing
                                                    HKCU\software\microsoft\internet explorer\toolbar
   Opens key:
                                                     \label{lem:hkcu} \mbox{HKCU\software\mbox{$\mbox{microsoft\internet explorer\toolbar\shellbrowser}} \\
   Opens key:
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\toolbar\webbrowser
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\typedurls
   Opens key:
                                                    HKCU\software\microsoft\internet explorer\urlsearchhooks
                                                     HKCU\software\microsoft\internet explorer\user preferences
   Opens key:
   Opens key:
                                                     HKCU\software\microsoft\internet explorer\zoom
   Opens key:
                                                     HKCU\software\microsoft\java vm
   Opens key:
                                                     HKCU\software\microsoft\keyboard
                                                    HKCU\software\microsoft\keyboard\native media players
   Opens key:
                                                     HKCU\software\microsoft\keyboard\native media players\wmp
   Opens key:
   Opens key:
                                                    HKCU\software\microsoft\mediaplayer
   Opens key:
                                                     HKCU\software\microsoft\mediaplayer\health
   Opens key:
                                                    HKCU\software\microsoft\mediaplayer\player
   Opens key:
                                                     HKCU\software\microsoft\mediaplayer\player\settings
   Opens key:
                                                     HKCU\software\microsoft\mediaplayer\player\tasks
                                                     HKCU\software\microsoft\mediaplayer\player\tasks\nowplaying
   Opens key:
   Opens key:
                                                     HKCU\software\microsoft\mediaplayer\preferences
   Opens key:
                                                    HKCU\software\microsoft\mediaplayer\preferences\hme
                                                     \label{local-operator} \begin{tabular}{ll} HKCU \software \mbox{$\stackrel{\cdot}{m}$ crosoft \mbox{$\cdot$ ediaplayer \preferences \proxysettings} \end{tabular}
   Opens kev:
                                                    \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc mediaplayer\preferences\proxysettings\http}} \label{lem:hkcu}
   Opens key:
   Opens key:
                                                    \label{lem:hkcu} \verb+KCU\software\microsoft\mediaplayer\preferences\proxysettings\normalfootnotes and the lemma of the lem
   Opens key:
                                                    HKCU\software\microsoft\mediaplayer\setup
   Opens key:
                                                     HKCU\software\microsoft\mediaplayer\setup\createdlinks
   Opens key:
                                                     HKCU\software\microsoft\microsoft management console
   Opens key:
                                                     HKCU\software\microsoft\microsoft management console\recent file list
   Opens key:
                                                     HKCU\software\microsoft\microsoft management console\settings
   Opens key:
                                                     HKCU\software\microsoft\ms design tools
   Opens key:
                                                     HKCU\software\microsoft\ms design tools\mdtdbd
                                                    HKCU\software\microsoft\msdaipp
   Opens key:
   Opens key:
                                                    {\tt HKCU \ } software \verb|\ microsoft \verb|\ msdaipp \verb|\ providers 
   Opens key:
                                                    HKCU \setminus software \setminus microsoft \setminus msdaipp \setminus providers \setminus \{9fecd 570 - b9d 4 - 11d 1 - 9c78 - b9d 4 - b9
0000f875ac61}
    Opens key:
                                                     HKCU\software\microsoft\msdaipp\providers\{9fecd571-b9d4-11d1-9c78-
```

```
0000f875ac61}
                                                                     HKCU\software\microsoft\msf
     Opens kev:
                                                                     HKCU\software\microsoft\msf\registration
     Opens key:
                                                                     HKCU\software\microsoft\msf\registration\listen
    Opens key:
    Opens key:
                                                                     HKCU\software\microsoft\multimedia
    Opens key:
                                                                    HKCU\software\microsoft\multimedia\activemovie
    Opens kev:
                                                                     HKCU\software\microsoft\multimedia\activemovie\filter cache64
                                                                    HKCU\software\microsoft\notepad
    Opens key:
    Opens key:
                                                                    HKCU\software\microsoft\office
    Opens key:
                                                                    HKCU\software\microsoft\office\11.0
    Opens key:
                                                                     HKCU\software\microsoft\office\11.0\common
    Opens key:
                                                                    HKCU\software\microsoft\office\11.0\common\drawalerts
                                                                     HKCU \ software \ microsoft \ office \ 11.0 \ common \ drawalerts \ ftp \ sites
    Opens key:
    Opens key:
                                                                     HKCU\software\microsoft\office\11.0\common\dspadaptermru
                                                                    HKCU\software\microsoft\office\11.0\common\general
    Opens kev:
                                                                     HKCU\software\microsoft\office\11.0\common\languageresources
    Opens key:
                                                                    HKCU\software\microsoft\office\11.0\common\migration
    Opens kev:
                                                                     HKCU\software\microsoft\office\11.0\common\migration\office
    Opens key:
    Opens key:
                                                                    HKCU\software\microsoft\office\11.0\common\migration\word
    Opens key:
                                                                    HKCU\software\microsoft\office\11.0\common\open find
    Opens key:
                                                                    HKCU\software\microsoft\office\11.0\common\open find\microsoft office
word
    Opens key:
                                                                     HKCU\software\microsoft\office\11.0\common\open find\places
    Opens key:
                                                                    HKCU\software\microsoft\office\11.0\common\research
                                                                     HKCU\software\microsoft\office\11.0\common\research\translation
    Opens kev:
    Opens key:
                                                                    HKCU\software\microsoft\office\11.0\common\toolbars
                                                                     HKCU\software\microsoft\office\11.0\common\toolbars\settings
    Opens key:
                                                                    HKCU\software\microsoft\office\11.0\common\userinfo
    Opens key:
    Opens key:
                                                                     Opens key:
                                                                    HKCU\software\microsoft\office\11.0\word\options
    Opens key:
                                                                     HKCU\software\microsoft\office\11.0\word\userinfo
    Opens key:
                                                                    HKCU\software\microsoft\office\11.0\word\wizards
    Opens key:
                                                                    HKCU\software\microsoft\office\11.0\wordview
    Opens key:
                                                                     HKCU\software\microsoft\office\11.0\wordview\data
    Opens key:
                                                                     HKCU\software\microsoft\office\12.0
    Opens key:
                                                                     HKCU\software\microsoft\office\12.0\common
                                                                    HKCU\software\microsoft\office\12.0\common\drawalerts
    Opens key:
    Opens key:
                                                                    HKCU\software\microsoft\office\12.0\common\drawalerts\ftp sites
    Opens key:
                                                                    HKCU\software\microsoft\office\12.0\common\general
    Opens key:
                                                                    HKCU\software\microsoft\office\12.0\common\languageresources
    Opens key:
HKCU\software\microsoft\office\12.0\common\languageresources\enabledlanguages
    Opens key:
                                                                    HKCU\software\microsoft\office\12.0\common\migration
    Opens key:
                                                                    HKCU\software\microsoft\office\12.0\common\migration\excel
    Opens key:
                                                                    HKCU\software\microsoft\office\12.0\common\migration\office
    Opens key:
                                                                    HKCU\software\microsoft\office\12.0\common\open find
    Opens key:
                                                                     HKCU\software\microsoft\office\12.0\common\open find\microsoft office
excel viewer
    Opens key:
                                                                    HKCU \ software \ microsoft \ office \ 12.0 \ common \ research
    Opens key:
                                                                    HKCU \setminus software \setminus microsoft \setminus office \setminus 12.0 \setminus common \setminus research \setminus translation
    Opens key:
                                                                     HKCU\software\microsoft\office\12.0\excel
                                                                     HKCU\software\microsoft\office\12.0\excel\options
    Opens key:
    Opens key:
                                                                     HKCU\software\microsoft\office\12.0\excel viewer
    Opens key:
                                                                     HKCU\software\microsoft\office\12.0\excel viewer\viewer options
    Opens key:
                                                                    HKCU\software\microsoft\office\12.0\user settings
                                                                    Opens key:
                                                                    HKCU\software\microsoft\office\12.0\user settings\mso_intl
    Opens key:
                                                                    HKCU\software\microsoft\office\12.0\user settings\powerpoint_intl
    Opens key:
    Opens key:
                                                                    HKCU\software\microsoft\office\14.0
    Opens key:
                                                                     HKCU\software\microsoft\office\14.0\common
    Opens key:
                                                                    HKCU\software\microsoft\office\14.0\common\drawalerts
                                                                     HKCU \ software \ microsoft \ office \ 14.0 \ common \ drawalerts \ ftp \ sites
    Opens key:
    Opens key:
                                                                     HKCU\software\microsoft\office\14.0\common\general
    Opens key:
                                                                     HKCU\software\microsoft\office\14.0\common\languageresources
    Opens key:
\label{thm:languageresources} \begin{tabular}{ll} HKCU \software \microsoft \office \14.0 \common \languageresources \end to \common \cite{Allow} and \cite{A
                                                                    HKCU\software\microsoft\office\14.0\common\open find
    Opens key:
    Opens key:
                                                                    HKCU\software\microsoft\office\14.0\common\open find\microsoft
powerpoint viewer
     Opens key:
                                                                     Opens key:
                                                                     HKCU\software\microsoft\office\14.0\common\research\translation
                                                                     HKCU\software\microsoft\office\14.0\powerpoint
    Opens key:
    Opens key:
                                                                     HKCU\software\microsoft\office\14.0\powerpoint viewer
                                                                     HKCU\software\microsoft\office\14.0\powerpoint viewer\options
    Opens key:
    Opens key:
                                                                    HKCU\software\microsoft\office\common
    Opens kev:
                                                                     HKCU\software\microsoft\office\common\offdiag
    Opens key:
                                                                    HKCU\software\microsoft\office\common\smart tag
    Opens key:
                                                                    HKCU\software\microsoft\office\common\smart tag\actions
    Opens key:
                                                                    HKCU\software\microsoft\office\common\smart tag\actions\{339361cd-6723-
455d-a40b-c95f1f91ff8a}
                                                                     \label{thm:local_hammon} \begin{tabular}{ll} HKCU \software \microsoft \software \common \small tag \actions \end{tabular} \begin{tabular}{ll} 49df 3409 - 46b 3 - 4
    Opens key:
4b0c-b7bf-fec0f9401edd}
    Opens key:
                                                                    HKCU\software\microsoft\office\common\smart tag\actions\{64ab6c69-b40e-
40af-9b7f-f5687b48e2b6}
                                                                    \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \office \common \small tag \actions \common \common \common \small tag \actions \common \comm
    Opens key:
4085-8cfb-97705b57a98f}
    Opens key:
                                                                    4238-92c9-bbe330af25fd}
    Opens key:
                                                                    HKCU\software\microsoft\office\common\smart tag\recognizers
    Opens key:
                                                                     HKCU \setminus software \setminus microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-microsoft \setminus office \setminus smart \ tag \setminus recognizers \setminus smart \ tag \setminus recognizers \setminus smart \ tag \setminus smart \ tag \setminus recognizers \setminus smart \ tag \setminus recognize \cap smart \ tag \setminus recognizers \setminus smart \ tag \setminus recognize \cap smart \ tag \setminus recognize \cap smart \ t
```

