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\SvcctrlStartEvent_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\SysWOW64
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\imm32.dll
Opens:	C:\Windows\Temp\752d6fe81122349daf998a56f48e0b38.exe
Opens:	C:\windows\temp\DNSAPI.dll
Opens:	C:\Windows\SysWOW64\dnsapi.dll
Opens:	C:\windows\temp\IPHLPAPI.DLL
Opens:	C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens:	C:\windows\temp\WINNSI.DLL
Opens:	C:\Windows\SysWOW64\winnsi.dll
Opens:	C:\windows\temp\MSWSOCK.dll
Opens:	C:\Windows\SysWOW64\mswsock.dll
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
Opens:	C:\Windows\System32\C_932.NLS
Opens:	C:\Windows\System32\C_949.NLS
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

```
  Opens:                  C:\Windows\system\wpcap.dll
  Opens:                  C:\Windows\wpcap.dll
  Opens:                  C:\Windows\SysWOW64\Wbem\wpcap.dll
  Opens:                  C:\Windows\SysWOW64\WindowsPowerShell\v1.0\wpcap.dll
  Opens:                  C:\
  Opens:                  C:\$Recycle.Bin
  Opens:                  C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001
  Opens:                  C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\desktop.ini
  Opens:                  C:\Users\Admin\AppData\Roaming
  Opens:                  C:\Users\Admin\AppData\Roaming\FlashFXP\3\Sites.dat
  Opens:                  C:\Users\Admin\AppData\Roaming\FlashFXP\3\Quick.dat
  Opens:                  C:\Users\Admin\AppData\Roaming\FlashFXP\3\History.dat
  Opens:                  C:\Users\Admin\AppData\Roaming\FlashFXP\4\Sites.dat
  Opens:                  C:\Users\Admin\AppData\Roaming\FlashFXP\4\Quick.dat
  Opens:                  C:\Users\Admin\AppData\Roaming\FlashFXP\4\History.dat
  Opens:                  C:\Documents and Settings\
  Opens:                  C:\dump.pcap
  Opens:                  C:\exception.log
  Opens:                  C:\Users\Admin\AppData\Local
  Opens:                  C:\Users\Admin\AppData\Local\BulletProof Software\BulletProof FTP Client
2009\sites\Bookmarks\
  Opens:                  C:\Users\Admin\AppData\Roaming\BulletProof Software\BulletProof FTP
Client 2009\sites\Bookmarks\
  Opens:                  C:\windows\temp\profapi.dll
  Opens:                  C:\Windows\SysWOW64\profapi.dll
  Opens:                  C:\ProgramData
  Opens:                  C:\ProgramData\BulletProof Software\BulletProof FTP Client
2009\sites\Bookmarks\
  Opens:                  C:\Users\Admin\AppData\Local\BulletProof Software\BulletProof FTP
Client\2010\sites\Bookmarks\
  Opens:                  C:\Users\Admin\AppData\Roaming\BulletProof Software\BulletProof FTP
Client\2010\sites\Bookmarks\
  Opens:                  C:\ProgramData\BulletProof Software\BulletProof FTP
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
  Opens:                  C:\Program Files\Common Files\Microsoft Shared\ink\Alphabet.xml
  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
  Opens:                  C:\ProgramData\BulletProof Software\BulletProof FTP Client
2009\Default.bps
  Opens:                  C:\Users\Admin\AppData\Local\BulletProof Software\BulletProof FTP
Client\2010\Default.bps
  Opens:                  C:\Users\Admin\AppData\Roaming\BulletProof Software\BulletProof FTP
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
  Opens:                  C:\Users\Admin\AppData\Roaming\GPSoftware\Directory
Opus\Layouts\System\default.oll
  Opens:                  C:\Users\Admin\AppData\Local\GPSoftware\Directory
Opus\ConfigFiles\ftp.oxc
  Opens:                  C:\Users\Admin\AppData\Local\GPSoftware\Directory
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
  Opens:                  C:\Users\Admin\AppData\Roaming\BitKinex\bitkinex.ds
  Opens:                  C:\Users\Admin\AppData\Roaming\GlobalSCAPE\CuteFTP
  Opens:                  C:\Users\Admin\AppData\Roaming\GlobalSCAPE\CuteFTP Pro
  Opens:                  C:\Users\Admin\AppData\Roaming\GlobalSCAPE\CuteFTP Lite
  Opens:                  C:\ProgramData\GlobalSCAPE\CuteFTP
  Opens:                  C:\ProgramData\GlobalSCAPE\CuteFTP Pro
  Opens:                  C:\ProgramData\GlobalSCAPE\CuteFTP Lite
  Opens:                  C:\Program Files (x86)
  Opens:                  C:\Program Files (x86)\CuteFTP
  Opens:                  C:\Windows\win.ini
  Opens:                  C:\Program Files (x86)\Common Files
  Opens:                  C:\Program Files (x86)\Common Files\Ipswitch\WS_FTP
  Opens:                  C:\Users\Admin\AppData\Roaming\Ipswitch\WS_FTP\Sites
  Opens:                  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:                  C:\Users\Admin\AppData\Local\Ipswitch\WS_FTP\Sites
  Opens:                  C:\Users\Admin\AppData\Local\Ipswitch\WS_FTP Home\Sites
  Opens:                  C:\Users\Admin\AppData\Roaming\NetDrive\NDSites.ini
  Opens:                  C:\ProgramData\NetDrive\NDSites.ini
  Opens:                  C:\Users\Admin\AppData\Local\NetDrive\NDSites.ini
  Opens:                  C:\Users\Admin\AppData\Roaming\FileZilla\sitemanager.xml
  Opens:                    C:\Users\Admin\AppData\Roaming\FileZilla\recentservers.xml
  Opens:                    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
2.0\Favorites\Favorites.dat
  Opens:                    C:\Users\Admin\AppData\Roaming\SmartFTP\History.dat
  Opens:                    C:\Users\Admin\AppData\Roaming\SmartFTP\Client 2.0\Favorites\
  Opens:                    C:\ProgramData\SmartFTP\Favorites.dat
  Opens:                    C:\ProgramData\SmartFTP\Client 2.0\Favorites\Favorites.dat
  Opens:                    C:\ProgramData\SmartFTP\History.dat
  Opens:                    C:\ProgramData\SmartFTP\Client 2.0\Favorites\
  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
  Opens:                    C:\Users\Default User
  Opens:                    C:\Users\Default
  Opens:                    C:\Users\Admin\AppData\Roaming\Bitcoin\wallet.dat
  Opens:                    C:\ProgramData\APPDATA\ROAMING\BITCOIN\WALLET.DAT
  Opens:                    C:\Users\Default\AppData\Roaming\Bitcoin\wallet.dat
  Opens:                    C:\Users\Public\AppData\Roaming\Bitcoin\wallet.dat
  Opens:                    C:\Windows\wcx_ftp.ini
  Opens:                    C:\Windows\Windows Commander\wcx_ftp.ini
  Opens:                    C:\Windows\Total Commander\wcx_ftp.ini
  Opens:                    C:\Users\Admin
  Opens:                    C:\Users\Admin\wcx_ftp.ini
  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
  Opens:                    C:\Users\Admin\AppData\Roaming\Total Commander\GHISLER\wcx_ftp.ini
  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
  Opens:                    C:\Users\Admin\AppData\Local\Total Commander\GHISLER\wcx_ftp.ini
  Opens:                    C:\Users\Admin\AppData\Roaming\AceBIT\
  Opens:                    C:\ProgramData\AceBIT\
  Opens:                    C:\Windows\SysWOW64\tzres.dll
  Opens:                    C:\Windows\SysWOW64\en-US\tzres.dll.mui
  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
  Opens:                    C:\Program Files\Common Files\Microsoft Shared\ink\ar-SA\tipresx.dll.mui
  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
  Opens:                    C:\Program Files\Common Files\Microsoft Shared\ink\Content.xml
  Opens:                    C:\Windows\SysWOW64\wship6.dll
  Opens:                    C:\Program Files\Common Files\Microsoft Shared\ink\cs-CZ
  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
  Opens:                    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:                    C:\Program Files\Common Files\Microsoft Shared\ink\de-DE\tipresx.dll.mui
  Opens:                    C:\Program Files\Common Files\Microsoft Shared\ink\el-GR
  Opens:                    C:\Program Files\Common Files\Microsoft Shared\ink\el-GR\tipresx.dll.mui
  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
  Opens:                    C:\Program Files\Common Files\Microsoft Shared\ink\en-US\InkObj.dll.mui
  Opens:                    C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\InkWatson.exe.mui
  Opens:                    C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\InputPersonalization.exe.mui
  Opens:                    C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\IPSEventLogMsg.dll.mui
  Opens:                    C:\Users\Admin\AppData\Roaming\Google\Chrome\
  Opens:                    C:\Users\Admin\AppData\Local\Google\Chrome\
  Opens:                    C:\ProgramData\Google\Chrome\
  Opens:                    C:\Users\Admin\AppData\Roaming\Chromium\
  Opens:                    C:\Users\Admin\AppData\Local\Chromium\
  Opens:                    C:\ProgramData\Chromium\
  Opens:                    C:\Users\Admin\AppData\Roaming\ChromePlus\
  Opens:                    C:\Users\Admin\AppData\Local\ChromePlus\
  Opens:                    C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\IpsMigrationPlugin.dll.mui
  Opens:                    C:\ProgramData\ChromePlus\
  Opens:                    C:\Users\Admin\AppData\Roaming\Bromium\
  Opens:                    C:\Users\Admin\AppData\Local\Bromium\
  Opens:                    C:\ProgramData\Bromium\
  Opens:                    C:\Users\Admin\AppData\Roaming\Nichrome\
  Opens:                 C:\Users\Admin\AppData\Local\Nichrome\
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\ink\en-US\micaut.dll.mui
  Opens:                 C:\ProgramData\Nichrome\
  Opens:                 C:\Users\Admin\AppData\Roaming\Comodo\
  Opens:                 C:\Users\Admin\AppData\Local\Comodo\
  Opens:                 C:\ProgramData\Comodo\
  Opens:                 C:\Users\Admin\AppData\Roaming\RockMelt\
  Opens:                 C:\Users\Admin\AppData\Local\RockMelt\
  Opens:                 C:\ProgramData\RockMelt\
  Opens:                 C:\Users\Admin\AppData\Roaming\MapleStudio\ChromePlus\
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\ink\en-US\mip.exe.mui
  Opens:                 C:\Users\Admin\AppData\Local\MapleStudio\ChromePlus\
  Opens:                 C:\ProgramData\MapleStudio\ChromePlus\
  Opens:                 C:\Users\Admin\AppData\Roaming\browser.yandex\
  Opens:                 C:\Users\Admin\AppData\Local\browser.yandex\
  Opens:                 C:\ProgramData\browser.yandex\
  Opens:                 C:\Users\Admin\Desktop
  Opens:                 C:\Users\Admin\AppData\Roaming\Adobe
  Opens:                 C:\Users\Admin\AppData\Roaming\Adobe\Acrobat
  Opens:                 C:\Users\Admin\AppData\Roaming\Adobe\Acrobat\9.0
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\ink\en-
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
  Opens:                 C:\Users\Admin\AppData\Roaming\Adobe\Acrobat\9.0\JavaScripts
  Opens:                 C:\Users\Admin\AppData\Roaming\Identities
  Opens:                 C:\Users\Admin\AppData\Roaming\Identities\{9506AC1B-447F-4459-900E-
43BE84A098E7}
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\ink\en-US\rtscom.dll.mui
  Opens:                 C:\Users\Admin\AppData\Roaming\Media Center Programs
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft
  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
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-980053277-
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
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick
Launch\User Pinned
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick
Launch\User Pinned\ImplicitAppShortcuts
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick
Launch\User Pinned\TaskBar
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\MMC
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Network
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk\_hiddenPbk
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Office
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Office\Recent
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Protect
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Protect\S-1-5-21-980053277-
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
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\ink\en-US\TipBand.dll.mui
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates
  Opens:                 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:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
  Opens:                 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:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\Low
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Network Shortcuts
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\ink\en-US\tipresx.dll.mui
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE\Low
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\ink\en-US\TipTsf.dll.mui
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\ink\es-ES
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\ink\es-ES\tipresx.dll.mui
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\SendTo
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories\Accessibility
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories\System Tools
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Administrative Tools
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Maintenance
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Templates
  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
  Opens:                  C:\Users\Admin\AppData\Roaming\Oracle\Java\Uninstall
  Opens:                  C:\Users\Admin\AppData\Local\Adobe
  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
  Opens:                  C:\Users\Admin\AppData\Local\Adobe\Acrobat\9.0
  Opens:                  C:\Users\Admin\AppData\Local\Adobe\Acrobat\9.0\Cache
  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\
  Opens:                  C:\Users\Admin\AppData\Local\History\
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Credentials
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Event Viewer
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Event Viewer\Views
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Feeds
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Feeds\Feeds for United States~
  Opens:                  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:                  C:\Users\Admin\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-
666AE6A92D3D}~
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-
666AE6A92D3D}~\WebSlices~
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Feeds Cache
  Opens:                  C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions
  Opens:                  C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\auxpad
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Feeds Cache\8CQ8LU44
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Feeds Cache\GH2Y6ANO
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Feeds Cache\JH8KG3LN
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Feeds Cache\Q0UWLZUG
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\auxpad\auxbase.xml
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\DOMStore
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\2UWQWYVI
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\K0WHMEP2
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\NLN2O6FE
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\VU73CBGV
  Opens:                  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:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\auxpad.xml
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Recovery\High\Active
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\Recovery\High\Last Active
  Opens:                  C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\keypad\ea.xml
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\keypad\keypadbase.xml
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\Recovery\Last
Active
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Media Player
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\keypad\kor-kor.xml
  Opens:                  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-
US\000207D6
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\keypad.xml
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Office
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Office\12.0
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Office\14.0
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\TaskSchedulerConfig
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\1033
  Opens:                 C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base.xml
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Burn
  Opens:                 C:\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
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\GameExplorer
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Ringtones
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\AntiPhishing
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S
  Opens:                 C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\baseAltGr_rtl.xml
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J
  Opens:                 C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base_altgr.xml
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.MSO