```
b40e-40af-9b7f-f5687b48e2b6}
                          HKCU\software\microsoft\office\common\smart tag\recognizers\{87ef1cfe-
  Opens key:
51ca-4e6b-8c76-e576aa926888}
 Opens key:
                          HKCU\software\microsoft\office\common\userinfo
 Opens key:
                          HKCU\software\microsoft\peernet
                          HKCU\software\microsoft\peernet\event config
 Opens key:
                          HKCU\software\microsoft\protected storage system provider
 Opens key:
                          HKCU\software\microsoft\protected storage system provider\s-1-5-21-
 Opens key:
980053277-1733835069-2361817685-1001
                          HKCU\software\microsoft\ras autodial
 Opens key:
 Opens key:
                          HKCU\software\microsoft\ras autodial\default
 Opens key:
                          HKCU\software\microsoft\remote assistance
 Opens key:
                          HKCU\software\microsoft\shared
 Opens key:
                          HKCU\software\microsoft\shared tools
 Opens key:
                          HKCU\software\microsoft\shared tools\font mapping
                          HKCU\software\microsoft\shared tools\proofing tools
 Opens key:
                          HKCU\software\microsoft\shared tools\proofing tools\custom dictionaries
 Opens kev:
 Opens key:
                          HKCU\software\microsoft\sideshow
                          HKCU\software\microsoft\sideshow\gadgets
 Opens key:
 Opens key:
                          HKCU\software\microsoft\speech
 Opens key:
                          HKCU\software\microsoft\speech\preferences
 Opens key:
                          HKCU\software\microsoft\speech\preferences\appcompatdisabledictation
 Opens key:
                          HKCU\software\microsoft\speech\preferences\appcompatdisablemsaa
 Opens key:
                          HKCU\software\microsoft\sqmclient
 Opens key:
                          HKCU\software\microsoft\systemcertificates
 Opens key:
                          HKCU\software\microsoft\systemcertificates\ca
                          HKCU\software\microsoft\systemcertificates\ca\certificates
 Opens kev:
 Opens key:
                          HKCU\software\microsoft\systemcertificates\ca\crls
 Opens key:
                          {\tt HKCU \setminus software \setminus microsoft \setminus system certificates \setminus ca \setminus ctls}
 Opens key:
                          HKCU\software\microsoft\systemcertificates\disallowed
 Opens key:
                          HKCU\software\microsoft\systemcertificates\disallowed\certificates
 Opens key:
                          HKCU\software\microsoft\systemcertificates\disallowed\crls
 Opens key:
                          HKCU\software\microsoft\systemcertificates\disallowed\ctls
 Opens key:
                          HKCU\software\microsoft\systemcertificates\my
 Opens key:
                          HKCU\software\microsoft\systemcertificates\root
 Opens key:
                          HKCU\software\microsoft\systemcertificates\root\certificates
 Opens key:
                          HKCU\software\microsoft\systemcertificates\root\crls
 Opens key:
                          HKCU\software\microsoft\systemcertificates\root\ctls
 Opens key:
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \system certificates \noot \protected roots
 Opens key:
                          HKCU\software\microsoft\systemcertificates\smartcardroot
 Opens key:
                          HKCU\software\microsoft\systemcertificates\smartcardroot\certificates
                          HKCU\software\microsoft\systemcertificates\smartcardroot\crls
 Opens key:
 Opens key:
                          HKCU\software\microsoft\systemcertificates\smartcardroot\ctls
 Opens key:
                          HKCU\software\microsoft\systemcertificates\trust
 Opens key:
                          HKCU\software\microsoft\systemcertificates\trust\certificates
 Opens key:
                          HKCU\software\microsoft\systemcertificates\trust\crls
                          HKCU\software\microsoft\systemcertificates\trust\ctls
 Opens key:
 Opens key:
                          HKCU\software\microsoft\systemcertificates\trustedpeople
 Opens key:
                          Opens key:
                          HKCU\software\microsoft\systemcertificates\trustedpeople\crls
 Opens key:
                          HKCU\software\microsoft\systemcertificates\trustedpeople\ctls
 Opens key:
                          HKCU\software\microsoft\systemcertificates\trustedpublisher
                          HKCU\software\microsoft\systemcertificates\trustedpublisher\certificates
 Opens key:
 Opens key:
                          HKCU\software\microsoft\systemcertificates\trustedpublisher\crls
 Opens key:
                          HKCU\software\microsoft\systemcertificates\trustedpublisher\ctls
                          HKCU\software\microsoft\wab
 Opens key
 Opens key:
                          HKCU\software\microsoft\wab\me
                          HKCU\software\microsoft\wab\wab4
 Opens key:
 Opens key:
                          HKCU\software\microsoft\wab\wab4\wab file name
 Opens key:
                          HKCU\software\microsoft\wfs
 Opens key:
                          HKCU\software\microsoft\wfs\draftsview
                          HKCU\software\microsoft\wfs\inboxview
 Opens key:
 Opens key:
                          HKCU\software\microsoft\wfs\incomingview
 Opens key:
                          HKCU\software\microsoft\wfs\outboxview
 Opens key:
                          HKCU\software\microsoft\wfs\sentitemsview
                          HKCU\software\microsoft\windows
 Opens key:
                          HKCU\software\microsoft\windows\currentversion
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\action center
 Opens key:
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\action center\checks
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
 Opens key:
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101
                          HKCU\software\microsoft\windows\currentversion\action
 Opens kev:
center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101
                          HKCU\software\microsoft\windows\currentversion\action
 Opens key:
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.100
 Opens key:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101
                          HKCU\software\microsoft\windows\currentversion\action
 Opens key:
center\checks\{945a8954-c147-4acd-923f-40c45405a658\}.check.42
 Opens key:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\action
center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4\}.check.0
```

HKCU\software\microsoft\windows\currentversion\action

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

HKCU\software\microsoft\windows\currentversion\action

center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100

center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100

Opens key:

Opens key:

```
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101
                                                                                              HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102
     Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103
                                                                                             HKCU\software\microsoft\windows\currentversion\action
     Opens key:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104
                                                                                             \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
     Opens key:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106
      Opens key:
                                                                                             \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action center\+ providers
      Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\app paths
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\app paths\pythonwin.exe
     Opens kev:
                                                                                             HKCU\software\microsoft\windows\currentversion\applets
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\applets\regedit
                                                                                             HKCU\software\microsoft\windows\currentversion\applets\systray
     Opens kev:
                                                                                              \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ explorer and the software explorer and the so
      Opens key:
     Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\advanced
      Opens key:
\label{thm:local_hammon} \begin{tabular}{l} HKCU \software \verb|\microsoft| windows \current version \explorer \application destinations \end{tabular}
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
       Opens kev:
      Opens key:
                                                                                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\autoplay} handlers \\
      Opens key:
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\bitbucket
      Opens key:
      Opens key:
                                                                                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\bitbucket\volume}} \\
      Opens key:
                                                                                             HKCU \ software \ microsoft \ windows \ current version \ explorer \ cabinet state
      Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\cd burning
      Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\cd
burning\drives
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\cd
burning\staginginfo
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\cidopen
      Opens key:
                                                                                             \label{thm:linear} \mbox{HKCU\software\mbox{\sc urrentversion\explorer\cidopen\mbodules}} \label{thm:linear}
      Opens key:
     Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\cidsave
     Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\cidsave\modules
      Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\clsid
      Opens key:
                                                                                             HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-theoryte \} + theoryte \setminus foreign \setminus for
3aea-1069-a2d8-08002b30309d}
      Opens key:
                                                                                             HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (59031a47-b) + (59031a47-
3f72-44a7-89c5-5595fe6b30ee}
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\clsid\{645ff040-
     Opens kev:
5081-101b-9f08-00aa002f954e}
      Opens key:
                                                                                             HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (871c5380-64) + (871c53
42a0-1069-a2ea-08002b30309d}
     Opens key:
                                                                                             be21-4350-88b0-7367fc96ef3c}
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\comdlg32
      Opens kev:
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\cidsizemru
     Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\firstfolder
      Onens key:
\label{thm:local_hamma} \begin{tabular}{ll} HKCU \software \verb|microsoft| windows \current version \explorer \comdlg 32 \last visited pidlmrus \comdlg 32 \last visited pidlmrus \comdlg 32 \comdlg 32
     Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\opensavepidlmru
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\controlpanel
       Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\discardable
      Opens kev:
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\discardable\postsetup
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts
     Opens key:
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.3g2
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.3gp
     Opens kev:
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.3gp2
     Opens key:
                                                                                             \label{lem:hkcu} \verb+KCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+ file exts \verb+ .3gpp+ \\
      Opens key:
                                                                                              \label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\fileexts|.aac | file exts|.aac | fil
      Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.adt
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.adts
      Opens kev:
      Opens key:
                                                                                              \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.aif}
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.aifc
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.aiff
      Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.asf
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.asx
      Opens kev:
     Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.au
      Opens key:
                                                                                              \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\.avi}} \mbox{\tt avi}
      Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.bmp
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.cab
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.contact
      Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.css
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dib
      Opens kev:
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dll
     Opens key:
                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.doc
      Opens key:
                                                                                             \label{lem:hkcu} \verb+KCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+fileexts \verb+.docm+ \\
      Opens key:
                                                                                             \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \file exts \cdots \end{tabular}. docx \end{tabular}
      Opens key:
                                                                                             \label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\fileexts|.dot | for the constraint of the constrai
                                                                                              Opens key:
```

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dvr-ms HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dwfx Opens kev: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.easmx Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.edrwx Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.emf Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.eprtx Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.fon Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.gif Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\fileexts|. htm \\ \end{tabular}$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ico Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ini Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.jfif Opens kev: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ipe Opens key: HKCU\software\microsoft\windows\currentyersion\explorer\fileexts\.ipeg Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.jpg Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.jtx Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.lnk Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m1v Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m2t HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m2ts Opens kev: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m2v Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m3u HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m4a Opens kev: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m4v HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mht Opens kev: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mhtml Opens key: $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+currentversion \verb+explorer \verb+fileexts \verb+.mid+ \\$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.midi HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mod Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mov Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp2 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp2v Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp3 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp4 HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp4v Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpa Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.mpe} \\$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpeg Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpg Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpv2 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.msc Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mts Opens kev: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ocx Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.odt Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.otf Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.png Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\fileexts|.pot | fileexts|.pot | file$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.potm Opens kev: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.potx Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ppsm Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ppsx Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ppt Opens kev: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.pptm Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.pptx Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ps1xml Opens key: $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+fileexts \verb+.. rle+ \\$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.rmi Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.rtf HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.scf Opens kev: Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.search-ms

HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.snd Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.sys Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.tif Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.tiff Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ts Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|microsoft| windows \verb|currentversion| explorer \verb|fileexts||.ttc| \\ \end{tabular}$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ttf HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.tts Opens kev: Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.txt}$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wav Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wax Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wdp Opens kev: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wm Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wma Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\.wmf}}$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wmv HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wmx Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wpl Opens key: $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc urrentversion\explorer\fileexts\.wtv}} \mbox{\sc urrentversion\explorer\fileexts\.wtv} \mbox{\sc urrentversion\explorer\fileexts\.wtv} \mbox{\sc urrentversion\explorer\exp$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wvx Opens kev: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlam Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xls Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlsb Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ fileexts\+ .xlsm$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlsx Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\fileexts|.xlt| \\ \end{tabular}$ HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xltm Opens key:

```
Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xltx
       Opens key:
                                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xml
       Opens key:
                                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xps
       Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xsl
      Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.zip
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\directorv
       Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\lowregistry
       Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\menuorder
      Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus menuor der \setminus favorites
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\modules
        Opens kev:
       Opens key:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \modules \common places \end{tabular}
      Opens kev:
\label{thm:linear} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\mbox{\tt modules\globalsettings}} \\
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\modules\navpane
       Opens kev:
      Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2
      Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc
      Opens key:
\label{thm:local_explorer_mount} HKCU \software \mbox{$\mbox{8063a3d4-8213-11e3-a68e-microsoft}$} \label{thm:local_explorer_mount} HKCU \software \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\
806e6f6e6963}
      Opens key:
806e6f6e6963}
      Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus newshort cut handlers
      Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\recentdocs
       Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\runmru
       Opens key:
                                                                                                             \label{lem:hkcu} \verb+KCU\+software\+microsoft\+windows\+currentversion\+explorer\+searchplatform
       Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\searchplatform\preferences
       Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\shell folders
       Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\startpage
      Opens kev:
HKCU\software\microsoft\windows\currentversion\explorer\startpage\newshortcuts
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\startpage2
      Opens key:
       Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\streams
      Opens key:
                                                                                                             \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \streams \desktop \end{tabular}
      Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\stuckrects2
      Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\taskband
       Opens key:
                                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\typedpaths
       Opens key:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders
       Opens kev:
                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\userassist
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}
       Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ user as sist \ \{f4e57c4b-2036-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-a9ab-45f0-
443bcfe33d9f}
       Opens key:
                                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\visualeffects
      Opens key:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \solin visual effects \animatem in max \end{tabular} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \solin visual effects \animatem in max \end{tabular} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \columnwise \end{tabular} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \columnwise \end{tabular} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \end{tabular} \begin{tabular}{ll} H
      Opens kev:
HKCU \ software \ microsoft \ windows \ \ current version \ \ explorer \ \ visual effects \ \ combobox an imation
      Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus visual effects \setminus control an imations
      Opens key:
HKCU \ software \ microsoft \ windows \ current version \ leaf fects \ cursors hadow \ leaf to the large \ microsoft \ windows \ leaf to the large \ large \ large \ leaf to the large \ lar
       Opens kev:
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dropshadow
       Opens key:
HKCU \ software \ \ microsoft \ \ windows \ \ current version \ \ \ \ visual effects \ \ \ dwmaer opee kenabled
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dwmenabled
       Opens key:
Opens kev:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \soling} \end{tabular} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current \curren
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listboxsmoothscrolling
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewalphaselect
      Opens key:
\label{thm:local_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version} \end{tabular} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows} \end{tabular} \begin{tabular}{ll} HKCU \software \mbox{$
       Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\menuanimation
      Opens key:
\label{thm:local_hammon} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\visualeffects| selection fade | local factor of the local factor of the
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\taskbaranimations
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\themes
       Opens key:
HKCU \ software \ microsoft \ windows \ current version \ lex plorer \ visual effects \ thumb nails or icon \ lex plorer \ visual effects \ thumb nails or icon \ lex plorer \ visual effects \ thumb nails or icon \ lex plorer \ visual effects \ thumb nails or icon \ lex plorer \ visual effects \ thumb nails or icon \ lex plorer \ visual effects \ thumb nails or icon \ lex plorer \ visual effects \ thumb nails or icon \ lex plorer \ visual effects \ thumb nails or icon \ lex plorer \ visual effects \ visual effet \ visual 
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\tooltipanimation
```

Opens key: $HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ \ visual effects \ \ transparent glass$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\wallpapers Opens key: $\label{thm:convex} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \wall papers \colored \end{tabular} \label{thm:convexplorer}$ Opens key: $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \wall papers \known folders \end{tabular}$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1 Opens key: HKCU\software\microsoft\windows\currentversion\ext Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings Opens kev: HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081ce8ad-4283-a596-fa578c2ebdc3} HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-Opens key: a445-435b-bc74-9c25c1c588a9} Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501} Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3} Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{cfbfae00-17a6-11d0-99cb-00c04fd64497} Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus stats \setminus \{dbc80044 - a445 - a455 - a555 -$ 435b-bc74-9c25c1c588a9} Opens kev: HKCU\software\microsoft\windows\currentversion\group policy Opens key: HKCU\software\microsoft\windows\currentversion\group policy\groupmembership Opens key: HKCU\software\microsoft\windows\currentversion\group policy\history Opens key: $\label{lem:hkcu} \verb+KCU\+ software\+ microsoft\+ windows\+ current version\+ group$ policy\policyapplicationstate HKCU\software\microsoft\windows\currentversion\group policy editor Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\group policy editor\admx filter Opens key: HKCU\software\microsoft\windows\currentversion\group policy editor\admx filter.cache HKCU\software\microsoft\windows\currentversion\group policy objects Opens kev: HKCU\software\microsoft\windows\currentversion\group policy Opens kev: objects\{f2660594-63ea-4618-8650-1a5a4fb9ca52}machine Opens key: HKCU\software\microsoft\windows\currentversion\group policy objects\{f2660594-63ea-4618-8650-1a5a4fb9ca52}machine\software Opens key: HKCU\software\microsoft\windows\currentversion\group policy objects\{f2660594-63ea-4618-8650-1a5a4fb9ca52}user Opens key: HKCU\software\microsoft\windows\currentversion\homegroup Opens key: HKCU\software\microsoft\windows\currentversion\homegroup\printers Opens kev: HKCU\software\microsoft\windows\currentversion\homegroup\uistatuscache Opens key: HKCU\software\microsoft\windows\currentversion\ime Opens key: HKCU\software\microsoft\windows\currentversion\ime\imtc70 Opens key: HKCU\software\microsoft\windows\currentversion\ime\imtc70\fuzzyscheme Opens key: HKCU\software\microsoft\windows\currentversion\internet settings Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0 HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\user agent Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\activities Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\activities\blog HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\activities\email Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\activities\map HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\activities\translate Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\cache Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\connections Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\http filters Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\http filters\rpa HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\lockdown zones HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\lockdown_zones\0 Opens key: $\label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ internet$ settings\lockdown_zones\1 HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\2 Opens key: $\label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ internet$ settings\lockdown zones\3 Opens kev: HKCU\software\microsoft\windows\currentversion\internet

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\p3p\history
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\passport

HKCU\software\microsoft\windows\currentversion\internet settings\p3p

settings\lockdown_zones\4

```
Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\passport\lowdamap
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\protocols
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\protocols\mailto
                                      HKCU\software\microsoft\windows\currentversion\internet settings\wpad
   Opens kev:
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\3e-68-f6-0d-2d-0f
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\9e-87-70-29-a3-67
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\wpad\e2-c2-d0-09-69-0f
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\wpad\{4dc0ee17-9725-46c6-9208-9e741c29932a}
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\wpad\{97510e62-091a-49b5-9797-24fe4dde0abc}
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\wpad\{c034e4b5-6859-46ca-b262-e1e2cfd7fcab}
                                      HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\wpad\{f9145a4d-b491-47f1-8afa-50f81461036d}
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zonemap
   Opens kev:
   Opens key:
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft + windows + current version + internet
settings\zonemap\domains
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\escdomains
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
\verb|settings|zonemap|| protocoldefaults||
   Opens key:
                                      \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ internet
settings\zonemap\ranges
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones
   Opens key:
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
   Opens key:
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\mct
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\mct\us
  Opens key:
                                      HKCU \setminus software \setminus microsoft \setminus windows \setminus current \vee ersion \setminus mct \setminus us \setminus link
   Opens key:
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\mbox{\tt mct\us\rssfeed}} \\
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\mct\us\theme
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\mct\us\wallpaper
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\netcache
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\policies
   Opens kev:
                                      HKCU\software\microsoft\windows\currentversion\radar
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\run
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\runonce
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\screensavers
   Opens key:
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\screensavers\bubbles} \\
   Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\bubbles\screen 1
   Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\bubbles\screen 2
                                      HKCU\software\microsoft\windows\currentversion\screensavers\mystify
   Opens key:
   Opens kev:
HKCU\software\microsoft\windows\currentversion\screensavers\mystifv\screen 1
   Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\mystify\screen 2
   Opens key:
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\screensavers\ribbons} \\
   Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\ribbons\screen 1
   Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\ribbons\screen 2
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\screensavers\sstext3d
   Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\sstext3d\screen 1
  Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\sstext3d\screen 2
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\shell extensions
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\shell extensions\cached
                                      HKCU\software\microsoft\windows\currentversion\sidebar
   Opens kev:
   Opens key:
                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \sidebar \settings \end{tabular}
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\telephony
   Opens kev:
\label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\telephony\handoff priorities
  Opens kev:
HKCU\software\microsoft\windows\currentversion\telephony\handoffpriorities\mediamodes
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\thememanager
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\themes
   Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus themes \setminus default visual style of full visual style of the first version \setminus themes \setminus default visual style of full visual style of full visual style of the first version \setminus themes \setminus default visual style of full visual style of
   Opens key:
HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleon
   Opens kev:
                                      HKCU\software\microsoft\windows\currentversion\themes\installedthemes
  Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus themes \setminus mct
   Opens key:
                                      HKCU\software\microsoft\windows\currentversion\wintrust
   Opens key:
                                      \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+wintrust\+trust\+providers
                                      HKCU\software\microsoft\windows\currentversion\wintrust\trust
   Opens key:
```

providers\software publishing

```
Opens key:
                                   HKCU\software\microsoft\windows\dwm
  Opens key:
                                    HKCU\software\microsoft\windows\shell
                                    HKCU\software\microsoft\windows\shell\bagmru
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\windows\shell\bags
  Opens key:
                                    HKCU\software\microsoft\windows\shell\bags\1
                                   HKCU\software\microsoft\windows\shell\bags\1\desktop
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\windows\tabletnc
                                   HKCU\software\microsoft\windows\tabletpc\tabsetup
  Opens key:
  Opens key:
                                   \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\windows}} \ \mbox{\tt error reporting}
  Opens key:
                                   HKCU\software\microsoft\windows\windows error reporting\consent
  Opens key:
                                    HKCU\software\microsoft\windows\windows error reporting\hangs
  Opens key:
                                   HKCU\software\microsoft\windows\windows error reporting\hangs\nhrtimes
                                    HKCU\software\microsoft\windows mail
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\windows mail\mail
  Opens key:
                                   HKCU\software\microsoft\windows mail\news
                                    HKCU\software\microsoft\windows mail\trident
  Opens key:
  Opens key:
                                   HKCU\software\microsoft\windows mail\trident\main
                                    HKCU\software\microsoft\windows mail\trident\settings
  Opens key:
                                   HKCU\software\microsoft\windows media
  Opens key:
  Opens key:
                                   HKCU\software\microsoft\windows media\wmsdk
  Opens key:
                                   HKCU\software\microsoft\windows media\wmsdk\general
  Opens key:
                                    HKCU\software\microsoft\windows media\wmsdk\namespace
  Opens key:
                                    HKCU\software\microsoft\windows nt
  Opens key:
                                    HKCU\software\microsoft\windows nt\currentversion
  Opens key:
                                    HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:
                                   HKCU\software\microsoft\windows
nt\currentversion\appcompatflags\compatibility assistant
                                   HKCU\software\microsoft\windows
  Opens key:
nt\currentversion\appcompatflags\compatibility assistant\persisted
  Opens key:
                                   HKCU\software\microsoft\windows nt\currentversion\devices
  Opens key:
                                   HKCU\software\microsoft\windows nt\currentversion\efs
  Opens key:
                                   HKCU\software\microsoft\windows
nt\currentversion\msicorruptedfilerecovery
  Opens key:
                                   HKCU\software\microsoft\windows
nt\currentversion\msicorruptedfilerecovery\repairedproducts
                                   HKCU\software\microsoft\windows nt\currentversion\network
  Opens key:
  Opens key:
                                   HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
  Opens key:
                                    HKCU\software\microsoft\windows nt\currentversion\peernet
  Opens key:
                                    \label{lem:hkcu} \mbox{HKCU\software\mbox{$\mbox{$\mbox{microsoft\windows}$} nt\current\version\end{\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox
  Opens key:
                                   HKCU\software\microsoft\windows nt\currentversion\printerports
  Opens key:
                                    HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform
  Opens key:
                                   HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\activation
  Opens key:
                                   HKCU\software\microsoft\windows nt\currentversion\taskmanager
  Opens key:
                                   HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:
                                   HKCU\software\microsoft\windows nt\currentversion\winlogon
  Opens key:
                                    HKCU\software\microsoft\windows script
  Opens key:
                                   HKCU\software\microsoft\windows script\settings
  Opens key:
                                    HKCU\software\microsoft\windows search
                                    HKCU\software\microsoft\windows search\processedsearchroots
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\windows search\processedsearchroots\0000
  Opens key:
                                    HKCU\software\microsoft\windows search\processedsearchroots\0001
  Opens key:
                                   HKCU\software\microsoft\windows search\processedsearchroots\0002
                                   HKCU\software\microsoft\windows search\processedsearchroots\0003
  Opens key
                                   HKCU\software\microsoft\windows sidebar
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\windows sidebar\ieoverride
  Opens key:
                                   \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\windows} sidebar\end{\sc everyde} \mbox{\sc main}
  Opens key:
                                    HKCU\software\microsoft\windows sidebar\ieoverride\settings
  Opens key:
                                   HKCU\software\microsoft\windows sidebar\ieoverride\styles
  Opens key:
                                    HKCU\software\microsoft\wisp
  Opens key:
                                    HKCU\software\microsoft\wisp\multitouch
  Opens key:
                                    HKCU\software\microsoft\wisp\pen
  Opens key:
                                    HKCU\software\microsoft\wisp\pen\syseventparameters
  Opens key:
                                   HKCU\software\microsoft\wisp\pen\syseventparameters\customflickcommands
                                    \label{thm:condition} \mbox{HKCU\software\mbox{\sc microsoft\wisp\pen\syseventparameters\sc flickcommands}} \label{thm:condition}
  Opens key:
  Opens key:
                                   HKCU\software\microsoft\wisp\touch
  Opens key:
                                   HKCU\software\netscape
  Opens key:
                                   HKCU\software\netscape\netscape navigator
  Opens key:
                                    HKCU\software\netscape\netscape navigator\suffixes
  Opens key:
                                    HKCU\software\netscape\netscape navigator\user trusted external
applications
  Opens kev:
                                   HKCU\software\netscape\netscape navigator\viewers
                                   HKCU\software\policies
  Opens key:
  Opens key:
                                    HKCU\software\policies\microsoft
                                   HKCU\software\policies\microsoft\systemcertificates
  Opens key:
  Opens key:
                                   HKCU\software\policies\microsoft\systemcertificates\ca
  Opens key:
                                   HKCU\software\policies\microsoft\systemcertificates\ca\certificates
  Opens key:
                                    HKCU\software\policies\microsoft\systemcertificates\ca\crls
  Opens key:
                                   HKCU\software\policies\microsoft\systemcertificates\ca\ctls
  Opens key:
                                    HKCU\software\policies\microsoft\systemcertificates\disallowed
  Opens key:
HKCU\software\policies\microsoft\systemcertificates\disallowed\certificates
                                   HKCU\software\policies\microsoft\systemcertificates\disallowed\crls
  Opens key:
                                   HKCU\software\policies\microsoft\systemcertificates\disallowed\ctls
  Opens key:
                                   HKCU\software\policies\microsoft\systemcertificates\trust
  Opens key:
  Opens key:
                                   \label{lem:hkcusoftware belief} HKCU \software \parbox{$\sim$ microsoft system} trust \certificates
  Opens key:
                                   HKCU\software\policies\microsoft\systemcertificates\trust\crls
  Opens key:
                                   HKCU\software\policies\microsoft\systemcertificates\trust\ctls
```