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low
  Opens:                 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
  Opens:                 C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base_ca.xml
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5\175TAQYU
  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
  Opens:                 C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base_jpn.xml
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized\C
  Opens:                 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
Files\Virtualized\C\Users\Admin\AppData
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized\C\Users\Admin\AppData\Roaming
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized\C\Users\Admin\AppData\Roaming\Microsoft
  Opens:                 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
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized\C\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE\Low
  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
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ReportQueue
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ReportQueue\NonCritical_VCRED000.EXE_8fab9a8aafb14ca3aa6b78edacd1d07896b1794_cab_088f7855
  Opens:                 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:                 C:\Users\Admin\AppData\Local\Microsoft\Windows Mail\Stationery
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows Media
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows Media\12.0
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows Sidebar
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows Sidebar\Gadgets
  Opens:                  C:\Users\Admin\AppData\Local\Programs
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base_kor.xml
  Opens:                  C:\Users\Admin\AppData\Local\Programs\Common
  Opens:                  C:\Users\Admin\AppData\Local\Temp
  Opens:                  C:\Users\Admin\AppData\Local\Temp\gen_py
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base_rtl.xml
  Opens:                  C:\Users\Admin\AppData\Local\Temp\gen_py\2.7
  Opens:                  C:\Users\Admin\AppData\Local\Temp\hsperfdata_Admin
  Opens:                  C:\Users\Admin\AppData\Local\Temp\Low
  Opens:                  C:\Users\Admin\AppData\Local\Temp\Microsoft Visual C++ 2010 x64
Redistributable Setup_10.0.30319
  Opens:                  C:\Users\Admin\AppData\Local\Temp\Microsoft Visual C++ 2010 x86
Redistributable Setup_10.0.30319
  Opens:                  C:\Users\Admin\AppData\Local\Temp\WPDNSE
  Opens:                  C:\Users\Admin\AppData\Local\Temp\{68d3b73e-efd0-4f70-a22c-4831abb9599a}
  Opens:                  C:\Users\Admin\AppData\Local\Temporary Internet Files\
  Opens:                  C:\Users\Admin\AppData\Local\VirtualStore
  Opens:                  C:\ProgramData\Adobe
  Opens:                  C:\ProgramData\Adobe\Acrobat
  Opens:                  C:\ProgramData\Adobe\Acrobat\9.0
  Opens:                  C:\ProgramData\Adobe\Acrobat\9.0\Replicate
  Opens:                  C:\ProgramData\Adobe\Acrobat\9.0\Replicate\Security
  Opens:                  C:\ProgramData\Adobe\Reader
  Opens:                  C:\ProgramData\Adobe\Reader\9.3
  Opens:                  C:\ProgramData\Adobe\Reader\9.3\ARM
  Opens:                  C:\ProgramData\Adobe\Reader\9.3\ARM\26091
  Opens:                  C:\ProgramData\Adobe\Updater6
  Opens:                  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\
  Opens:                  C:\ProgramData\Favorites\
  Opens:                  C:\ProgramData\Microsoft
  Opens:                  C:\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
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\ko-kr.xml
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\zh-changjei.xml
  Opens:                  C:\ProgramData\Microsoft\Crypto
  Opens:                  C:\ProgramData\Microsoft\Crypto\DSS
  Opens:                  C:\ProgramData\Microsoft\Crypto\DSS\MachineKeys
  Opens:                  C:\ProgramData\Microsoft\Crypto\Keys
  Opens:                  C:\ProgramData\Microsoft\Crypto\RSA
  Opens:                  C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
  Opens:                  C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18
  Opens:                  C:\ProgramData\Microsoft\Device Stage
  Opens:                  C:\ProgramData\Microsoft\Device Stage\Device
  Opens:                  C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-
97838f1b04b0}
  Opens:                  C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-
4d3decd87120}
  Opens:                  C:\ProgramData\Microsoft\Device Stage\Task
  Opens:                  C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-
d8f2cf8722c9}
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\zh-dayi.xml
  Opens:                  C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-
d8f2cf8722c9}\en-US
  Opens:                  C:\ProgramData\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-
1775fb1a7a42}
  Opens:                  C:\ProgramData\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-
1775fb1a7a42}\en-US
  Opens:                  C:\ProgramData\Microsoft\DeviceSync
  Opens:                  C:\ProgramData\Microsoft\DRM
  Opens:                  C:\ProgramData\Microsoft\DRM\Server
  Opens:                  C:\ProgramData\Microsoft\eHome
  Opens:                  C:\ProgramData\Microsoft\eHome\logs
  Opens:                  C:\ProgramData\Microsoft\Event Viewer
  Opens:                  C:\ProgramData\Microsoft\Event Viewer\Views
  Opens:                  C:\ProgramData\Microsoft\Event Viewer\Views\ApplicationViewsRootNode
  Opens:                  C:\ProgramData\Microsoft\Event Viewer\Windows Logs
  Opens:                  C:\ProgramData\Microsoft\IdentityCRL
  Opens:                  C:\ProgramData\Microsoft\IlsCache
  Opens:                  C:\ProgramData\Microsoft\Media Player
  Opens:                  C:\ProgramData\Microsoft\MF
  Opens:                  C:\ProgramData\Microsoft\Network
  Opens:                  C:\ProgramData\Microsoft\Network\Connections
  Opens:                  C:\ProgramData\Microsoft\Network\Downloader
  Opens:                  C:\ProgramData\Microsoft\PlayReady
  Opens:                  C:\ProgramData\Microsoft\RAC
  Opens:                  C:\ProgramData\Microsoft\RAC\Outbound
  Opens:                  C:\ProgramData\Microsoft\RAC\PublishedData
  Opens:                  C:\ProgramData\Microsoft\RAC\StateData
  Opens:                 C:\ProgramData\Microsoft\RAC\Temp
  Opens:                 C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\zh-phonetic.xml
  Opens:                 C:\ProgramData\Microsoft\Search
  Opens:                 C:\ProgramData\Microsoft\Search\Data
  Opens:                 C:\ProgramData\Microsoft\Search\Data\Applications
  Opens:                 C:\ProgramData\Microsoft\Search\Data\Applications\Windows
  Opens:                 C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Config
  Opens:                 C:\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs
  Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex
  Opens:                 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:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer
  Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles
  Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\PropMap
  Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\SecStore
  Opens:                 C:\ProgramData\Microsoft\Search\Data\Temp
  Opens:                 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:                 C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\numbers\numbase.xml
  Opens:                 C:\ProgramData\Microsoft\Vault
  Opens:                 C:\ProgramData\Microsoft\Windows
  Opens:                 C:\ProgramData\Microsoft\Windows\AIT
  Opens:                 C:\ProgramData\Microsoft\Windows\Caches
  Opens:                 C:\ProgramData\Microsoft\Windows\DeviceMetadataStore
  Opens:                 C:\ProgramData\Microsoft\Windows\DeviceMetadataStore\en-US
  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
  Opens:                 C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics
  Opens:                 C:\ProgramData\Microsoft\Windows\Ringtones
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskmenu
  Opens:                 C:\Program Files\Common Files\Microsoft
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
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu\Programs
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories
  Opens:                 C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\Accessories\Accessibility
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\System
Tools
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Tablet
PC
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows
PowerShell
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative
Tools
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Games
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Python 2.7
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
  Opens:                 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Tablet PC
  Opens:                 C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\oskmenu.xml
  Opens:                 C:\ProgramData\Microsoft\Windows\Templates
  Opens:                 C:\ProgramData\Microsoft\Windows\WER
  Opens:                 C:\ProgramData\Microsoft\Windows\WER\ReportArchive
  Opens:                 C:\ProgramData\Microsoft\Windows\WER\ReportQueue
  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
  Opens:                 C:\ProgramData\Microsoft\Windows Defender\Definition Updates
  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}
  Opens:                 C:\ProgramData\Microsoft\Windows Defender\LocalCopy
  Opens:                 C:\ProgramData\Microsoft\Windows Defender\Quarantine
  Opens:                 C:\ProgramData\Microsoft\Windows Defender\Scans
  Opens:                 C:\ProgramData\Microsoft\Windows Defender\Scans\History
  Opens:                 C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\osknumpad
```

```
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\osknumpad\osknumpadbase.xml
  Opens:                  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
  Opens:                  C:\ProgramData\Microsoft\Windows NT
  Opens:                  C:\ProgramData\Microsoft\Windows NT\MSFax
  Opens:                  C:\ProgramData\Microsoft\Windows NT\MSFax\ActivityLog
  Opens:                  C:\ProgramData\Microsoft\Windows NT\MSFax\Common Coverpages
  Opens:                  C:\ProgramData\Microsoft\Windows NT\MSFax\Common Coverpages\en-US
  Opens:                  C:\ProgramData\Microsoft\Windows NT\MSFax\Inbox
  Opens:                  C:\ProgramData\Microsoft\Windows NT\MSFax\Queue
  Opens:                  C:\ProgramData\Microsoft\Windows NT\MSFax\SentItems
  Opens:                  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:                  C:\ProgramData\Microsoft\WwanSvc
  Opens:                  C:\ProgramData\Microsoft\WwanSvc\Profiles
  Opens:                  C:\ProgramData\Start Menu\
  Opens:                  C:\ProgramData\Sun
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\osknumpad.xml
  Opens:                  C:\ProgramData\Sun\Java
  Opens:                  C:\ProgramData\Sun\Java\Java Update
  Opens:                  C:\ProgramData\Templates\
  Opens:                  C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskpred
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\oskpred\oskpredbase.xml
  Opens:                  C:\Program Files (x86)\Whisper Technology\FTP Surfer\
  Opens:                  C:\Users\Admin\AppData\Roaming\FTPGetter\
  Opens:                  C:\ProgramData\FTPGetter\
  Opens:                  C:\Users\Admin\AppData\Local\FTPGetter\
  Opens:                  C:\Users\Admin\AppData\Roaming\Estsoft\ALFTP\
  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\
  Opens:                  C:\Users\Admin\AppData\Roaming\SiteDesigner\
  Opens:                  C:\ProgramData\SiteDesigner\
  Opens:                  C:\Users\Admin\AppData\Local\SiteDesigner\
  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
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\symbols\ja-jp-sym.xml
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\symbols\symbase.xml
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\symbols.xml
  Opens:                  C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\web
  Opens:                  C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\web\webbase.xml
  Opens:                  C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\web.xml
  Opens:                  C:\Program Files\Common Files\Microsoft Shared\ink\he-IL
  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
  Opens:                  C:\Program Files\Common Files\Microsoft Shared\ink\hr-HR\tipresx.dll.mui
  Opens:                  C:\Program Files\Common Files\Microsoft Shared\ink\hu-HU
  Opens:                  C:\Program Files\Common Files\Microsoft Shared\ink\hu-HU\tipresx.dll.mui
  Opens:                  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
  Reads from:             C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
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
  Reads from:             C:\Program Files\Common Files\Microsoft Shared\ink\ar-SA\tipresx.dll.mui
  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
  Reads from:             C:\Program Files\Common Files\Microsoft Shared\ink\da-DK\tipresx.dll.mui
  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
  Reads from:             C:\Program Files\Common Files\Microsoft Shared\ink\en-
US\FlickLearningWizard.exe.mui
  Reads from:             C:\Program Files\Common Files\Microsoft Shared\ink\en-US\InkObj.dll.mui
  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
  Reads from:               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-
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
  Reads from:               C:\Program Files\Common Files\Microsoft Shared\ink\en-US\tabskb.dll.mui
  Reads from:               C:\Program Files\Common Files\Microsoft Shared\ink\en-US\TipBand.dll.mui
  Reads from:               C:\Program Files\Common Files\Microsoft Shared\ink\en-US\TipRes.dll.mui
  Reads from:               C:\Program Files\Common Files\Microsoft Shared\ink\en-US\tipresx.dll.mui
  Reads from:               C:\Program Files\Common Files\Microsoft Shared\ink\en-US\TipTsf.dll.mui
  Reads from:               C:\Program Files\Common Files\Microsoft Shared\ink\es-ES\tipresx.dll.mui
  Reads from:               C:\Program Files\Common Files\Microsoft Shared\ink\et-EE\tipresx.dll.mui
  Reads from:               C:\Program Files\Common Files\Microsoft Shared\ink\fi-FI\tipresx.dll.mui
  Reads from:               C:\Program Files\Common Files\Microsoft Shared\ink\fr-FR\tipresx.dll.mui
  Reads from:               C:\Program Files\Common Files\Microsoft
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
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\keypad\keypadbase.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\keypad\kor-kor.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\keypad.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\baseAltGr_rtl.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\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
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base_jpn.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\base_kor.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\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
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\zh-dayi.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main\zh-phonetic.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\main.xml
  Reads from:               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
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\oskmenu\oskmenubase.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\oskmenu.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\osknumpad\osknumpadbase.xml
  Reads from:               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
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\oskpred.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\symbols\ea-sym.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\symbols\ja-jp-sym.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\symbols\symbase.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
Shared\ink\fsdefinitions\symbols.xml
  Reads from:               C:\Program Files\Common Files\Microsoft
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
  Reads from:               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
Reads from:	C:\Program Files\Common Files\Microsoft Shared\ink\hwrenalm.dat
Deletes:	C:\Windows\Temp\tmp.exe

Network Events

Connects to:	127.0.0.1:49160
Connects to:	93.79.131.49:80
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:	127.0.0.1:49199
Connects to:	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:	93.79.131.49:80

```
  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\software\microsoft\windows\currentversion\ime\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:                HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:                HKLM\system\currentcontrolset\control\nls\language
  Opens key:                HKLM\system\currentcontrolset\control\mui\uilanguages
  Opens key:                HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
  Opens key:                HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
  Opens key:                HKLM\software\wow6432node\policies\microsoft\mui\settings
  Opens key:                HKLM\software\policies\microsoft\mui\settings
  Opens key:                HKCU\
  Opens key:                HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:                HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop\languageconfiguration
  Opens key:                HKCU\control panel\desktop
  Opens key:                HKCU\control panel\desktop\muicached
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:                HKLM\
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\software\wow6432node\microsoft\ole
  Opens key:                HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\wow6432node\microsoft\oleaut
  Opens key:                HKLM\system\currentcontrolset\services\crypt32
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
  Opens key:
```

```
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\397ab6e2
  Opens key:
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 key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  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:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
  Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key:                HKLM\system\currentcontrolset\control\cmf\config
  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:                HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:                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
  Opens key:                HKCU\software\adobe\acrobat reader\9.0\annots
  Opens key:                HKCU\software\adobe\acrobat reader\9.0\annots\cannots
  Opens key:                HKCU\software\adobe\acrobat reader\9.0\annots\cannots\cannot
  Opens key:                HKCU\software\adobe\acrobat reader\9.0\avconversionfrompdf
  Opens key:                HKCU\software\adobe\acrobat reader\9.0\avconversionfrompdf\csettings
  Opens key:                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
  Opens key:                HKCU\software\adobe\acrobat reader\9.0\avgeneral\cdockables
  Opens key:                HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars
  Opens key:                HKCU\software\adobe\acrobat
reader\9.0\avgeneral\ctoolbars\cadvcommenting
  Opens key:                HKCU\software\adobe\acrobat
reader\9.0\avgeneral\ctoolbars\cbasiccommenting
  Opens key:                HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars\ccommenting
  Opens key:                HKCU\software\adobe\acrobat reader\9.0\avtracker
  Opens key:                HKCU\software\adobe\acrobat reader\9.0\collab
  Opens key:                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 key:               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:               HKCU\software\adobe\acrobat reader\9.0\installpath
  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 key:               HKCU\software\adobe\acrobat reader\9.0\originals
  Opens key:               HKCU\software\adobe\acrobat reader\9.0\prefsdialog
  Opens key:               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
  Opens key:               HKCU\software\adobe\adobe acrobat\9.0\diskcabs
  Opens key:               HKCU\software\adobe\adobe arm
  Opens key:               HKCU\software\adobe\adobe arm\1.0
  Opens key:               HKCU\software\adobe\adobe arm\1.0\arm
  Opens key:               HKCU\software\adobe\adobe synchronizer
  Opens key:               HKCU\software\adobe\adobe synchronizer\9.0
  Opens key:               HKCU\software\adobe\adobe synchronizer\9.0\acrobat.com
  Opens key:               HKCU\software\adobe\commonfiles
  Opens key:               HKCU\software\adobe\commonfiles\usage
  Opens key:               HKCU\software\adobe\commonfiles\usage\reader 9
  Opens key:               HKCU\software\appdatalow
  Opens key:               HKCU\software\appdatalow\software
  Opens key:               HKCU\software\appdatalow\software\microsoft
  Opens key:               HKCU\software\appdatalow\software\microsoft\internet explorer
  Opens key:               HKCU\software\appdatalow\software\microsoft\internet explorer\security
  Opens key:               HKCU\software\appdatalow\software\microsoft\internet
explorer\security\antiphishing
  Opens key:               HKCU\software\javasoft
  Opens key:               HKCU\software\javasoft\java update
  Opens key:               HKCU\software\javasoft\java update\policy
  Opens key:               HKCU\software\javasoft\java update\policy\javafx
  Opens key:               HKCU\software\macromedia
  Opens key:               HKCU\software\macromedia\flashplayer
  Opens key:               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}
  Opens key:               HKCU\software\microsoft\active setup\installed components\{44bba840-
cc51-11cf-aafa-00aa00b6015c}
  Opens key:               HKCU\software\microsoft\active setup\installed components\{6bf52a52-
394a-11d3-b153-00c04f79faa6}
  Opens key:               HKCU\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4340}
  Opens key:               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
  Opens key:               HKCU\software\microsoft\activemovie\devenum 64-bit
  Opens key:               HKCU\software\microsoft\activemovie\devenum 64-bit\{4efe2452-168a-11d1-
bc76-00c04fb9453b}
  Opens key:               HKCU\software\microsoft\activemovie\devenum 64-bit\{4efe2452-168a-11d1-
bc76-00c04fb9453b}\default midiout device
  Opens key:               HKCU\software\microsoft\activemovie\devenum 64-bit\{e0f158e1-cb04-11d0-
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
  Opens key:               HKCU\software\microsoft\assistance\client
  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
  Opens key:               HKCU\software\microsoft\ctf
  Opens key:               HKCU\software\microsoft\ctf\assemblies
  Opens key:               HKCU\software\microsoft\ctf\assemblies\0x00000409
  Opens key:               HKCU\software\microsoft\ctf\assemblies\0x00000409\{34745c63-b2f0-4784-
8b67-5e12c8701a31}
  Opens key:               HKCU\software\microsoft\ctf\directswitchhotkeys
  Opens key:               HKCU\software\microsoft\ctf\hiddendummylayouts
  Opens key:               HKCU\software\microsoft\ctf\msutb
  Opens key:               HKCU\software\microsoft\ctf\sortorder
  Opens key:               HKCU\software\microsoft\ctf\sortorder\language
  Opens key:               HKCU\software\microsoft\ctf\tip
  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\faxoptions
  Opens key:                  HKCU\software\microsoft\fax\fxsclnt
  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\iam
  Opens key:                  HKCU\software\microsoft\iam\accounts
  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:                  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\software\microsoft\imejp\10.0\stylelist\atok\color
  Opens key:                  HKCU\software\microsoft\imejp\10.0\stylelist\ms-ime2000
  Opens key:                  HKCU\software\microsoft\imejp\10.0\stylelist\ms-ime2000\color
  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\color
  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\colors
  Opens key:                  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\document windows
  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\ietld
  Opens key:                  HKCU\software\microsoft\internet explorer\ietld\lowmic
  Opens key:                  HKCU\software\microsoft\internet explorer\intelliforms
  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
  Opens key:                  HKCU\software\microsoft\internet explorer\international\scripts\11
  Opens key:                  HKCU\software\microsoft\internet explorer\international\scripts\12
  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
  Opens key:                  HKCU\software\microsoft\internet explorer\international\scripts\16
  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
  Opens key:                  HKCU\software\microsoft\internet explorer\international\scripts\21
  Opens key:                  HKCU\software\microsoft\internet explorer\international\scripts\22
  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
  Opens key:                  HKCU\software\microsoft\internet explorer\international\scripts\30
  Opens key:                  HKCU\software\microsoft\internet explorer\international\scripts\34
  Opens key:                  HKCU\software\microsoft\internet explorer\international\scripts\35
  Opens key:                  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
  Opens key:               HKCU\software\microsoft\internet explorer\international\scripts\4
  Opens key:               HKCU\software\microsoft\internet explorer\international\scripts\5
  Opens key:               HKCU\software\microsoft\internet explorer\international\scripts\6
  Opens key:               HKCU\software\microsoft\internet explorer\international\scripts\7
  Opens key:               HKCU\software\microsoft\internet explorer\international\scripts\8
  Opens key:               HKCU\software\microsoft\internet explorer\international\scripts\9
  Opens key:               HKCU\software\microsoft\internet explorer\internetregistry
  Opens key:               HKCU\software\microsoft\internet explorer\linksbar
  Opens key:               HKCU\software\microsoft\internet explorer\linksbar\itemcache
  Opens key:               HKCU\software\microsoft\internet explorer\linksbar\itemcache\0
  Opens key:               HKCU\software\microsoft\internet explorer\linksbar\itemcache\1
  Opens key:               HKCU\software\microsoft\internet explorer\lowregistry
  Opens key:               HKCU\software\microsoft\internet explorer\lowregistry\domstorage
  Opens key:               HKCU\software\microsoft\internet explorer\lowregistry\domstorage\total
  Opens key:               HKCU\software\microsoft\internet
explorer\lowregistry\dontshowmethisdialogagain
  Opens key:               HKCU\software\microsoft\internet explorer\lowregistry\shell extensions
  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:               HKCU\software\microsoft\internet explorer\main\default feeds\{728bab62-
50c0-4a2a-b9a6-951f2355feb2}
  Opens key:               HKCU\software\microsoft\internet explorer\main\default feeds\{bab07688-
e349-461a-b4f5-b4674114d3a6}
  Opens key:               HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
  Opens key:               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown\settings
  Opens key:               HKCU\software\microsoft\internet explorer\main\windowssearch
  Opens key:               HKCU\software\microsoft\internet explorer\new windows
  Opens key:               HKCU\software\microsoft\internet explorer\pagesetup
  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
  Opens key:               HKCU\software\microsoft\internet explorer\recovery\adminactive
  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
  Opens key:               HKCU\software\microsoft\internet explorer\security\antiphishing
  Opens key:               HKCU\software\microsoft\internet
explorer\security\antiphishing\2cedbfbc-dba8-43aa-b1fd-cc8e6316e3e2
  Opens key:               HKCU\software\microsoft\internet explorer\services
  Opens key:               HKCU\software\microsoft\internet explorer\settings
  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
  Opens key:               HKCU\software\microsoft\internet explorer\toolbar
  Opens key:               HKCU\software\microsoft\internet explorer\toolbar\shellbrowser
  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
  Opens key:               HKCU\software\microsoft\internet explorer\user preferences
  Opens key:               HKCU\software\microsoft\internet explorer\zoom
  Opens key:               HKCU\software\microsoft\java vm
  Opens key:               HKCU\software\microsoft\keyboard
  Opens key:               HKCU\software\microsoft\keyboard\native media players
  Opens key:               HKCU\software\microsoft\keyboard\native media players\wmp
  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
  Opens key:               HKCU\software\microsoft\mediaplayer\player\tasks\nowplaying
  Opens key:               HKCU\software\microsoft\mediaplayer\preferences
  Opens key:               HKCU\software\microsoft\mediaplayer\preferences\hme
  Opens key:               HKCU\software\microsoft\mediaplayer\preferences\proxysettings
  Opens key:               HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http
  Opens key:               HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp
  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
  Opens key:               HKCU\software\microsoft\msdaipp
  Opens key:               HKCU\software\microsoft\msdaipp\providers
  Opens key:               HKCU\software\microsoft\msdaipp\providers\{9fecd570-b9d4-11d1-9c78-
0000f875ac61}
  Opens key:               HKCU\software\microsoft\msdaipp\providers\{9fecd571-b9d4-11d1-9c78-
```