```
Opens key:
                                               HKCU\software\policies\microsoft\systemcertificates\trustedpeople
   Opens kev:
HKCU\software\policies\microsoft\systemcertificates\trustedpeople\certificates
   Opens key:
                                               HKCU\software\policies\microsoft\systemcertificates\trustedpeople\crls
   Opens key:
                                               HKCU\software\policies\microsoft\systemcertificates\trustedpeople\ctls
   Opens key:
                                               HKCU\software\policies\microsoft\systemcertificates\trustedpublisher
   Opens kev:
HKCU \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus trusted publisher \setminus certificates
   Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\crls
   Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\ctls
   Opens key:
                                               HKCU\software\policies\microsoft\windows
   Opens key:
                                               HKCU\software\policies\microsoft\windows\currentversion
   Opens key:
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
settings
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\5.0
   Opens key:
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\cache
   Opens key:
                                               HKCU\software\policies\power
                                               HKCU\software\policies\power\powersettings
   Opens kev:
   Opens key:
                                               HKCU\software\python
   Opens key:
                                               HKCU\software\python\pythoncore
                                               HKCU\software\python\pythoncore\2.7
   Opens kev:
   Opens key:
                                               HKCU\software\python\pythoncore\2.7\help
                                               HKCU\software\python\pythoncore\2.7\help\pythonwin reference
   Opens key:
   Opens key:
                                               HKCU\software\wow6432node
   Opens key:
                                               HKCU\software\wow6432node\microsoft
   Opens key:
                                               HKCU\software\wow6432node\microsoft\active setup
                                               HKCU\software\wow6432node\microsoft\active setup\installed components
   Opens key:
   Opens key:
                                               HKCU\software\wow6432node\microsoft\active setup\installed
components\>{26923b43-4d38-484f-9b9e-de460746276c}
                                               HKCU\software\wow6432node\microsoft\active setup\installed
   Opens key:
components\>{60b49e34-c7cc-11d0-8953-00a0c90347ff}
                                               HKCU\software\wow6432node\microsoft\active setup\installed
   Opens key:
components\{2c7339cf-2b09-4501-b3f3-f3508c9228ed}
   Opens key:
                                               \label{lem:hkcusoftware} \begin{tabular}{l} HKCU \software \wow 6432 node \microsoft \active setup \node \
components\{44bba840-cc51-11cf-aafa-00aa00b6015c}
                                               HKCU\software\wow6432node\microsoft\active setup\installed
   Opens key:
components\{6bf52a52-394a-11d3-b153-00c04f79faa6}
                                               HKCU\software\wow6432node\microsoft\active setup\installed
   Opens key:
components\{89820200-ecbd-11cf-8b85-00aa005b4340}
   Opens key:
                                               HKCU\software\wow6432node\microsoft\active setup\installed
components\{89820200-ecbd-11cf-8b85-00aa005b4383}
                                               \label{local-condition} \mbox{HKCU\software\wow} 6432 node\mbox{\sm microsoft\active setup\sm installed}
   Opens key:
components\{89b4c1cd-b018-4511-b0a1-5476dbf70820}
   Opens key:
                                               HKCU\software\classes
   Opens key:
                                               HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid
   Opens key:
                                               HKCU\software\classes\wow6432node\clsid\{8ad9c840-044e-11d1-b3e9-
00805f499d93}
   Opens key:
                                               HKCU\software\classes\wow6432node\clsid\{8ad9c840-044e-11d1-b3e9-
00805f499d93}\inprocserver32
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0003-
   Opens key:
abcdeffedcba}
   Opens key:
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0003-
abcdeffedcba}\inprocserver32
   Opens key:
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0004-
abcdeffedcba}
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0004-
   Opens key
abcdeffedcba}\inprocserver32
   Opens key:
                                               abcdeffedcba}
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0005-
   Opens key:
abcdeffedcba}\inprocserver32
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0000-
   Opens kev:
abcdeffedcba}
   Opens key
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0000-
abcdeffedcba}\inprocserver32
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0001-
   Opens key:
abcdeffedcba}
   Opens key:
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0001-
abcdeffedcba}\inprocserver32
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0001-
   Opens kev:
abcdeffedcbb}
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0001-
   Opens kev:
abcdeffedcbb}\inprocserver32
   Opens key:
                                               \label{locality} HKCU \software \classes \wow 6432 node \clsid \cafee fac-0013-0001-0002-0001-0002-0001-0002-0001-0002-0001-0002-0001-0002-0001-0002-0001-0002-0001-0002-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-00001-00001-0001-0001-00001-0001-0001-00000-0001-00001-00000-00000-0000-00000-0000-0000-0000-00
abcdeffedcba}
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0002-
   Opens key:
abcdeffedcba}\inprocserver32
   Opens key:
                                               abcdeffedcbb}
   Opens kev:
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0002-
abcdeffedcbb}\inprocserver32
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0003-
   Opens key:
abcdeffedcba}
   Opens key
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0003-
abcdeffedcba}\inprocserver32
                                               HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0003-
   Opens key:
```

```
abcdeffedcbb}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0003-
abcdeffedcbb}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0004-
abcdeffedcba}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0004-
abcdeffedcba}\inprocserver32
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0004-
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0004-
  Opens key
abcdeffedcbb}\inprocserver32
  Opens kev:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0005-
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0005-
  Opens key:
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0005-
  Opens key:
abcdeffedcbb}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0005-
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0006-
  Opens key:
abcdeffedcba}
  Opens kev:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0006-
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0006-
  Opens key:
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0006-
  Opens key:
abcdeffedcbb}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0007-
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0007-
  Opens key:
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0007-
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0007-
  Opens key
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0008-
  Opens key:
abcdeffedcba}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0008-
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0008-
  Opens key:
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0008-
  Opens key
abcdeffedcbb}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0009-
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0009-
  Opens key:
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0009-
abcdeffedcbb}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0009-
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0010-
  Opens key:
abcdeffedcba}
                                    Opens key:
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0010-
abcdeffedcbb}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0010-
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0011-
  Opens key
abcdeffedcba}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0011-
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0011-
  Opens key:
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0011-
  Opens kev:
abcdeffedcbb}\inprocserver32
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0012-
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0012-
  Opens key
abcdeffedcba}\inprocserver32
  Opens key:
                                    \label{locality} HKCU \software \classes \wow 6432 node \clsid \cafee fac-0013-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0001-0012-0012-0001-0012-0001-0012-0001-0012-0012-0001-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-0012-00012-00012-0012-0012-00012-0012-0012-0012-0012-0012-0012-0012-00012-00012-0012-0012-0012-0012-
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0012-
  Opens kev:
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0013-
  Opens kev:
abcdeffedcba}
  Opens key
                                    abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0013-
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0013-
  Opens key:
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0014-
  Opens kev:
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0014-
  Opens key:
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0014-
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0014-
  Opens key:
```

```
abcdeffedcbb}\inprocserver32
  Opens kev:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0015-
abcdeffedcba}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0015-
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0015-
abcdeffedchb}
                                    \label{locality} HKCU \software \classes \wow 6432 node \clsid \cafee fac-0013-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0015-0001-0001-0015-0001-0001-0015-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-0001-00001-00001-0001-0001-00001-0001-0001-00000-0001-00001-00000-00000-0000-00000-0000-0000-0000-00
  Opens key
abcdeffedcbb}\inprocserver32
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0016-
abcdeffedcba}
  Opens kev:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0016-
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0016-
  Opens key:
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0016-
  Opens key
abcdeffedcbb}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0017-
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0017-
  Opens key:
abcdeffedcba}\inprocserver32
  Opens kev:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0017-
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0017-
  Opens key:
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0018-
  Opens key:
abcdeffedcba}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0018-
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0018-
  Opens key
abcdeffedcbb}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0018-
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0019-
  Opens key:
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0019-
  Opens key:
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0019-
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0019-
  Opens key:
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0020-
  Opens key:
abcdeffedcba}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0020-
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0020-
  Opens key:
abcdeffedcbb}
  Opens key:
                                    abcdeffedcbb}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0021-
abcdeffedcba}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0021-
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0021-
  Opens key:
abcdeffedcbb}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0021-
abcdeffedcbb}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0000-
abcdeffedcba}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0000-
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0000-
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0000-
  Opens key:
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0001-
  Opens kev:
abcdeffedcba}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0001-
abcdeffedcba}\inprocserver32
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0001-
abcdeffedcbb}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0001-
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0002-
  Opens kev:
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0002-
  Opens kev:
abcdeffedcba}\inprocserver32
  Opens key
                                    abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0002-
  Opens key:
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0003-
  Opens key:
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0003-
  Opens kev:
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0003-
  Opens key:
abcdeffedcbb}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0003-
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0004-
  Opens key:
```

```
abcdeffedcba}
 Opens key
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0004-
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0004-
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0004-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0000-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0000-
 Opens key
abcdeffedcba}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0000-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0000-
 Opens key:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0001-
 Opens key:
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0001-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0001-
 Opens key
abcdeffedcbb}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0001-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0002-
 Opens key:
abcdeffedcba}
                        Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0002-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0002-
 Opens key
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0003-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0003-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0003-
 Opens key:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0003-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0004-
 Opens key:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0004-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0004-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0004-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0005-
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0005-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0005-
 Opens key:
abcdeffedcbb}
                        Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0006-
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0006-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0006-
 Opens key
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0006-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0007-
 Opens key:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0007-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0007-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0001-0007-
 Opens key
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0000-
abcdeffedcba}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0000-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0000-
 Opens kev:
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0000-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0001-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0001-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0001-
 Opens kev:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0001-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0002-
abcdeffedcba}
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0002-
 Opens key:
```

```
abcdeffedcba}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0002-
abcdeffedcbb)
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0002-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0003-
abcdeffedcha}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0003-
 Opens key
abcdeffedcba}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0003-
abcdeffedcbb}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0003-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0004-
 Opens key:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0004-
 Opens key
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0004-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0004-
 Opens key
abcdeffedcbb}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0005-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0005-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0005-
 Opens key:
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0005-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0006-
 Opens key:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0006-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0006-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0006-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0007-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0007-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0007-
 Opens key:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0007-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0008-
 Opens key:
abcdeffedcba}
 Opens key:
                        abcdeffedcba}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0008-
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0008-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0009-
 Opens key:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0009-
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0009-
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0009-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0010-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0010-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0010-
 Opens kev:
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0010-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0011-
abcdeffedcba}
 Opens key:
                        abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0011-
 Opens kev:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0011-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key
                        abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0012-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0012-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0012-
 Opens kev:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0013-
 Opens key:
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0013-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0013-
 Opens key:
```

```
abcdeffedcbb}
 Opens key
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0013-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0014-
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0014-
abcdeffedcba}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0014-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0014-
 Opens key
abcdeffedcbb}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0015-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0015-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0015-
 Opens key:
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0015-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0016-
 Opens key:
abcdeffedcba}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0016-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0016-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0016-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0017-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0017-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0017-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0017-
 Opens key
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0018-
 Opens key:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0018-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0018-
 Opens key:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0018-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0019-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0019-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0019-
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0019-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0020-
 Opens key:
abcdeffedcba}
                        Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0020-
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0020-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0021-
 Opens key
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0021-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0021-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0021-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0022-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0022-
 Opens key
abcdeffedcba}\inprocserver32
 Opens key:
                        abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0022-
 Opens kev:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0023-
 Opens kev:
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0023-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0023-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0023-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0024-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0024-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0024-
abcdeffedcbb}
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0024-
 Opens key:
```

```
abcdeffedcbb}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0025-
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0025-
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0025-
abcdeffedcbb3
                        Opens key
abcdeffedcbb}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0026-
abcdeffedcba}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0026-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0026-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0026-
 Opens key
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0027-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0027-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0027-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0027-
 Opens key:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0028-
 Opens key:
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0028-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0028-
 Opens key
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0028-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0029-
 Opens key:
abcdeffedcba}
                        Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0029-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0029-
 Opens key:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0030-
 Opens key:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0030-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0030-
 Opens key:
abcdeffedcbb}
 Opens key:
                        abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0031-
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0031-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0031-
 Opens key:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0031-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0032-
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0032-
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0032-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0032-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0033-
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0033-
abcdeffedcba}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0033-
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0033-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0034-
 Opens kev:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0034-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0034-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0034-
 Opens key:
abcdeffedcbb}\inprocserver32
                        Opens key:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-ffff-
 Opens kev:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0000-
 Opens key:
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0000-
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0000-
```

```
abcdeffedcbb}
 Opens key
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0000-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0000-
abcdeffedcbc}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0000-
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0001-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0001-
 Opens key
abcdeffedcba}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0001-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0001-
 Opens key:
abcdeffedcbb\\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0001-
 Opens key:
abcdeffedcbc}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0001-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
 Opens key:
abcdeffedcba}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
 Opens kev:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
 Opens key:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0004-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0004-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0004-
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0004-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0004-
 Opens key:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0004-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0005-
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0005-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0005-
 Opens key
abcdeffedcbb}
 Opens key:
                        abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0005-
 Opens key:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0005-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0006-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0006-
 Opens key
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0006-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0006-
 Opens kev:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0006-
 Opens kev:
abcdeffedcbc}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0006-
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0007-
abcdeffedcba}
                        Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0007-
 Opens kev:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0007-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0007-
abcdeffedcbc}
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0007-
 Opens key:
```

```
abcdeffedcbc}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0008-
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0008-
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0008-
abcdeffedchb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0008-
 Opens key
abcdeffedcbb}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0008-
abcdeffedcbc}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0008-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0009-
 Opens key:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0009-
 Opens key
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0009-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0009-
 Opens key
abcdeffedcbb}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0009-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0009-
 Opens key:
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0010-
 Opens kev:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0010-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0010-
 Opens key:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0010-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0010-
 Opens key:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0010-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0011-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0011-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0011-
 Opens key:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0011-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0011-
 Opens kev:
abcdeffedcbc}
 Opens key:
                        abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0012-
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0012-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0012-
 Opens key:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0012-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0012-
abcdeffedcbc}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0012-
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0013-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0013-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0013-
 Opens kev:
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0013-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0013-
abcdeffedcbc}
 Opens key:
                        abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0014-
 Opens kev:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0014-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key
                        abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0014-
 Opens key:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0014-
 Opens key:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0014-
 Opens kev:
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0015-
 Opens key:
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0015-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0015-
 Opens key:
```

```
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0015-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0015-
abcdeffedcbc}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0015-
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0016-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0016-
 Opens key
abcdeffedcba}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0016-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0016-
 Opens key:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0016-
 Opens key:
abcdeffedcbc}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0016-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0017-
 Opens key:
abcdeffedcba}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0017-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0017-
 Opens key:
abcdeffedcbb}
                        Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0017-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0017-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0018-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0018-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0018-
 Opens kev:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0018-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0018-
 Opens key:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0018-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0019-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0019-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0019-
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0019-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0019-
 Opens key:
abcdeffedcbc}
                        Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0020-
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0020-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0020-
 Opens key
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0020-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0020-
 Opens key:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0020-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0021-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0021-
 Opens key
abcdeffedcba}\inprocserver32
 Opens key:
                        abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0021-
 Opens kev:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0021-
 Opens kev:
abcdeffedcbc}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0021-
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0022-
abcdeffedcba}
                        Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0022-
 Opens kev:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0022-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0022-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0022-
 Opens key:
```