```
0000f875ac61}
  Opens key:               HKCU\software\microsoft\msf
  Opens key:               HKCU\software\microsoft\msf\registration
  Opens key:               HKCU\software\microsoft\msf\registration\listen
  Opens key:               HKCU\software\microsoft\multimedia
  Opens key:               HKCU\software\microsoft\multimedia\activemovie
  Opens key:               HKCU\software\microsoft\multimedia\activemovie\filter cache64
  Opens key:               HKCU\software\microsoft\notepad
  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
  Opens key:               HKCU\software\microsoft\office\11.0\common\drawalerts\ftp sites
  Opens key:               HKCU\software\microsoft\office\11.0\common\dspadaptermru
  Opens key:               HKCU\software\microsoft\office\11.0\common\general
  Opens key:               HKCU\software\microsoft\office\11.0\common\languageresources
  Opens key:               HKCU\software\microsoft\office\11.0\common\migration
  Opens key:               HKCU\software\microsoft\office\11.0\common\migration\office
  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
  Opens key:               HKCU\software\microsoft\office\11.0\common\research\translation
  Opens key:               HKCU\software\microsoft\office\11.0\common\toolbars
  Opens key:               HKCU\software\microsoft\office\11.0\common\toolbars\settings
  Opens key:               HKCU\software\microsoft\office\11.0\common\userinfo
  Opens key:               HKCU\software\microsoft\office\11.0\word
  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
  Opens key:               HKCU\software\microsoft\office\12.0\common\drawalerts
  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\software\microsoft\office\12.0\common\research\translation
  Opens key:               HKCU\software\microsoft\office\12.0\excel
  Opens key:               HKCU\software\microsoft\office\12.0\excel\options
  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\excel_intl
  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:               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
  Opens key:               HKCU\software\microsoft\office\14.0\common\drawalerts\ftp sites
  Opens key:               HKCU\software\microsoft\office\14.0\common\general
  Opens key:               HKCU\software\microsoft\office\14.0\common\languageresources
  Opens key:
HKCU\software\microsoft\office\14.0\common\languageresources\enabledlanguages
  Opens key:               HKCU\software\microsoft\office\14.0\common\open find
  Opens key:               HKCU\software\microsoft\office\14.0\common\open find\microsoft
powerpoint viewer
  Opens key:               HKCU\software\microsoft\office\14.0\common\research
  Opens key:               HKCU\software\microsoft\office\14.0\common\research\translation
  Opens key:               HKCU\software\microsoft\office\14.0\powerpoint
  Opens key:               HKCU\software\microsoft\office\14.0\powerpoint viewer
  Opens key:               HKCU\software\microsoft\office\14.0\powerpoint viewer\options
  Opens key:               HKCU\software\microsoft\office\common
  Opens key:               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}
  Opens key:               HKCU\software\microsoft\office\common\smart tag\actions\{49df3409-46b3-
4b0c-b7bf-fec0f9401edd}
  Opens key:               HKCU\software\microsoft\office\common\smart tag\actions\{64ab6c69-b40e-
40af-9b7f-f5687b48e2b6}
  Opens key:               HKCU\software\microsoft\office\common\smart tag\actions\{c3754d1a-04d3-
4085-8cfb-97705b57a98f}
  Opens key:               HKCU\software\microsoft\office\common\smart tag\actions\{f114ae61-1331-
4238-92c9-bbe330af25fd}
  Opens key:               HKCU\software\microsoft\office\common\smart tag\recognizers
  Opens key:               HKCU\software\microsoft\office\common\smart tag\recognizers\{64ab6c69-
```

```
b40e-40af-9b7f-f5687b48e2b6}
  Opens key:                HKCU\software\microsoft\office\common\smart tag\recognizers\{87ef1cfe-
51ca-4e6b-8c76-e576aa926888}
  Opens key:                HKCU\software\microsoft\office\common\userinfo
  Opens key:                HKCU\software\microsoft\peernet
  Opens key:                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-
980053277-1733835069-2361817685-1001
  Opens key:                HKCU\software\microsoft\ras autodial
  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
  Opens key:                HKCU\software\microsoft\shared tools\proofing tools
  Opens key:                HKCU\software\microsoft\shared tools\proofing tools\custom dictionaries
  Opens key:                HKCU\software\microsoft\sideshow
  Opens key:                HKCU\software\microsoft\sideshow\gadgets
  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
  Opens key:                HKCU\software\microsoft\systemcertificates\ca\certificates
  Opens key:                HKCU\software\microsoft\systemcertificates\ca\crls
  Opens key:                HKCU\software\microsoft\systemcertificates\ca\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:                HKCU\software\microsoft\systemcertificates\root\protectedroots
  Opens key:                HKCU\software\microsoft\systemcertificates\smartcardroot
  Opens key:                HKCU\software\microsoft\systemcertificates\smartcardroot\certificates
  Opens key:                HKCU\software\microsoft\systemcertificates\smartcardroot\crls
  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
  Opens key:                HKCU\software\microsoft\systemcertificates\trust\ctls
  Opens key:                HKCU\software\microsoft\systemcertificates\trustedpeople
  Opens key:                HKCU\software\microsoft\systemcertificates\trustedpeople\certificates
  Opens key:                HKCU\software\microsoft\systemcertificates\trustedpeople\crls
  Opens key:                HKCU\software\microsoft\systemcertificates\trustedpeople\ctls
  Opens key:                HKCU\software\microsoft\systemcertificates\trustedpublisher
  Opens key:                HKCU\software\microsoft\systemcertificates\trustedpublisher\certificates
  Opens key:                HKCU\software\microsoft\systemcertificates\trustedpublisher\crls
  Opens key:                HKCU\software\microsoft\systemcertificates\trustedpublisher\ctls
  Opens key:                HKCU\software\microsoft\wab
  Opens key:                HKCU\software\microsoft\wab\me
  Opens key:                HKCU\software\microsoft\wab\wab4
  Opens key:                HKCU\software\microsoft\wab\wab4\wab file name
  Opens key:                HKCU\software\microsoft\wfs
  Opens key:                HKCU\software\microsoft\wfs\draftsview
  Opens key:                HKCU\software\microsoft\wfs\inboxview
  Opens key:                HKCU\software\microsoft\wfs\incomingview
  Opens key:                HKCU\software\microsoft\wfs\outboxview
  Opens key:                HKCU\software\microsoft\wfs\sentitemsview
  Opens key:                HKCU\software\microsoft\windows
  Opens key:                HKCU\software\microsoft\windows\currentversion
  Opens key:                HKCU\software\microsoft\windows\currentversion\action center
  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
  Opens key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101
  Opens key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101
  Opens key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100
  Opens key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101
  Opens key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{945a8954-c147-4acd-923f-40c45405a658}.check.42
  Opens key:                HKCU\software\microsoft\windows\currentversion\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
  Opens key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100
  Opens key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100
  Opens key:                HKCU\software\microsoft\windows\currentversion\action
```

```
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101
  Opens key:                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
  Opens key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104
  Opens key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106
  Opens key:                HKCU\software\microsoft\windows\currentversion\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 key:                HKCU\software\microsoft\windows\currentversion\applets
  Opens key:                HKCU\software\microsoft\windows\currentversion\applets\regedit
  Opens key:                HKCU\software\microsoft\windows\currentversion\applets\systray
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\applicationdestinations
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\autoplayhandlers
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\autoplayhandlers\eventhandlersdefaultselection
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\autoplayhandlers\userchosenexecutehandlers
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\bitbucket
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\bitbucket\volume
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\cabinetstate
  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
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\cidopen
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\cidopen\modules
  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\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-
3f72-44a7-89c5-5595fe6b30ee}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{645ff040-
5081-101b-9f08-00aa002f954e}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
42a0-1069-a2ea-08002b30309d}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{f02c1a0d-
be21-4350-88b0-7367fc96ef3c}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\comdlg32
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\cidsizemru
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\firstfolder
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\lastvisitedpidlmru
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\opensavepidlmru
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\controlpanel
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\discardable
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\discardable\postsetup
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.3g2
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.3gp
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.3gp2
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.3gpp
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.aac
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.adt
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.adts
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.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
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.asx
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.au
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.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
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dib
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.doc
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.docm
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.docx
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dot
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dvr
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dvr-ms
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dwfx
  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:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm
  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 key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.jpe
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.jpeg
  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
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m2ts
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m2v
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m3u
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m4a
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m4v
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mht
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mhtml
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mid
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.midi
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mod
  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
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp4v
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpa
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.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 key:               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:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.pot
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.potm
  Opens key:               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 key:               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:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.rle
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.rmi
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.rtf
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.scf
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.search-ms
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.snd
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.sys
  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:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ttc
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ttf
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.tts
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.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 key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wm
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wma
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wmf
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wmv
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wmx
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wpl
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wtv
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wvx
  Opens key:               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:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlsm
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlsx
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlt
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xltm
  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\directory
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\lowregistry
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\menuorder
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\modules
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\modules\commonplaces
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\modules\globalsettings
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\modules\navpane
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{8063a3d4-8213-11e3-a68e-
806e6f6e6963}
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{8063a3d7-8213-11e3-a68e-
806e6f6e6963}
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\newshortcuthandlers
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\recentdocs
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\runmru
  Opens key:                HKCU\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 key:
HKCU\software\microsoft\windows\currentversion\explorer\startpage\newshortcuts
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\startpage2
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\streams
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\streams\desktop
  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 key:                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\currentversion\explorer\userassist\{f4e57c4b-2036-45f0-a9ab-
443bcfe33d9f}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\visualeffects
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\animateminmax
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\comboboxanimation
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\controlanimations
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\cursorshadow
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dragfullwindows
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dropshadow
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dwmaeropeekenabled
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dwmenabled
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dwmsavethumbnailenabled
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\fontsmoothing
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listboxsmoothscrolling
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewalphaselect
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewshadow
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\menuanimation
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\selectionfade
  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\currentversion\explorer\visualeffects\thumbnailsoricon
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\tooltipanimation
```