```
abcdeffedcbc}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0023-
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0023-
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0023-
abcdeffedcbb3
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0023-
 Opens key
abcdeffedcbb}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0023-
abcdeffedcbc}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0023-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
 Opens key:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
 Opens key
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
 Opens key
abcdeffedcbb}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
 Opens key:
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
 Opens kev:
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
 Opens key
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
 Opens key:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0026-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0026-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0026-
 Opens key:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0026-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0026-
 Opens kev:
abcdeffedcbc}
 Opens key:
                        abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0027-
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0027-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0027-
 Opens key:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0027-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0027-
abcdeffedcbc}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0027-
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0028-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0028-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0028-
 Opens kev:
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0028-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0028-
abcdeffedcbc}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0028-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0029-
 Opens kev:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0029-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key
                        abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0029-
 Opens key:
abcdeffedcbb}\inprocserver32
                        Opens key:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0029-
 Opens kev:
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0030-
 Opens key:
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0030-
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0030-
```

```
abcdeffedcbb}
 Opens key
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0030-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0030-
abcdeffedcbc}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0030-
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0031-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0031-
 Opens key
abcdeffedcba}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0031-
 Opens key:
abcdeffedcbb\\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0031-
 Opens key:
abcdeffedcbc}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0032-
 Opens key:
abcdeffedcba}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0032-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0032-
 Opens key:
abcdeffedcbb}
                        Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0032-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0032-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-ffff-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-ffff-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
 Opens kev:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
 Opens key
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0001-
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0001-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0001-
 Opens key:
abcdeffedcbb}
                        Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0001-
abcdeffedcbc}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0001-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
 Opens key
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
 Opens key
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0003-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0003-
 Opens kev:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0003-
 Opens kev:
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0003-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0003-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0003-
 Opens key:
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0004-
 Opens kev:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0004-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0004-
abcdeffedcbb}
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0004-
 Opens key:
```

```
abcdeffedcbb}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0004-
abcdeffedcbc)
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0004-
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0005-
abcdeffedcha}
                        Opens key:
abcdeffedcba}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0005-
abcdeffedcbb}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0005-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0005-
 Opens key:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0005-
 Opens key
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0006-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0006-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0006-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0006-
 Opens key:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0006-
 Opens key:
abcdeffedcbc}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0006-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0007-
 Opens key:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0007-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0007-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0007-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0007-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0007-
 Opens key:
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0008-
 Opens key:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0008-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0008-
 Opens key:
abcdeffedcbb}
 Opens key:
                        abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0008-
abcdeffedcbc}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0008-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0009-
 Opens key:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0009-
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0009-
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0009-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0009-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0009-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0010-
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0010-
abcdeffedcba}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0010-
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0010-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0010-
 Opens kev:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0010-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key
                        abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0011-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0011-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0011-
 Opens kev:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0011-
 Opens key:
abcdeffedcbc}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0011-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0012-
 Opens key:
```

```
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0012-
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0012-
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0012-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0012-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0012-
 Opens key
abcdeffedcbc}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0013-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0013-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0013-
 Opens key:
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0013-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0013-
 Opens key:
abcdeffedcbc}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0013-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0014-
 Opens key:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0014-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0014-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0014-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0014-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0014-
 Opens key:
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0015-
 Opens key:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0015-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0015-
 Opens key:
abcdeffedcbb}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0015-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0015-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0015-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0016-
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0016-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0016-
 Opens key:
abcdeffedcbb}
                        Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0016-
abcdeffedcbc}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0016-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0017-
 Opens key
abcdeffedcba}
 Opens key:
                        abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0017-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0017-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0017-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0017-
 Opens key
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0018-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0018-
 Opens kev:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0018-
 Opens kev:
abcdeffedcbb}
 Opens key
                        abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0018-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0018-
 Opens key:
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0019-
 Opens kev:
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0019-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0019-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0019-
 Opens key:
```

```
abcdeffedcbb}\inprocserver32
 Opens kev:
                         HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0019-
abcdeffedcbc)
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0019-
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0020-
abcdeffedcha}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0020-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0020-
abcdeffedcbb}
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0020-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0020-
 Opens key:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0020-
 Opens key
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
 Opens key:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
 Opens key:
abcdeffedcbc}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
 Opens key:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
 Opens key:
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0023-
 Opens key:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0023-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0023-
 Opens key:
abcdeffedcbb}
 Opens key:
                        abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0023-
abcdeffedcbc}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0023-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0024-
 Opens key:
abcdeffedcba}
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0024-
abcdeffedcba}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0024-
abcdeffedcbb}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0024-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0024-
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0024-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens kev:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0025-
abcdeffedcba}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0025-
abcdeffedcba}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0025-
abcdeffedcbb}
 Opens key:
                        abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0025-
 Opens kev:
abcdeffedcbc}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0025-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0026-
abcdeffedcba}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0026-
 Opens key:
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0026-
 Opens key:
abcdeffedcbb}
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0026-
 Opens kev:
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0026-
 Opens key:
abcdeffedcbc}
 Opens key
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0026-
abcdeffedcbc}\inprocserver32
 Opens key:
                        HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0027-
```

```
abcdeffedcba}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0027-
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0027-
abcdeffedcbb}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0027-
abcdeffedcbb}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0027-
abcdeffedcbc}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0027-
  Opens key
abcdeffedcbc}\inprocserver32
  Opens kev:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
  Opens key:
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
  Opens key:
abcdeffedcbb}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
  Opens key:
abcdeffedcbc}
  Opens kev:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
abcdeffedcbc}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
  Opens key:
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
  Opens key:
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
  Opens key:
abcdeffedcbb}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
abcdeffedcbc}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
  Opens key:
abcdeffedcbc}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-ffff-
  Opens key:
abcdeffedcba}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-ffff-
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
  Opens key:
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
  Opens key:
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
  Opens key:
abcdeffedcbb}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
abcdeffedcbc}
  Opens key
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
abcdeffedcbc}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcba}
                                    Opens key:
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbb}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
  Opens key
abcdeffedcbc}
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbc}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
  Opens key:
abcdeffedcba}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
  Opens kev:
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
  Opens key
abcdeffedcbb}\inprocserver32
  Opens key:
                                    abcdeffedcbc}
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
  Opens kev:
abcdeffedcbc}\inprocserver32
                                    HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-ffff-
  Opens kev:
abcdeffedcba}
  Opens key
                                    \label{lem:hkcusoftware} HKCU \software \classes \wow 6432 node \clsid \cafee fac-0017-0000-ffff-0000-ffff-0000-ffff-0000-ffff-0000-ffff-0000-ffff-0000-ffff-0000-ffff-0000-ffff-0000-ffff-0000-ffff-0000-fff-0000-ffff-0000-fff-0000-fff-0000-fff-0000-fff-0000-fff-0000-fff-0000-fff-0000-fff-0000-ff-0000-fff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-0000-ff-000
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid\{e19f9331-3110-11d4-991c-
005004d3b3db}
                                    Opens key:
005004d3b3db}\inprocserver32
  Opens key:
                                    HKCU\software\classes\iavaplugin.1020
                                    HKCU\software\classes\javaplugin.1020\clsid
  Opens key:
  Opens key:
                                    HKCU\software\classes\local settings
  Opens key:
                                    {\tt HKCU \setminus software \setminus classes \setminus local \ settings \setminus muicache}
  Opens key:
                                    HKCU\software\classes\local settings\muicache\16
                                    HKCU\software\classes\local settings\muicache\16\52c64b7e
  Opens key:
  Opens key:
                                    HKCU\software\classes\local settings\software
```

```
Opens key:
                                                                                                     HKCU\software\classes\local settings\software\microsoft
                                                                                                      HKCU\software\classes\local settings\software\microsoft\windows
       Opens kev:
       Opens key:
                                                                                                     HKCU\software\classes\local
settings\software\microsoft\windows\currentversion
                                                                                                     HKCU\software\classes\local settings\software\microsoft\windows\shell
       Opens key:
       Opens key:
                                                                                                     HKCU\software\classes\python.file
      Opens kev:
                                                                                                     HKCU\software\classes\python.file\shell
                                                                                                     \label{thm:likelike} \label{thm:likeliked} \mbox{HKCU\software\classes\python.file\shell\edit\ with\ pythonwin} \\
      Opens key:
      Opens key:
                                                                                                     \label{thm:local_hammon} \begin{tabular}{ll} HKCU \software \classes \python.file \shell \ed it with pythonwin \command \end{tabular}
      Opens key:
                                                                                                     HKCU\software\classes\python.noconfile
       Opens key:
                                                                                                      HKCU\software\classes\python.noconfile\shell
       Opens key:
                                                                                                     HKCU\software\classes\python.noconfile\shell\edit with pythonwin
       Opens key:
                                                                                                      HKCU\software\classes\python.noconfile\shell\edit with pythonwin\command
       Opens key:
                                                                                                     HKCU\software\classes\virtualstore
      Opens kev:
                                                                                                     HKCU\software\classes\virtualstore\machine
       Opens key:
                                                                                                     HKCU\software\classes\virtualstore\machine\software
      Opens kev:
                                                                                                     HKCU\software\classes\virtualstore\machine\software\wow6432node
      Opens key:
HKCU \setminus software \setminus classes \setminus virtual store \setminus machine \setminus software \setminus wow 6432 node \setminus microsoft
        Opens key:
                                                                                                     HKCU\software\classes\wow6432node
       Opens key:
                                                                                                     HKLM\software\wow6432node\microsoft\windows\currentversion\run
       Opens kev:
                                                                                                     HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
       Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
       Opens key:
                                                                                                     HKLM\software\wow6432node\microsoft\rpc
       Opens key:
                                                                                                     HKLM\system\currentcontrolset\control\computername\activecomputername
                                                                                                     HKLM\system\setup
      Opens key:
       Opens key:
                                                                                                     HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
       Opens key:
                                                                                                     HKLM\software\policies\microsoft\windows nt\rpc
                                                                                                     HKLM\system\currentcontrolset\services\tcpip\linkage
       Opens key:
      Opens key:
                                                                                                     HKCU\software\flashfxp
      Opens key:
                                                                                                     HKCU\software\flashfxp\3
       Opens key:
                                                                                                     HKCU\software\flashfxp\4
      Opens kev:
                                                                                                     HKLM\software\wow6432node\flashfxp
       Opens key:
                                                                                                     HKLM\software\wow6432node\flashfxp\3
                                                                                                     HKLM\software\wow6432node\flashfxp\4
      Opens key:
       Opens key:
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}
      Opens key:
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
      Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session info \ 1\ known folders
      Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (explorer \ known folders ettings) \ for the software \ wow 6432 node \ microsoft \ windows \ (explorer \ known folders ettings) \ for the software \ wow 6432 node \ microsoft \ windows \ (explorer \ known folders ettings) \ for the software \ for the software
      Opens key:
                                                                                                     Opens kev:
HKLM \verb|\software| wow 6432 node \verb|\microsoft| windows \verb|\currentversion| uninstall \verb|\addressbook| and the state of the 
      Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ adobe flash player active x \ microsoft \ windows \ current \ version \ versio
      Opens kev:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\connection manager
      Opens key:
HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus windows \setminus current \lor version \setminus uninstall \setminus direct drawex
      Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\fontcore
       Opens kev:
Opens key:
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie5bakex
      Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\iedata
       Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mobileoptionpack
      Opens kev:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Wow 6432 node \mbox{\current} windows \label{lem:hklm} \label{lem:hklm} wow 6432 node \mbox{\current} windows \label{lem:hklm} Wow 6432 node \mbox{\current} windows \label{lem:hklm} \label{lkm} \label{lkm}
      Opens key:
                                                                                                     HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\wic
      Opens kev:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ \{196bb40d-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-3d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b289-1578-5d01-b28
befc77a11a1e}
      Opens key:
2f83217002ff}
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ \{4a03706f-666a-4037-7777-18411, 18403706f-666a-4037-7777-18411, 18403706f-666a-4037-777-18411, 18403706f-666a-4037-777-18411, 18403706f-666a-4037-777-18411, 18403706f-666a-4037-777-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-18411, 184037-184111, 184037-18411, 184037-184111, 184037-184111, 184037-18411, 184037-184110, 184037-184111, 1
5f2748764d10}
      Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-
0000000ff1ce}
      Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ \{90850409-6000-11d3-8cfe-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-1
0150048383c9}
```