```
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\transparentglass
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\wallpapers
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\wallpapers\images
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\wallpapers\knownfolders
  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 key:                HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-
e8ad-4283-a596-fa578c2ebdc3}
  Opens key:                HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-
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\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
435b-bc74-9c25c1c588a9}
  Opens key:                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:                HKCU\software\microsoft\windows\currentversion\group
policy\policyapplicationstate
  Opens key:                HKCU\software\microsoft\windows\currentversion\group policy editor
  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
  Opens key:                HKCU\software\microsoft\windows\currentversion\group policy objects
  Opens key:                HKCU\software\microsoft\windows\currentversion\group policy
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 key:                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
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
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
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\activities\email
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\activities\map
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
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
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\p3p
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\passport
```

```
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\passport\lowdamap
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\protocols
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\protocols\mailto
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  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
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\e2-c2-d0-09-69-0f
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{4dc0ee17-9725-46c6-9208-9e741c29932a}
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{97510e62-091a-49b5-9797-24fe4dde0abc}
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{c034e4b5-6859-46ca-b262-e1e2cfd7fcab}
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f9145a4d-b491-47f1-8afa-50f81461036d}
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zonemap
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\escdomains
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:                HKCU\software\microsoft\windows\currentversion\mct
  Opens key:                HKCU\software\microsoft\windows\currentversion\mct\us
  Opens key:                HKCU\software\microsoft\windows\currentversion\mct\us\link
  Opens key:                HKCU\software\microsoft\windows\currentversion\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 key:                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:                HKCU\software\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
  Opens key:                HKCU\software\microsoft\windows\currentversion\screensavers\mystify
  Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\mystify\screen 1
  Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\mystify\screen 2
  Opens key:                HKCU\software\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
  Opens key:                HKCU\software\microsoft\windows\currentversion\sidebar
  Opens key:                HKCU\software\microsoft\windows\currentversion\sidebar\settings
  Opens key:                HKCU\software\microsoft\windows\currentversion\telephony
  Opens key:
HKCU\software\microsoft\windows\currentversion\telephony\handoffpriorities
  Opens key:
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\software\microsoft\windows\currentversion\themes\defaultvisualstyleoff
  Opens key:
HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleon
  Opens key:                HKCU\software\microsoft\windows\currentversion\themes\installedthemes
  Opens key:
HKCU\software\microsoft\windows\currentversion\themes\installedthemes\mct
  Opens key:                HKCU\software\microsoft\windows\currentversion\wintrust
  Opens key:                HKCU\software\microsoft\windows\currentversion\wintrust\trust providers
  Opens key:                HKCU\software\microsoft\windows\currentversion\wintrust\trust
providers\software publishing
```

```
  Opens key:               HKCU\software\microsoft\windows\dwm
  Opens key:               HKCU\software\microsoft\windows\shell
  Opens key:               HKCU\software\microsoft\windows\shell\bagmru
  Opens key:               HKCU\software\microsoft\windows\shell\bags
  Opens key:               HKCU\software\microsoft\windows\shell\bags\1
  Opens key:               HKCU\software\microsoft\windows\shell\bags\1\desktop
  Opens key:               HKCU\software\microsoft\windows\tabletpc
  Opens key:               HKCU\software\microsoft\windows\tabletpc\tabsetup
  Opens key:               HKCU\software\microsoft\windows\windows 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
  Opens key:               HKCU\software\microsoft\windows mail
  Opens key:               HKCU\software\microsoft\windows mail\mail
  Opens key:               HKCU\software\microsoft\windows mail\news
  Opens key:               HKCU\software\microsoft\windows mail\trident
  Opens key:               HKCU\software\microsoft\windows mail\trident\main
  Opens key:               HKCU\software\microsoft\windows mail\trident\settings
  Opens key:               HKCU\software\microsoft\windows media
  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
  Opens key:               HKCU\software\microsoft\windows
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
  Opens key:               HKCU\software\microsoft\windows nt\currentversion\network
  Opens key:               HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
  Opens key:               HKCU\software\microsoft\windows nt\currentversion\peernet
  Opens key:               HKCU\software\microsoft\windows nt\currentversion\peernet\collabhost
  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
  Opens key:               HKCU\software\microsoft\windows search\processedsearchroots
  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
  Opens key:               HKCU\software\microsoft\windows search\processedsearchroots\0003
  Opens key:               HKCU\software\microsoft\windows sidebar
  Opens key:               HKCU\software\microsoft\windows sidebar\ieoverride
  Opens key:               HKCU\software\microsoft\windows sidebar\ieoverride\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
  Opens key:               HKCU\software\microsoft\wisp\pen\syseventparameters\flickcommands
  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 key:               HKCU\software\netscape\netscape navigator\viewers
  Opens key:               HKCU\software\policies
  Opens key:               HKCU\software\policies\microsoft
  Opens key:               HKCU\software\policies\microsoft\systemcertificates
  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
  Opens key:               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:               HKCU\software\policies\microsoft\systemcertificates\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 key:
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 key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\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
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\cache
  Opens key:                HKCU\software\policies\power
  Opens key:                HKCU\software\policies\power\powersettings
  Opens key:                HKCU\software\python
  Opens key:                HKCU\software\python\pythoncore
  Opens key:                HKCU\software\python\pythoncore\2.7
  Opens key:                HKCU\software\python\pythoncore\2.7\help
  Opens key:                HKCU\software\python\pythoncore\2.7\help\pythonwin reference
  Opens key:                HKCU\software\wow6432node
  Opens key:                HKCU\software\wow6432node\microsoft
  Opens key:                HKCU\software\wow6432node\microsoft\active setup
  Opens key:                HKCU\software\wow6432node\microsoft\active setup\installed components
  Opens key:                HKCU\software\wow6432node\microsoft\active setup\installed
components\>{26923b43-4d38-484f-9b9e-de460746276c}
  Opens key:                HKCU\software\wow6432node\microsoft\active setup\installed
components\>{60b49e34-c7cc-11d0-8953-00a0c90347ff}
  Opens key:                HKCU\software\wow6432node\microsoft\active setup\installed
components\{2c7339cf-2b09-4501-b3f3-f3508c9228ed}
  Opens key:                HKCU\software\wow6432node\microsoft\active setup\installed
components\{44bba840-cc51-11cf-aafa-00aa00b6015c}
  Opens key:                HKCU\software\wow6432node\microsoft\active setup\installed
components\{6bf52a52-394a-11d3-b153-00c04f79faa6}
  Opens key:                HKCU\software\wow6432node\microsoft\active setup\installed
components\{89820200-ecbd-11cf-8b85-00aa005b4340}
  Opens key:                HKCU\software\wow6432node\microsoft\active setup\installed
components\{89820200-ecbd-11cf-8b85-00aa005b4383}
  Opens key:                HKCU\software\wow6432node\microsoft\active setup\installed
components\{89b4c1cd-b018-4511-b0a1-5476dbf70820}
  Opens key:                HKCU\software\classes
  Opens key:                HKCU\software\classes\wow6432node\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
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0003-
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}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0004-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0005-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0005-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0000-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0000-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0001-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0001-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0001-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0001-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0002-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0002-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0002-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0002-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0003-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0003-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0003-
```

```
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}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0004-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0005-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0005-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0005-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0005-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0006-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0006-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0006-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0006-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0007-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0007-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0007-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0007-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0008-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0008-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0008-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0008-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0009-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0009-
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
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0010-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0010-
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
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0011-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0011-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0011-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0011-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0012-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0012-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0012-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0012-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0013-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0013-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0013-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0013-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0014-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0014-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0014-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0014-
```

```
abcdeffedcbb}\inprocserver32
  Opens key:                 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-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0015-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0016-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0016-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0016-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0016-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0017-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0017-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0017-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0017-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0018-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0018-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0018-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0018-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0019-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0019-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0019-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0019-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0020-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0020-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0020-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0020-
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
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0021-
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}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0000-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0001-
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
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0002-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0002-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0002-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0002-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0003-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0003-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0003-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0003-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0000-0004-
```

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

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

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

```
abcdeffedcbb}\inprocserver32
  Opens key:                 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-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0025-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0026-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0026-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0026-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0026-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0027-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0027-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0027-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0027-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0028-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0028-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0028-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0028-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0029-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0029-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0029-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0029-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0030-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0030-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0030-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0030-
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
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0031-
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}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0032-
abcdeffedcbb}\inprocserver32
  Opens key:                 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
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0034-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0034-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0034-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-0034-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-ffff-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0014-0002-ffff-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0000-
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}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0001-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0001-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0001-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0001-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0001-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0002-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0003-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0004-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0004-
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
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0004-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0004-
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
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0005-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0005-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0005-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0005-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0006-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0006-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0006-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0006-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0006-
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:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0007-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0007-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0007-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0007-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0007-
```

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

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

```
abcdeffedcbc}\inprocserver32
  Opens key:                 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-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0023-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0023-
abcdeffedcbc}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0023-
abcdeffedcbc}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
abcdeffedcbc}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0024-
abcdeffedcbc}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
abcdeffedcbc}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0025-
abcdeffedcbc}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0026-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0026-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0026-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0026-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0026-
abcdeffedcbc}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0026-
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
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0027-
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}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0028-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0028-
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
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0029-
abcdeffedcba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0029-
abcdeffedcba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0029-
abcdeffedcbb}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0029-
abcdeffedcbb}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0029-
abcdeffedcbc}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0029-
abcdeffedcbc}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0030-
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}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0031-
abcdeffedcba}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbb}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbb}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbc}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbc}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0032-
abcdeffedcba}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0032-
abcdeffedcba}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0032-
abcdeffedcbb}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0032-
abcdeffedcbb}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0032-
abcdeffedcbc}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-0032-
abcdeffedcbc}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-ffff-
abcdeffedcba}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0015-0000-ffff-
abcdeffedcba}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
abcdeffedcba}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
abcdeffedcba}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
abcdeffedcbb}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
abcdeffedcbb}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
abcdeffedcbc}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0000-
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
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0001-
abcdeffedcbb}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0001-
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
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
abcdeffedcba}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
abcdeffedcba}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
abcdeffedcbb}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
abcdeffedcbb}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
abcdeffedcbc}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0002-
abcdeffedcbc}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0003-
abcdeffedcba}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0003-
abcdeffedcba}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0003-
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}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0003-
abcdeffedcbc}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0004-
abcdeffedcba}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0004-
abcdeffedcba}\inprocserver32
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0004-
abcdeffedcbb}
   Opens key:                 HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0004-
```

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

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

```
abcdeffedcbb}\inprocserver32
  Opens key:                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-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0020-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0020-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0020-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0020-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0020-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0021-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0022-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0023-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0023-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0023-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0023-
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
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0024-
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}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0024-
abcdeffedcbc}\inprocserver32
  Opens key:                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:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0025-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0025-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0025-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0026-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0026-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0026-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0026-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0026-
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}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0027-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0028-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-0029-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-ffff-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0016-0000-ffff-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
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:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
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
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbc}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbc}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-ffff-
abcdeffedcba}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-ffff-
abcdeffedcba}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{e19f9331-3110-11d4-991c-
005004d3b3db}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{e19f9331-3110-11d4-991c-
005004d3b3db}\inprocserver32
  Opens key:                HKCU\software\classes\javaplugin.1020
  Opens key:                HKCU\software\classes\javaplugin.1020\clsid
  Opens key:                HKCU\software\classes\local settings
  Opens key:                HKCU\software\classes\local settings\muicache
  Opens key:                HKCU\software\classes\local settings\muicache\16
  Opens key:                HKCU\software\classes\local settings\muicache\16\52c64b7e
  Opens key:                HKCU\software\classes\local settings\software
  Opens key:                HKCU\software\classes\local settings\software\microsoft
  Opens key:                HKCU\software\classes\local settings\software\microsoft\windows
  Opens key:                HKCU\software\classes\local
settings\software\microsoft\windows\currentversion
  Opens key:                HKCU\software\classes\local settings\software\microsoft\windows\shell
  Opens key:                HKCU\software\classes\python.file
  Opens key:                HKCU\software\classes\python.file\shell
  Opens key:                HKCU\software\classes\python.file\shell\edit with pythonwin
  Opens key:                HKCU\software\classes\python.file\shell\edit with pythonwin\command
  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 key:                HKCU\software\classes\virtualstore\machine
  Opens key:                HKCU\software\classes\virtualstore\machine\software
  Opens key:                HKCU\software\classes\virtualstore\machine\software\wow6432node
  Opens key:
HKCU\software\classes\virtualstore\machine\software\wow6432node\microsoft
  Opens key:                HKCU\software\classes\wow6432node
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\run
  Opens key:                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
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:                HKCU\software\flashfxp
  Opens key:                HKCU\software\flashfxp\3
  Opens key:                HKCU\software\flashfxp\4
  Opens key:                HKLM\software\wow6432node\flashfxp
  Opens key:                HKLM\software\wow6432node\flashfxp\3
  Opens key:                HKLM\software\wow6432node\flashfxp\4
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\addressbook
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\adobe flash player activex
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\connection manager
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\directdrawex
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\fontcore
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie40
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie4data
  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 key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\schedulingagent
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\wic
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{196bb40d-1578-3d01-b289-
befc77a11a1e}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-4ca4-87b4-
2f83217002ff}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{4a03706f-666a-4037-7777-
5f2748764d10}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-
0000000ff1ce}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90850409-6000-11d3-8cfe-
0150048383c9}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95120000-003f-0409-0000-
0000000ff1ce}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-
0000000ff1ce}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-
a93000000001}
  Opens key:                HKCU\software\bpftp\bullet proof ftp\main
  Opens key:                HKCU\software\bulletproof software\bulletproof ftp client\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:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}\propertybag
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}\propertybag
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
  Opens key:                HKCU\software\turboftp
  Opens key:                HKCU\software\cryer\websitepublisher
  Opens key:                HKU\
  Opens key:                HKCU\software\ftpclient\sites
  Opens key:                HKCU\software\softx.org\ftpclient\sites
  Opens key:                HKCU\software\vandyke\securefx
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}\propertybag
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
  Opens key:                HKCU\software\globalscape\cuteftp 6 home\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
  Opens key:                HKCU\software\globalscape\cuteftp 8 home\qctoolbar
  Opens key:                HKCU\software\globalscape\cuteftp 8 professional\qctoolbar
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}\propertybag
  Opens key:                HKCU\software\sota\ffftp\options
  Opens key:                HKCU\software\south river technologies\webdrive\connections
  Opens key:                HKCU\software\nch software\classicftp\ftpaccounts
  Opens key:                HKLM\software\wow6432node\nch software\fling\accounts
  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
  Opens key:                HKCU\software\ftpware\coreftp\sites
  Opens key:                HKCU\software\far\plugins\ftp\hosts
  Opens key:                HKCU\software\far2\plugins\ftp\hosts
  Opens key:                HKCU\software\far\saveddialoghistory\ftphost
  Opens key:                HKCU\software\far2\saveddialoghistory\ftphost
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}\propertybag
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
980053277-1733835069-2361817685-1001
  Opens key:                HKCU\software\ghisler\windows commander
  Opens key:                HKCU\software\ghisler\total commander
  Opens key:                HKLM\software\wow6432node\ghisler\windows commander
  Opens key:                HKLM\software\wow6432node\ghisler\total commander
  Opens key:                HKLM\software\wow6432node
```

```
 Opens key:                  HKCU\software\acebit
 Opens key:                  HKLM\software\wow6432node\acebit
 Opens key:                  HKCR\typelib\{cb1f2c0f-8094-4aac-bcf5-41a64e27f777}
 Opens key:                  HKCR\typelib\{9ea55529-e122-4757-bc79-e4825f80732c}
 Opens key:                  HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
 Opens key:                  HKLM\system\currentcontrolset\control\sqmservicelist
 Opens key:                  HKCU\software\mozilla
 Opens key:                  HKLM\software\wow6432node\mozilla
 Opens key:                  HKCU\software\chromeplus
 Opens key:                  HKCU\software\leechftp
 Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}
 Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}\propertybag
 Opens key:                  HKCU\software\classes\
 Opens key:                  HKLM\software\classes
 Opens key:                  HKCU\software\flashpeak\blazeftp\settings
 Opens key:                  HKCR\typelib\{f9043c88-f6f2-101a-a3c9-08002b2f49fb}\1.2\0\win32
 Queries value:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
 Queries value:              HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
 Queries value:              HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value:              HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[empty]
 Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
 Queries value:              HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Queries value:              HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
 Queries value:              HKCU\control panel\desktop[preferreduilanguages]
 Queries value:              HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
 Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 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]
 Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
 Queries value:              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Queries value:              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
 Queries value:              HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
 Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
 Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
 Queries value:              HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[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\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
  Queries 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]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
  Queries value:
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]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
  Queries value:
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]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
  Queries 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\000000000006[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Queries value:            HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:            HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:            HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:            HKLM\software\wow6432node\microsoft\windows\windows error
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]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[bg-bg]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[bg-bg]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ca]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ca]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ca-es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ca-es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[zh-hans]
  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]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[cs]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[cs]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[cs-cz]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[cs-cz]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[da]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[da]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[da-dk]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[da-dk]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[de]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[de]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[de-de]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[de-de]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[el]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[el]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[el-gr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[el-gr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[es-es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[es-es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[fi]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[fi]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[fi-fi]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[fi-fi]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[fr-fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[he]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[he]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[he-il]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[he-il]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[hu]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[hu]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[hu-hu]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[hu-hu]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[is]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[is]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[is-is]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[is-is]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[it]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[it]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[it-it]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[it-it]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ja]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ja]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ja-jp]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ja-jp]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ko]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ko]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ko-kr]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ko-kr]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[nl]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[nl]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[nl-nl]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[nl-nl]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[no]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[no]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[nb-no]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[nb-no]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[pl]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[pl]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[pl-pl]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[pl-pl]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[pt]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[pt]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[pt-br]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[pt-br]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[rm]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[rm]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[rm-ch]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[rm-ch]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ro]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ro]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ro-ro]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ro-ro]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ru]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ru]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ru-ru]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ru-ru]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[hr]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[hr]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[hr-hr]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[hr-hr]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sk]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sk]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sk-sk]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sk-sk]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sq]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sq]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sq-al]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sq-al]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sv]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sv]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sv-se]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sv-se]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[th]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[th]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[th-th]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[th-th]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[tr]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[tr]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[tr-tr]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[tr-tr]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ur]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ur]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ur-pk]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ur-pk]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[id]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[id]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[id-id]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[id-id]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[uk]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[uk]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[uk-ua]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[uk-ua]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[be]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[be]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[be-by]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[be-by]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sl]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sl]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sl-si]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sl-si]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[et]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[et]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[et-ee]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[et-ee]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[lv]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[lv]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[lv-lv]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[lv-lv]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[lt]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[lt]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[lt-lt]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[lt-lt]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[tg]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[tg]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[tg-cyrl-tj]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[tg-cyrl-tj]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[fa]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[fa]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[fa-ir]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[fa-ir]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[vi]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[vi]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[vi-vn]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[vi-vn]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[hy]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[hy]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[hy-am]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[hy-am]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[az]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[az]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[az-latn-az]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[az-latn-az]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[eu]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[eu]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[eu-es]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[eu-es]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[hsb]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[hsb]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[hsb-de]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[hsb-de]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[mk]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[mk]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[mk-mk]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[mk-mk]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[tn]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[tn]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[tn-za]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[tn-za]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[xh]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[xh]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[xh-za]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[xh-za]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[zu]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[zu]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[zu-za]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[zu-za]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[af]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[af]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[af-za]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[af-za]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ka]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ka]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ka-ge]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ka-ge]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[fo]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[fo]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[fo-fo]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[fo-fo]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[hi]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[hi]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[hi-in]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[hi-in]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[mt]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[mt]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[mt-mt]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[mt-mt]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[se]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[se]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[se-no]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[se-no]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ga]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ga]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ga-ie]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ga-ie]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ms]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ms]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ms-my]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ms-my]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[kk]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[kk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kk-kz]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kk-kz]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ky]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ky]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ky-kg]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ky-kg]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sw]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sw]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sw-ke]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sw-ke]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tk-tm]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tk-tm]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[uz]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[uz]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[uz-latn-uz]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[uz-latn-uz]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tt]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tt]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tt-ru]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tt-ru]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[bn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[bn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[bn-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[bn-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[pa]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[pa]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[pa-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[pa-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[gu]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[gu]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[gu-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[gu-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[or]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[or]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[or-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[or-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ta]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ta]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ta-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ta-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[te]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[te]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[te-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[te-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kn-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kn-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ml]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ml]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ml-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ml-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[as]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[as]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[as-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[as-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mr]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mr]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mr-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mr-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sa]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sa]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sa-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sa-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mn-mn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mn-mn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[bo]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[bo]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[bo-cn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[bo-cn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[cy]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[cy]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[cy-gb]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[cy-gb]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[km]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[km]
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]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[lo]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[lo-la]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[lo-la]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[gl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[gl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[gl-es]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[gl-es]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kok]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kok]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kok-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kok-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[syr]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[syr]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[syr-sy]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[syr-sy]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[si]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[si]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[si-lk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[si-lk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[iu]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[iu]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[iu-latn-ca]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[iu-latn-ca]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[am]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[am]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[am-et]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[am-et]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tzm]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tzm-latn-dz]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm-latn-dz]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ne]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ne]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ne-np]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ne-np]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fy]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fy]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fy-nl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fy-nl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ps]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ps]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ps-af]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ps-af]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fil]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fil]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fil-ph]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fil-ph]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[dv]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[dv]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[dv-mv]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[dv-mv]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ha]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ha]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ha-latn-ng]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ha-latn-ng]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[yo]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[yo]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[yo-ng]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[yo-ng]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[quz]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[quz]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[quz-bo]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[quz-bo]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[nso]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[nso]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[nso-za]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[nso-za]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ba]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ba]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ba-ru]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ba-ru]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[lb]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[lb]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[lb-lu]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[lb-lu]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kl-gl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kl-gl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ig]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ig]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ig-ng]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ig-ng]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ii]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ii]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ii-cn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ii-cn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[arn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[arn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[arn-cl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[arn-cl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[moh]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[moh]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[moh-ca]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[moh-ca]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[br]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[br]
```

```
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[br-fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[br-fr]
  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]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ug-cn]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[mi]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[mi]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[mi-nz]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[mi-nz]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[oc]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[oc]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[oc-fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[oc-fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[co]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[co]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[co-fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[co-fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[gsw]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[gsw]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[gsw-fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[gsw-fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sah]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sah]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sah-ru]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sah-ru]
  Queries 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]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[qut-gt]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[rw]
  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]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[wo]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[wo]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[wo-sn]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[wo-sn]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[prs]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[prs]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[prs-af]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[prs-af]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[gd]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[gd]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[gd-gb]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[gd-gb]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000401]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[d]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000402]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[5]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000403]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[zh-tw]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-tw]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000404]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[9]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000405]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[2]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000406]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000407]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000408]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[4]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[es-es_tradnl]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[es-es_tradnl]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[0000040a]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[0000040b]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[0000040c]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[0000040d]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[c]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[0000040e]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[0000040f]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000410]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000411]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[7]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000412]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[8]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000413]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000414]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000415]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000416]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000417]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000418]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000419]
  Queries value:            HKCU\software\microsoft\windows\currentversion\ime\imtc70[]
  Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[useupdatedfield]
  Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[infocompressedvalid]
  Queries value:
```

```
HKCU\software\microsoft\windows\currentversion\ime\imtc70[recordcompressedactive]
   Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[typeenabledcheck]
   Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[pagecompressedinvalid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\run[sonyagent]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[enabledhcp]
   Queries value:              HKLM\software\microsoft\rpc[maxrpcsize]
   Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
   Queries value:              HKLM\system\setup[oobeinprogress]
   Queries value:              HKLM\system\setup[systemsetupinprogress]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[category]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[name]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[description]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
   Queries value:
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\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
   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]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\adobe flash player
activex[displayname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\connection
manager[uninstallstring]
   Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\directdrawex[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\fontcore[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie40[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie4data[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie5bakex[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\iedata[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mobileoptionpack[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\schedulingagent[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\wic[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{196bb40d-1578-3d01-b289-
befc77a11a1e}[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{196bb40d-1578-3d01-b289-
befc77a11a1e}[displayname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-4ca4-87b4-
2f83217002ff}[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-4ca4-87b4-
2f83217002ff}[displayname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{4a03706f-666a-4037-7777-
5f2748764d10}[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-
0000000ff1ce}[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-
0000000ff1ce}[displayname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90850409-6000-11d3-8cfe-
0150048383c9}[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90850409-6000-11d3-8cfe-
0150048383c9}[displayname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95120000-003f-0409-0000-
0000000ff1ce}[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95120000-003f-0409-0000-
0000000ff1ce}[displayname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-
0000000ff1ce}[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-
0000000ff1ce}[displayname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-
a93000000001}[uninstallstring]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-
a93000000001}[displayname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[icon]
  Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[security]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
   Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[category]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[name]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[description]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[relativepath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[localizedname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[icon]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[security]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[initfolderhandler]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]
  Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[publishexpandedpath]
  Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-
9f6d-47a2-aaae-29d317c6f066}[initfolderhandler]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[commonfilesdir]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[category]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[name]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[parentfolder]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[description]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[relativepath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[localizedname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[icon]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[security]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[initfolderhandler]
   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:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
   Queries value:              HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\addressbook[addressbook]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\connection
```

```
manager[connection manager]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\directdrawex[directdrawex]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\fontcore[fontcore]
   Queries 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]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\iedata[iedata]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mobileoptionpack[mobileoptionpack]
   Queries 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\wow6432node\microsoft\windows\currentversion\uninstall\{4a03706f-666a-4037-7777-
5f2748764d10}[{4a03706f-666a-4037-7777-5f2748764d10}]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[category]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[name]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[parentfolder]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[description]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[relativepath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[localizedname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[icon]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[security]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[initfolderhandler]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
   Queries value:              HKCU\software\classes\[clsid\{11c1d741-a95b-11d2-8a80-
0080adb32ff4}\inprocserver32]
   Queries value:              HKLM\software\classes[clsid\{11c1d741-a95b-11d2-8a80-
0080adb32ff4}\inprocserver32]
   Queries value:              HKCU\software\classes\[ftp++.link\shell\open\command]
   Queries value:              HKLM\software\classes[ftp++.link\shell\open\command]
   Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[useupdatedfield]
   Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[infocompressedvalid]
   Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[recordcompressedactive]
   Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[typeenabledcheck]
   Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[pagecompressedinvalid]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\windows\currentversion\run[sonyagent]
   Value changes:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[pagecompressedinvalid]
```