```
0000000ff1ce}
   Opens kev:
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-
a9300000001}
                                                       HKCU\software\bpftp\bullet proof ftp\main
   Opens key:
   Opens key:
                                                       \label{thm:linear} \mbox{HKCU\software\bulletproof ftp client\mbox{\sc main}} \\
   Opens key:
                                                       HKCU\software\bpftp\bullet proof ftp\options
   Opens key:
                                                       HKCU\software\bulletproof software\bulletproof ftp client\options
   Opens key:
                                                       HKCU\software\bulletproof software\bulletproof ftp client 2010\options
   Opens key:
                                                       HKCU\software\bpftp
   Opens key:
6fba-4fcf-9d55-7b8e7f157091}
   Opens kev:
6fba-4fcf-9d55-7b8e7f157091}\propertybag
fdc1-4dc3-a9dd-070d1d495d97}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}\propertybag
                                                       HKLM\software\wow6432node\microsoft\windows
   Opens key:
nt\currentversion\profilelist
                                                       HKCU\software\turboftp
   Opens key:
   Opens key:
                                                       HKCU\software\cryer\websitepublisher
   Opens key:
                                                       HKU\
                                                       HKCU\software\ftpclient\sites
   Opens key:
                                                       HKCU\software\softx.org\ftpclient\sites
   Opens key:
   Opens key:
                                                       HKCU\software\vandyke\securefx
   Opens key:
c1bf-494e-b29c-65b732d3d21a}
   Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1
c1bf-494e-b29c-65b732d3d21a}\propertybag
    Opens kev:
                                                       HKLM\software\wow6432node\microsoft\windows\currentversion
   Opens key:
a0fb-4bfc-874a-c0f2e0b9fa8e}
   Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft\} \ description \ descriptio
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
   Opens key:
                                                       {\tt HKCU \backslash software \backslash global scape \backslash cuteftp~6~home \backslash qctoolbar}
   Opens key:
                                                       HKCU\software\globalscape\cuteftp 6 professional\qctoolbar
   Opens key:
                                                       HKCU\software\globalscape\cuteftp 7 home\qctoolbar
   Opens key:
                                                       HKCU\software\globalscape\cuteftp 7 professional\qctoolbar
                                                       HKCU\software\globalscape\cuteftp 8 home\qctoolbar
   Opens kev:
   Opens key:
                                                       HKCU\software\globalscape\cuteftp 8 professional\qctoolbar
   Opens key:
9f6d-47a2-aaae-29d317c6f066}
   Onens key:
HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \label{lem:hkklm}
9f6d-47a2-aaae-29d317c6f066\} \verb|\property| bag
   Opens key:
                                                       HKCU\software\sota\ffftp\options
   Opens key:
                                                       HKCU\software\south river technologies\webdrive\connections
                                                       HKCU\software\nch software\classicftp\ftpaccounts
   Opens kev:
                                                       HKLM\software\wow6432node\nch software\fling\accounts
   Opens key:
   Opens key:
                                                       HKCU\software\filezilla
   Opens key:
                                                       HKCU\software\filezilla\recent servers
   Opens key:
                                                       HKCU\software\filezilla\site manager
   Opens key:
                                                       HKCU\software\ftp explorer\profiles
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ultrafxp
    Opens key:
                                                       HKCU\software\martin prikryl
   Opens key:
                                                       HKLM\software\wow6432node\martin prikryl
                                                       HKCU\software\ftpware\coreftp\sites
   Opens kev:
                                                       HKCU\software\far\plugins\ftp\hosts
   Opens key:
   Opens key:
                                                       HKCU\software\far2\plugins\ftp\hosts
   Opens kev:
                                                       HKCU\software\far\saveddialoghistorv\ftphost
   Opens key:
                                                       HKCU\software\far2\saveddialoghistory\ftphost
   Opens kev:
0e22-4760-9afe-ea3317b67173}
   Opens key:
0e22-4760-9afe-ea3317b67173}\propertybag
   Opens key:
                                                       HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
   Opens kev:
                                                       HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
980053277-1733835069-2361817685-1001
                                                       HKCU\software\ghisler\windows commander
   Opens key:
   Opens key:
                                                       HKCU\software\ghisler\total commander
```

HKLM\software\wow6432node\ghisler\windows commander

Opens key: HKLM\software\wow6432node\ghisler\total commander
Opens key: HKLM\software\wow6432node

Opens key:

```
Opens key:
                                       HKCU\software\acebit
                                        HKLM\software\wow6432node\acebit
  Opens kev:
  Opens key:
                                        HKCR\typelib\{cb1f2c0f-8094-4aac-bcf5-41a64e27f777}
  Opens key:
                                       HKCR\typelib\{9ea55529-e122-4757-bc79-e4825f80732c}
                                       HKLM\system\currentcontrolset\services\winsock\setup
  Opens key:
migration\providers\tcpip6
                                       HKLM\system\currentcontrolset\control\sqmservicelist
  Opens kev:
                                       HKCU\software\mozilla
  Opens key:
  Opens key:
                                       HKLM\software\wow6432node\mozilla
  Opens key:
                                       HKCU\software\chromeplus
  Opens key:
                                       HKCU\software\leechftp
  Opens kev:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f
db2c-424c-b029-7fe99a87c641}
  Opens kev:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f
db2c-424c-b029-7fe99a87c641}\propertybag
                                       HKCU\software\classes\
  Opens key:
  Opens key:
                                       HKLM\software\classes
  Opens key:
                                       HKCU\software\flashpeak\blazeftp\settings
                                       HKCR\typelib\{f9043c88-f6f2-101a-a3c9-08002b2f49fb}\1.2\0\win32
  Opens key:
  Queries value:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
                                       HKLM\system\currentcontrolset\control\session
  Queries value:
manager[cwdillegalindllsearch]
                                       HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Oueries value:
                                       {\tt HKLM \ } system \verb| current control \verb| terminal server[tsuserenabled]|
  Oueries value:
  Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \software \policies \microsoft \windows \safer \code identifiers \cite{transparentenabled} \end{tabular}
                                       HKLM\system\currentcontrolset\control\nls\customlocale[empty]
   Queries value:
  Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
                                       HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  Queries value:
                                       HKLM\system\currentcontrolset\control\mui\uilanguages\en-
  Queries value:
us[alternatecodepage]
  Oueries value:
                                       HKCU\control panel\desktop[preferreduilanguages]
                                       HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Oueries value:
  Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ [prefer external manifest]
                                       HKLM\system\currentcontrolset\control\nls\sorting\versions[]
   Queries value:
  Queries value:
                                       HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
                                       HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:
                                       HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[752d6fe81122349daf998a56f48e0b38]
                                       HKLM\software\wow6432node\microsoft\windows
  Oueries value:
nt\currentversion\windows[loadappinit_dlls]
  Oueries value:
                                       {\tt HKLM \setminus software \setminus microsoft \setminus ole[pageallocatoruse system heap]}
  Queries value:
                                       {\tt HKLM \setminus software \setminus microsoft \setminus ole[pageallocator system heap is private]}
  Oueries value:
                                       HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
                                       HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[disableimprovedzonecheck]
                                       HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[security hklm only]
                                       HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Oueries value:
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock \setminus parameters [winsock_registry_version]
  Queries value:
                                       \label{lem:hklm} \verb+Kklm \+ system \+ current control \+ custom \+ locale \+ [en-us]
  Queries value:
                                       HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog 9 [serial\_access\_num]
  Queries value:
Oueries value:
Oueries value:
Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 000000000003 \ [packed catalog item]
  Oueries value:
Oueries value:
Queries value:
Queries value:
Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Oueries value:
```

- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
 Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \nam$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 00000000000002 [library path] \ Oueries \ value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000000002 [displaystring] \\ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$
- $\label{local-bound} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\space\space] Queries\value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
 Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catalo$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo] Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog \scatalog_entries \names \names \pace_catalog \scatalog_entries \names \names \pace_catalog \scatalog_entries \names \names \names \pace_catalog \scatalog_entries \names \names$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
 Oueries value:
- $\label{lem:hklm} HKL^{M} system \current control set \services \winsock 2 \parameters \namespace_catalog5 \catalog_entries \namespace_catalog5 \catalog5 \catalog6 \$
- $\label{lem:hklm/system/current} HKLM\system\current\controlset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]\ Queries\value:$
- $HKLM \ system \ current control set \ services \ win sock 2 \ parameters \ name space_catalog5 \ catalog_entries \ 0000000000005 \ [address family] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
 Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog \catalog_entries \names \names \pace_catalog \catalog_entries \names \names \names \pace_catalog \catalog_entries \names \names$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
 Oueries value:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[displaystring]
 Oueries value:
Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 0000000000006 \ [address family]
 Queries value:
Oueries value:
Oueries value:
HKLM \ system \ current control set \ services \ win sock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 0000000000006 [storesservice class info]]
 Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 000000000006 [providerinfo]
 Queries value:
HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
 Oueries value:
                     HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
                     HKLM\system\currentcontrolset\services\winsock\setup
 Oueries value:
migration\providers\tcpip[winsock 2.0 provider id]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
 Oueries value:
                     HKLM\system\currentcontrolset\control\cmf\config[system]
                     HKLM\software\wow6432node\microsoft\windows\windows error
 Oueries value:
reporting\wmr[disable]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[ar]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[ar]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[ar-sa]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-sa]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[bg]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[bg]
                     HKLM\system\currentcontrolset\control\nls\customlocale[bg-bg]
 Oueries value:
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[bg-bg]
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[ca]
 Oueries value:
                     Queries value:
                     Oueries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[ca-es]
                     HKLM\system\currentcontrolset\control\nls\customlocale[zh-hans]
 Oueries value:
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-hans]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[zh-cn]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-cn]
                     HKLM\svstem\currentcontrolset\control\nls\customlocale[cs]
 Oueries value:
 Oueries value:
                     HKLM\svstem\currentcontrolset\control\nls\extendedlocale[cs]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[cs-cz]
 Oueries value:
                     Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[da]
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[da]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[da-dk]
 Oueries value:
 Queries value:
                     Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[de]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[de]
                     HKLM\system\currentcontrolset\control\nls\customlocale[de-de]
 Oueries value:
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[de-de]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[el]
 Oueries value:
                     Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[el-gr]
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[el-gr]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[en]
 Oueries value:
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[es]
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[es]
 Oueries value:
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[es-es]
                     HKLM\svstem\currentcontrolset\control\nls\extendedlocale[es-es]
 Oueries value:
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[fi]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[fi-fi]
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[fi-fi]
 Queries value:
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[fr]
 Queries value:
                     Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[fr-fr]
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-fr]
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[hel
```

HKLM\system\currentcontrolset\control\nls\extendedlocale[he]

 $\label{lem:hklm} \verb+Kklm \+ system \+ control \+ ls \+ custom \+ locale [he-il]$

HKLM\system\currentcontrolset\control\nls\extendedlocale[hu]

HKLM\system\currentcontrolset\control\nls\extendedlocale[he-il]
HKLM\system\currentcontrolset\control\nls\customlocale[hu]

Oueries value:

Oueries value:

Queries value:

Queries value: Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[hu-hu] HKLM\system\currentcontrolset\control\nls\extendedlocale[hu-hu] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[is] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[is] HKLM\system\currentcontrolset\control\nls\customlocale[is-is] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[is-is] Oueries value: HKI M\system\currentcontrolset\control\nls\customlocale[it1] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[it] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[it-it] HKLM\system\currentcontrolset\control\nls\customlocale[ja] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ja] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ja-jp] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ja-jp] HKLM\svstem\currentcontrolset\control\nls\customlocale[ko] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[kol Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[ko-kr] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ko-kr] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[nl] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[nl] HKLM\system\currentcontrolset\control\nls\customlocale[nl-nl] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[nl-nl] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[no] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[no] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[nb-nol Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[nb-nol HKLM\system\currentcontrolset\control\nls\customlocale[pl] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[pl] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[p1-p1] HKLM\system\currentcontrolset\control\nls\customlocale[pt] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[pt] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[pt-br] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[pt-br] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[rm] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[rm] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[rm-ch] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ro] HKLM\system\currentcontrolset\control\nls\extendedlocale[ro] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ro-ro] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ro-ro] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ru] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ru] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ru-ru] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ru-ru] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[hr] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hr] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[hr-hr] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hr-hr] HKLM\system\currentcontrolset\control\nls\customlocale[sk] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sk] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sk-sk] HKLM\system\currentcontrolset\control\nls\extendedlocale[sk-sk] Queries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[sq] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sq] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sq-al] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[sv] HKLM\system\currentcontrolset\control\nls\extendedlocale[sv] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[sv-se] Oueries value: Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[th] HKLM\system\currentcontrolset\control\nls\extendedlocale[th] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[th-th] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[th-th] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[tr] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tr] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[tr-tr] HKLM\system\currentcontrolset\control\nls\extendedlocale[tr-tr] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ur] Oueries value: Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ur-pk] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ur-pk] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[id] HKLM\system\currentcontrolset\control\nls\extendedlocale[id] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[id-id] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[uk] HKLM\system\currentcontrolset\control\nls\extendedlocale[uk] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[uk-ua] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[be] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[be] HKLM\svstem\currentcontrolset\control\nls\customlocale[be-by] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[be-by] Oueries value: $HKLM \verb|\system| current controlset \verb|\control| nls \verb|\custom| locale[sl]|$ Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[s1] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sl-si] HKLM\system\currentcontrolset\control\nls\extendedlocale[sl-si] Queries value:

Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[et] HKLM\system\currentcontrolset\control\nls\extendedlocale[et] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[et-ee] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[et-ee] HKLM\system\currentcontrolset\control\nls\customlocale[lv] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[[v1] HKIM\system\currentcontrolset\control\nls\customlocale[lv-lv] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lv-lv] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[lt] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lt] HKLM\system\currentcontrolset\control\nls\customlocale[lt-lt] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lt-lt] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[tg] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tg] HKLM\system\currentcontrolset\control\nls\customlocaleftg-cyrl-til Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tg-cyrl-tj] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fa] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fa] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fa-ir] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fa-ir] HKLM\system\currentcontrolset\control\nls\customlocale[vi] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[vi] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[vi-vn] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[vi-vn] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[hv] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hv] HKLM\system\currentcontrolset\control\nls\customlocale[hy-am] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hy-am] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[az] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[az] HKLM\system\currentcontrolset\control\nls\customlocale[az-latn-az] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[az-latn-az] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[eu] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[eu] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[eu-es] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[eu-esl Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[hsb] Oueries value: $\label{lem:hklmsystem} \verb|HKLM\| system \verb| current control \verb| lnls \verb| extended locale [hsb]| \\$ Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[hsb-de] HKLM\system\currentcontrolset\control\nls\extendedlocale[hsb-de] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[mk] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mk] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[mk-mk] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mk-mk] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[tn] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tn] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[tn-za] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tn-za] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[xh] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[xh] HKLM\system\currentcontrolset\control\nls\customlocale[xh-za] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[xh-za] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[zu] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zu] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[zu-za] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[zu-za] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[af] Oueries value: $\label{lem:hklmsystem} \verb|HKLM\| system \verb| current control \verb| lnls \verb| extended locale[af]| \\$ Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[af-za] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ka] Oueries value: Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ka-ge] HKLM\system\currentcontrolset\control\nls\extendedlocale[ka-ge] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[fo] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[fo] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fo-fo] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fo-fo] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[hi] HKLM\system\currentcontrolset\control\nls\extendedlocale[hi] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[hi-in] Oueries value: Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[mt] HKLM\system\currentcontrolset\control\nls\extendedlocale[mt] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[mt-mt] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[mt-mt] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[se] Queries value: $HKLM \verb|\system| current controlset \verb|\control| nls \verb|\extended| locale [se]|$ Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[se-no] HKLM\system\currentcontrolset\control\nls\extendedlocale[se-no] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ga] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ga-ie] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ga-ie] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ms] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ms] Oueries value: $\label{lem:hklm} \verb+Kklm \ system \ current controls et \ \ control \ \ \ ls \ \ custom \ \ locale \ [ms-my]$ Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ms-my] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[kk] HKLM\system\currentcontrolset\control\nls\extendedlocale[kk] Queries value:

Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[kk-kz] HKLM\system\currentcontrolset\control\nls\extendedlocale[kk-kz] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ky] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ky] HKLM\system\currentcontrolset\control\nls\customlocale[ky-kg] Queries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[ky-kg] Oueries value: HKI M\system\currentcontrolset\control\nls\customlocale[sw] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sw] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sw-ke] HKLM\system\currentcontrolset\control\nls\customlocale[tk] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tk] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[tk-tm] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tk-tm] HKLM\svstem\currentcontrolset\control\nls\customlocale[uz] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[uz] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[uz-latn-uz] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[uz-latn-uz] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[tt] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tt] HKLM\system\currentcontrolset\control\nls\customlocale[tt-ru] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tt-ru] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[bn] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[bn] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[bn-in] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[bn-in] HKLM\system\currentcontrolset\control\nls\customlocale[pa] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[pa] Queries value: $HKLM \verb|\system| current controlset \verb|\control| nls \verb|\custom| locale[pa-in]|$ Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[pa-in] HKLM\system\currentcontrolset\control\nls\customlocale[gu] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gu] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[gu-in] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gu-in] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[or] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[or] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[or-in] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ta] HKLM\system\currentcontrolset\control\nls\extendedlocale[ta] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ta-in] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ta-in] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[te] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[te] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[te-in] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[te-in] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[kn] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[kn] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[kn-in] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[kn-in] HKLM\system\currentcontrolset\control\nls\customlocale[ml] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ml] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ml-in] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ml-in] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[as] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[as] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[as-in] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[mr] HKLM\system\currentcontrolset\control\nls\extendedlocale[mr] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[mr-in] Oueries value: Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sa] HKLM\system\currentcontrolset\control\nls\extendedlocale[sa] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[sa-in] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sa-in] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[mn] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mn] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[mn-mn] HKLM\system\currentcontrolset\control\nls\extendedlocale[mn-mn] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[bo] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[bo] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[bo-cn] HKLM\svstem\currentcontrolset\control\nls\extendedlocale[bo-cn] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[cv] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[cv] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[cy-gb] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[cy-gb] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[km] HKLM\system\currentcontrolset\control\nls\extendedlocale[km] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[km-kh] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[km-kh] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[lo] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lo] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[lo-la] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lo-la] Oueries value: $HKLM \verb|\system| current controlset| control \verb|\nls| custom locale[gl]|$ Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gl] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[gl-es] HKLM\system\currentcontrolset\control\nls\extendedlocale[gl-es] Queries value:

Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[kok] HKLM\system\currentcontrolset\control\nls\extendedlocale[kok] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[kok-in] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[kok-in] HKLM\system\currentcontrolset\control\nls\customlocale[syr] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[syrl HKI M\system\currentcontrolset\control\nls\customlocale[syr-syl Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[syr-sy] Oueries value: $\label{lem:hklmsystem} \verb|HKLM\| system \| current control set \| control \| nls \| custom \| locale[si]| \\$ Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[si] HKLM\system\currentcontrolset\control\nls\customlocale[si-lk] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[si-lk] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[iu] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[iu] HKLM\system\currentcontrolset\control\nls\customlocalefiu-latn-cal Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[iu-latn-cal Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[am] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[am] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[am-et] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[am-et] HKLM\system\currentcontrolset\control\nls\customlocale[tzm] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[tzm-latn-dz] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm-latn-dz] HKLM\system\currentcontrolset\control\nls\customlocale[ne] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ne] HKLM\system\currentcontrolset\control\nls\customlocale[ne-np] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ne-np] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[fy] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fy] HKLM\system\currentcontrolset\control\nls\customlocale[fy-nl] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fy-nl] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ps] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ps] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ps-af] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ps-afl] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fil] Oueries value: $\label{lem:hklmsystem} \\ \text{HKLM} \\ \text{system} \\ \text{control} \\ \text{nls} \\ \text{extendedlocale} \\ \text{[fil]} \\$ Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[fil-ph] HKLM\system\currentcontrolset\control\nls\extendedlocale[fil-ph] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[dv] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[dv] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[dv-mv] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[dv-mv] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[ha] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hal Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ha-latn-ng] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ha-latn-ng] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[yo] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[yo] HKLM\system\currentcontrolset\control\nls\customlocale[yo-ng] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[yo-ng] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[quz] HKLM\system\currentcontrolset\control\nls\extendedlocale[quz] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[quz-bol Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocalefguz-bol Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[nso] Oueries value: $\label{lem:hklmsystem} \verb|HKLM\| system \verb| current control \verb| should be a control \verb| ln ls \verb| extended locale [nso]| \\$ Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[nso-za] HKLM\system\currentcontrolset\control\nls\extendedlocale[nso-za] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ba] Oueries value: Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ba-ru] HKLM\system\currentcontrolset\control\nls\extendedlocale[ba-ru] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[]b] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[lb] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[lb-lu] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lb-lu] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[kl] HKLM\system\currentcontrolset\control\nls\extendedlocale[kl] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[kl-gl] Oueries value: Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ig] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ig] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ig-ng] HKLM\system\currentcontrolset\control\nls\extendedlocale[ig-ng] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ii] Queries value: $\label{lem:hklm} \verb+Kklm \+ system \+ control \+ ls \+ extended locale [ii]$ Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ii-cn] HKLM\system\currentcontrolset\control\nls\extendedlocale[ii-cn] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[arn] Queries value: $\label{lem:hklmsystem} \\ \text{HKLM} \\ \text{system} \\ \text{currentcontrolset} \\ \text{control} \\ \text{nls} \\ \text{extendedlocale} \\ [arn] \\$ Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[arn-cl] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[arn-cll Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[mohl Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[moh] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[moh-ca] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[br] HKLM\system\currentcontrolset\control\nls\extendedlocale[br] Queries value:

HKLM\system\currentcontrolset\control\nls\extendedlocale[br-fr] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ug] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ug] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ug-cn] HKLM\svstem\currentcontrolset\control\nls\extendedlocale[ug-cn] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[mi] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mi] Oueries value: $HKLM \verb|\system| current controlset \verb|\control| nls \verb|\custom| locale [mi-nz]|$ Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mi-nz] HKLM\system\currentcontrolset\control\nls\customlocale[oc] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[oc] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[oc-fr] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[oc-fr] HKLM\svstem\currentcontrolset\control\nls\customlocale[co] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[co] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[co-fr] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[co-fr] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[gsw] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gsw] HKLM\system\currentcontrolset\control\nls\customlocale[gsw-fr] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gsw-fr] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[sah] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sah] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sah-ru] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sah-rul Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[qut] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[qut] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[qut-gt] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[qut-gt] HKLM\system\currentcontrolset\control\nls\customlocale[rw] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[rw] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[rw-rw] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[rw-rw] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[wol Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[wol Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[wo-sn] Oueries value: $\label{lem:hklm} \verb+kklm \+ white-lem-control all lem: hkllm \+ white-lem: hkllm \+ w$ Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[prs] HKLM\system\currentcontrolset\control\nls\extendedlocale[prs] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[prs-af] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[prs-af] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[gd] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gd] HKLM\system\currentcontrolset\control\nls\customlocale[gd-gb] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[gd-gb] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000401] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000402] Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[5] HKLM\system\currentcontrolset\control\nls\locale[00000403] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[zh-tw] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-tw] Oueries value: HKLM\svstem\currentcontrolset\control\nls\locale[000004041] Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[9] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000405] Oueries value: $HKLM \ system \ current control set \ control \ nls \ language \ groups \ [2]$ Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000406] HKLM\system\currentcontrolset\control\nls\locale[00000407] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000408] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\language groups[4] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000409] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-es tradnl] HKLM\system\currentcontrolset\control\nls\extendedlocale[es-es_tradnl] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\locale[0000040a] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000040b] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000040c] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000040d] HKLM\system\currentcontrolset\control\nls\language groups[c] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000040e] Oueries value: Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000410] HKLM\svstem\currentcontrolset\control\nls\locale[000004111] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[7] HKLM\system\currentcontrolset\control\nls\locale[00000412] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\language groups[8] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000414] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000415] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000416] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000418] Oueries value: HKLM\svstem\currentcontrolset\control\nls\locale[00000419] Oueries value: HKCU\software\microsoft\windows\currentversion\ime\imtc70[] Oueries value:

HKLM\system\currentcontrolset\control\nls\customlocale[br-fr]

Oueries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ime \setminus imtc70 [useup dated field]$ Queries value:

HKCU\software\microsoft\windows\currentversion\ime\imtc70[typeenabledcheck]

Queries value:

HKCU\software\microsoft\windows\currentversion\ime\imtc70[pagecompressedinvalid]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\run[sonvagent]

Queries value:

e1e01c1f69b5}[enabledhcp]

HKLM\software\microsoft\rpc[maxrpcsize] Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

HKLM\system\setup[oobeinprogress] Queries value:

HKLM\system\setup[systemsetupinprogress] Oueries value:

HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Oueries value:

Oueries value:

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

 $\label{thm:local-continuous} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds folds \current \curr$ 65f9-4cf6-a03a-e3ef65729f3d}[name1

Queries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685db-1explorer\} \\ folder \\ descriptions \setminus \{3eb68db-1explorer\} \\ fold$ 65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]

Oueries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus explorer \setminus folder \\ descriptions \setminus folder \\ descriptions \setminus explorer \setminus folder \\ descriptions \setminus folder \\$ 65f9-4cf6-a03a-e3ef65729f3d}[description]

Queries value:

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

Queries value:

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

Oueries value:

 $HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus based \\ of the first o$ 65f9-4cf6-a03a-e3ef65729f3d}[infotip]

Oueries value:

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

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus based \\ of the first o$ 65f9-4cf6-a03a-e3ef65729f3d}[localredirectonlv] Oueries value:

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

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{3eb685db-microsoft \setminus windows \setminus current version \setminus \{3eb685db-microsoft \setminus \{3eb68db-microsoft \setminus \{3eb68db-microso$ 65f9-4cf6-a03a-e3ef65729f3d}[precreate]

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

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

folders[appdata]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\addressbook[uninstallstring] Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\adobe flash player activex[uninstallstring]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\adobe flash player activex[displayname]

Queries value:

 $HKLM \verb|\software| wow 6432 node \verb|\microsoft| windows \verb|\currentversion| uninstall \verb|\connection| and the state of the s$ manager[uninstallstring]

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\directdrawex[uninstallstring]

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \uninstall \font core \cite{thm:local-prop} Queries \ value:$

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie40[uninstallstring]
Oueries value:

 $\label{thm:local-problem} HKLM \software \wow 6432 node \microsoft \windows \current version \ninetall \ie 4 data \current version \ninetall \current \cur$

 $\label{thm:hkm} \begin{tabular}{ll} HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie5bakex[uninstallstring] \\ Oueries\ value: \end{tabular}$

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\iedata[uninstallstring]
Oueries value:

 $\label{thm:local_model} HKLM \software \wow 6432 node \microsoft \windows \current version \noine that \nobile option pack \cite{local_model} uninstall string \cite{local_model} Queries \ value:$

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\schedulingagent[uninstallstring]
 Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\wic[uninstallstring]
 Oueries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \uninstall \ \{196bb40d-1578-3d01-b289-befc77a11a1e\} \ [uninstall string]$

Queries value:

Queries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \uninstall \end{26a} 24ae 4-039d-4ca 4-87b 4-2f83 21700 2ff \end{27b} \[uninstall \string]$

Oueries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \wirdows \current version \uninstall \end{26a} 24ae 4-039d-4ca 4-87b 4-2f83 21700 2ff \end{26a} [display name]$

Queries value:

 $\label{thm:local-condition} HKLM \software \wow 6432 node \windows \current version \uninstall \end{tabular} $$4a03706f-666a-4037-7777-5f2748764d10 \current version \current$

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \uninstall \ \{90120000-0020-0409-0000-00000000ff1ce\} \ [display name]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \uninstall \end{constraints} \{90850409-6000-11d3-8cfe-0150048383c9\} [uninstall \string]$

Queries value:

 $\label{thm:main} HKL^{M}\ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ \{90850409-6000-11d3-8cfe-0150048383c9\} \ [display name]$

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \uninstall \ \{95120000-003f-0409-0000-0000000ff1ce\} \ [uninstall string]$

Queries value:

 $\label{thm:local-bound} $HKLM \sim (432 node) - 003f-0409-0000-0000000fflce \ [displayname] $$$

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \uninstall \ \{95140000-00af-0409-0000-0000000ff1ce\}[display name]$

Queries value:

 $\label{local-base-rad7-1033-7b44-a93000000001} \\ [uninstallstring]$

Queries value:

 $\label{local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \uninstall \end{constraint} \{ac76ba86-7ad7-1033-7b44-a9300000001\} \cite{Constraint} \end{constraint} Ac76ba86-7ad7-1033-7b44-a93000000001\} \cite{Constraint} \end{constraint} \end{constraint} Ac76ba86-7ad7-1033-7b44-a93000000001\} \cite{Constraint} \end{constraint} \end{constr$

Queries value:

 $\label{thm:local-bound} HKLM \software \www 6432 node \microsoft \windows \current version \explorer \folder descriptions \fill 1532785-66 ba-4fcf-9d55-7b8e7f157091 \cite{local-bound} \cite{local-bound$

Queries value:

 $\label{thm:local-bound} HKLM \software \ww 6432 node \microsoft \windows \current version \explorer \folder descriptions \fi1b32785-66ba-4fcf-9d55-7b8e7f157091 \[name]$

Queries value:

 $\label{thm:hammon} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fiba-24fcf-9d55-7b8e7f157091 \[parent folder]$

Queries value:

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM \software \ww 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

 $\label{thm:local-bound} HKLM \software \www 6432 node \microsoft \windows \current version \explorer \folder descriptions \fill 152785-66 ba-4fcf-9d55-7b8e7f157091 \cite{thm:local-bound} [infotip]$

Oueries value:

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

Queries value:

 $\label{local-hkklm} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fiba-2785-6798-7788-7757091 \cite{hkklm} icon \cite{hkklm} \end{subarray} The local \cite{hkklm} \cite{hkklm} \end{subarray} The local \cite{hkklm} \cite{hkk$

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

Queries value:

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

Oueries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]

Oueries value:

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

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

Oueries value:

 $HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{f1b32785-1000\} \\ f1b32785-1000 \\ f1b32785-1$ 6fba-4fcf-9d55-7b8e7f157091}[precreate]

Queries value:

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

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

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]

Oueries value:

 $\label{thm:local-ham} HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-b24764, b24764, b247644, b24764, b$ 6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]

Queries value:

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

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

folders[local appdata]

Oueries value:

fdc1-4dc3-a9dd-070d1d495d97}[category]

Oueries value:

fdc1-4dc3-a9dd-070d1d495d97}[name]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[description]

Queries value:

fdc1-4dc3-a9dd-070d1d495d97}[relativepath]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[parsingname]

Queries value:

 $HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{62ab5d82-1000\} \\ node \setminus folder \\ node \setminus f$ fdc1-4dc3-a9dd-070d1d495d97}[infotip1 Oueries value:

fdc1-4dc3-a9dd-070d1d495d97}[localizedname]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[icon1

Queries value:

fdc1-4dc3-a9dd-070d1d495d97}[security]

Oueries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \label{lem:hkklm}$ fdc1-4dc3-a9dd-070d1d495d97}[streamresource]

Oueries value:

fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]

fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]

Oueries value:

 $HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{62ab5d82-1000\} \\ node \setminus folder \\ node \setminus f$ fdc1-4dc3-a9dd-070d1d495d97}[roamable]

Queries value:

fdc1-4dc3-a9dd-070d1d495d97}[precreate]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[stream]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]

Oueries value:

fdc1-4dc3-a9dd-070d1d495d97}[attributes]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-

fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]

Oueries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \f$

Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

Oueries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \gamma 6905e63b6-c1bf-494e-b29c-65b732d3d21a \gamma [category]$

Queries value:

 $\label{thm:local-bound} HKLM \software \www6432 node \microsoft \windows \current version \explorer \folder descriptions \cdots \folder \cdots \folder \folder \cdots \folder \folde$

Queries value:

Oueries value:

 $\label{thm:local-ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\calebright{0.5}{0.5} \cite{1.5} \cite{1.5}$

Oueries value:

 $\label{thm:local-bound} HKLM \software \ww 6432 node \microsoft \windows \current version \explorer \folder descriptions \gray \folder \fold$

Queries value

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[parsingname]

Queries value:

 $\label{thm:local-bound} HKLM\software\wow6432\node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\$

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM \software \www 6432 node \microsoft \windows \current version \explorer \folder descriptions \gray \folder \fol$

Queries value:

 $HKLM \software \www6432 node \microsoft \windows \current version \explorer \folder descriptions \called{HKLM} for the sum of the$

Oueries value:

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \end{4905} $\{905e63b6-c1bf-494e-b29c-65b732d3d21a\} \ [stream resource type]$

Queries value:

 $HKLM \software \www6432 node \microsoft \windows \current version \explorer \folder descriptions \called \cite{thm:cond} for the large \cite{thm:cond} for$

Queries value:

Queries value:

 $\label{thm:local-basis} HKLM \software \www6432 node \microsoft \windows \current version \explorer \folder descriptions \cdots \folder \cdots \folder \folder \cdots \folder \folder \cdots \folder \folder$

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432\node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[stream]}$

Queries value:

 $\label{thm:local-bound} HKLM \software \www 6432 node \microsoft \windows \current version \explorer \folder descriptions \gamma \figure{100} \end{100} folder \folder \folder \gamma \gamma$

Queries value:

 $\label{thm:local-basis} HKLM \software \www6432 node \microsoft \windows \current version \explorer \folder descriptions \go 5e63b6-c1bf-494e-b29c-65b732d3d21a \go fattributes \go fattribu$

Queries value:

 $\label{thm:local-problem} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \gray \folder \folder \gray \g$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}\initfolderhandler1

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]

Queries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\name1

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

 $\label{thm:local-problem} HKLM \software \www 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \folder$

Queries value:

 $\label{thm:local-problem} HKLM \software \www 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{7} c5a40 ef-a0fb-4bfc-874a-c0f2e0b9fa8e \footnote{1}$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\}[parsing name]$

Oueries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} \ [icon]$

Oueries value:

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

Oueries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Oueries value:

Oueries value:

 $\label{thm:local-continuous} HKLM \software \www6432 node \mbox{\current version} \explorer \folder descriptions \footnote{\current version} \explorer \folder descriptions \footnote{\current version} \explorer \folder descriptions \footnote{\current version} \explorer \footnote{\current version}$

Queries value:

 $\label{thm:local-bound} HKLM \software \ww 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

 $\label{thm:local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]$

Queries value:

 $\label{thm:local-problem} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{2} a 0 fb-4b fc-874a-c0 f2e 0b 9 fa 8e \[publish expanded path]$

Queries value

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder type id]$

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[category]

Queries value:

 $\label{local-prop} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\ff7f1ed05-9f6d-47a2-aaae-29d317c6f066\fname]$

Oueries value:

Queries value:

Queries value:

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM \software \ww 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

 $\label{thm:local-continuous} HKLM \software \ww 6432 node \mbox{f7f1ed05-9f6d-47a2-aaae-29d317c6f066} [localized name]$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[icon]

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1} f7f1ed05-9f6d-47a2-aaae-29d317c6f066 \[security]$

Oueries value

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066\fstreamresourcel

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[streamresourcetype]

Oueries value:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\ff7f1ed05-9f6d-47a2-aaae-29d317c6f066\\[localredirectonly]$

Queries value:

 $\label{thm:local-bound} HKLM \software \www6432 node \microsoft \windows \current version \explorer \folder descriptions \folded \current version \explorer \folder descriptions \folded \current \curr$

Queries value:

 $\label{thm:local-bound} HKLM \software \ww 6432 node \microsoft \windows \current version \explorer \folder descriptions \folded \folds \fol$

Oueries value:

 $\label{thm:hklm:software} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \ff7f1ed05-9f6d-47a2-aaae-29d317c6f066 \[stream]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f7f1ed05-9f6d-47a2-aaae-29d317c6f066\} [publish expanded path]$

Queries value:

Oueries value:

 $\label{thm:local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescrip$

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion[commonfilesdir]

Oueries value:

 $\label{thm:local-bound} HKLM \software \www 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{2} each \footnote{2}{2} each \footnote{2} each \footnot$

Oueries value:

 $HKLM \software \wwo6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Oueries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]

Queries value:

Oueries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1} Gebox \footnote{2} Gebox \fo$

Queries value:

 $\label{thm:local-bound} HKLM \software \www6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

Oueries value:

 $\label{thm:local-prop} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\fold$

Oueries value:

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

Oueries value

 $\label{thm:local-ham} $$HKLM\software\wow6432\node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\[streamresource]$

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{2} e6c858f-0e22-4760-9afe-ea3317b67173 \footnote{1}{2} is tream resource type]$

Queries value:

 $\label{thm:local-continuous} HKLM \software \www 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{5}e6c858f-0e22-4760-9afe-ea3317b67173} \ [local redirectionly]$

Queries value:

 $\label{thm:local-bound} HKLM \software \www 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{5}e6c858f-0e22-4760-9afe-ea3317b67173} \[roamable \]$

Queries value:

 $\label{thm:local-prop} HKLM \software \ww 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder descriptions \folder \folder$

Queries value:

 $\label{thm:local-bound} HKLM \software \ww 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

 $\label{thm:local-problem} HKLM \software \ww 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \current \folder \folder \current \folder \current \folder \current \folder \$

Queries value:

 $\label{thm:local-bound} HKLM \software \www 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{2}{4760-9} af e-ea3317 b 67173 \footnote{1}{2}{1}$

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

980053277-1733835069-2361817685-1001[profileimagepath]

Queries value: HKLM\software\wow6432node[debuglogpath]
Queries value: HKLM\software\wow6432node[debugloglevel]
Queries value: HKLM\software\wow6432node[enabledebuglog]

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip6[winsock 2.0 provider id]

Queries value:

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]

Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\addressbook[addressbook]

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\connection

manager[connection manager] Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ direct drawex \ [direct drawex]$ Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\fontcore[fontcore] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie40[ie40] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie4data[ie4data] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie5bakex[ie5bakex] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mobileoptionpack[mobileoptionpack] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\schedulingagent[schedulingagent] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\wic[wic] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ \{4a03706f-666a-4037-7777-1844, and \ an all \ an a$ $5f2748764d10 \} [\, \{ 4a03706f - 666a - 4037 - 7777 - 5f2748764d10 \} \,]$ Queries value: $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-based \\ in the folder \\ descriptions \\ descript$ db2c-424c-b029-7fe99a87c641}[category] Oueries value: $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-bc1, b4bfcc3a-bc2, b4bfcc3a-bc2$ db2c-424c-b029-7fe99a87c641}[name] Queries value: db2c-424c-b029-7fe99a87c641}[parentfolder] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f$ db2c-424c-b029-7fe99a87c641}[description] Oueries value: $HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-bc1, b4bfcc3a-bc2, b4bfcc3a-bc2,$ db2c-424c-b029-7fe99a87c641}[relativepath] Oueries value: db2c-424c-b029-7fe99a87c641}[parsingname] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[infotip] Queries value: $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-based \\ in the folder \\ descriptions \\ descript$ db2c-424c-b029-7fe99a87c641}[localizedname] Queries value: db2c-424c-b029-7fe99a87c641}[icon] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[security] Queries value: $HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-bc1, b4bfcc3a-bc2, b4bfcc3a-bc2,$ db2c-424c-b029-7fe99a87c641}[streamresource] Oueries value: $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \la$ db2c-424c-b029-7fe99a87c641}[streamresourcetype] Queries value: db2c-424c-b029-7fe99a87c641}[localredirectonly] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f$ db2c-424c-b029-7fe99a87c641}[roamable] Oueries value: $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \label{lem:hkklm}$ db2c-424c-b029-7fe99a87c641}[precreate] Oueries value: db2c-424c-b029-7fe99a87c641}[stream] $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f$ db2c-424c-b029-7fe99a87c641}[publishexpandedpath] Oueries value: $HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-bc1, b4bfcc3a-bc2, b4bfcc3a-bc2,$ db2c-424c-b029-7fe99a87c641}[attributes] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f$ db2c-424c-b029-7fe99a87c641}[foldertypeid] HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[initfolderhandler]

HKCU\software\microsoft\windows\currentversion\explorer\user shell Queries value: folders[desktop] Oueries value: 0080adb32ff4}\inprocserver32] Oueries value: $HKLM \setminus software \setminus classes \\ [clsid \setminus \{11c1d741-a95b-11d2-8a80-a95b-11d2-8a00-a95b-11d2-8a00-a95b-11d2-8a00-a9$ 0080adb32ff4}\inprocserver32] Queries value: HKCU\software\classes\[ftp++.link\shell\open\command] HKLM\software\classes[ftp++.link\shell\open\command] Queries value:

Sets/Creates value:

 $\label{lem:hkcu} HKCU \software \microsoft \windows \current version \mbox{\current} elbel{lem:hkcu} Sets/Creates \ value:$

HKCU\software\microsoft\windows\currentversion\ime\imtc70[recordcompressedactive]
 Sets/Creates value:

Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\run[sonyagent]

Value changes: