# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3333, Task ID: 840

Task ID: 840 Risk Level: 10

Date Processed: 2016-05-18 10:44:56 (UTC)

Processing Time: 62.4 seconds IntelliVM Virtual Environment:

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

Sample ID: Type: admin Owner:

752d6fe81122349daf998a56f48e0b38 Label:

Date Added: 2016-05-18 10:30:52 (UTC) PE32:win32:gui File Type:

File Size: 827904 bytes

752d6fe81122349daf998a56f48e0b38 MD5:

e36aa66b3e7928b47f8c4beb0ab46a2e886f9f87ca6de7cf7fd05d8f5457b020 SHA256:

Description: None

### Pattern Matching Results

Modifies registry autorun entries

Writes to system32 folder

10 Creates malicious events: Kelihos trojan 2 [Spam]

3 Connects to local host.

5 Adds autostart object

5 PE: Contains compressed section

5 Creates file in drivers folder

#### Static Events

Anomaly: PE: No DOS stub

#### Process/Thread Events

C:\WINDOWS\Temp\752d6fe81122349daf998a56f48e0b38.exe Creates process:

["c:\windows\temp\752d6fe81122349daf998a56f48e0b38.exe"] Loads service: NPF [system32\drivers\NPF.sys]

## Named Object Events

Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-Creates mutex: 507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates event: \BaseNamedObjects\userenv: User Profile setup event

\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore: Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

## File System Events

C:\WINDOWS\Temp\tmp.exe Creates Creates: C:\WINDOWS\system32\Packet.dll

Creates C:\WINDOWS\system32\wpcap.dll Creates: C:\WINDOWS\system32\drivers\npf.sys

C:\WINDOWS\Prefetch\752D6FE81122349DAF998A56F48E0-1635C0C2.pf Opens:

Opens: C:\Documents and Settings\Admin Opens: C:\WINDOWS\system32\comcat.dll Opens: C:\WINDOWS\system32\wmdmps.dll Opens: C:\WINDOWS\system32\imm32.dll

C:\WINDOWS\system32\urlmon.dll.123.Manifest Opens: Opens: C:\WINDOWS\system32\urlmon.dll.123.Config C:\WINDOWS\WinSxS\x86\_Microsoft.Windows.Common-Opens:

Controls\_6595b64144ccf1df\_6.0.2600.5512\_x-ww\_35d4ce83

C:\WINDOWS\WinSxS\x86\_Microsoft.Windows.Common-Opens:

Controls\_6595b64144ccf1df\_6.0.2600.5512\_x-ww\_35d4ce83\comctl32.dll

C:\WINDOWS\WindowsShell.Manifest Opens: C:\WINDOWS\WindowsShell.Config Opens:

C:\WINDOWS\system32\WININET.dll.123.Manifest Opens: C:\WINDOWS\system32\WININET.dll.123.Config Opens:

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

Opens: C:\WINDOWS\system32\dnsapi.dll

```
C:\WINDOWS\system32\ws2_32.dll
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\psapi.dll
 Opens:
                         C:\WINDOWS\system32\shell32.dll
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
                         C:\WINDOWS\Temp
 Opens:
 Opens:
                         C:\WINDOWS\Temp\tmp.exe
                         C:\WINDOWS\Temp\8687eaa8-0e77-4e19-ad50-c3c35644151f
 Opens:
                         C:\dev\urandom
 Opens:
 Opens:
                         C:\
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\AUTOEXEC.BAT
 Opens:
                         C:\WINDOWS\system32\drivers
 Opens:
                         C:\WINDOWS\system32\wpcap.dll
 Opens:
                         C:\boot.ini
 Opens:
                         C:\CONFIG.SYS
 Opens:
                         C:\Documents and Settings
 Opens:
                         C:\Documents and Settings\Admin\Application Data
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\AdobeCMapFnt09.1st
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Acrobat\9.0\AdobeSysFnt09.lst
                         C:\WINDOWS\system32\wpcap.dll.2.Manifest
 Opens:
                         C:\WINDOWS\system32\wpcap.dll.2.Config
 Opens:
 Opens:
                         C:\WINDOWS\system32\Packet.dll
 Opens:
                         C:\WINDOWS\system32\packet.dll.2.Manifest
                         C:\WINDOWS\system32\packet.dll.2.Config
 Opens:
 Opens:
                         C:\WINDOWS\system32\npptools.dll
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0\Forms
 Opens:
                         C:\WINDOWS\system32\mfc42u.dll
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Acrobat\9.0\JavaScripts
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Acrobat\9.0\JavaScripts\glob.js
                         C:\WINDOWS\system32\drivers\npf.sys
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts\glob.settings.js
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\SharedDataEvents
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Acrobat\9.0\UserCache.bin
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Flash Player
                         C:\Documents and Settings\Admin\Application Data\Adobe\Flash
 Opens:
Player\AssetCache
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Flash
Player\AssetCache\7PLTA3CP
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Linguistics
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\all
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\brt
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\can
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\eng
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Adobe\LogTransport2}
 Opens:
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\LogTransport2\Logs
                         C:\Documents and Settings\Admin\Application Data\desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Identities
                         C:\Documents and Settings\Admin\Application Data\Identities\{5792731B-
 Opens:
1E8B-4ECF-8560-0E560368800D}
                         C:\Documents and Settings\Admin\Application Data\Macromedia
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Opens:
Player\#SharedObjects\45PY3TTW
```

```
Opens:
                        C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support
                        C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Opens:
Player\macromedia.com\support\flashplayer
                        C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Opens:
Player\macromedia.com\support\flashplayer\sys
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
                        C:\WINDOWS\system32\npp\ndisnpp.dll
 Opens:
 Opens:
                        C:\WINDOWS\system32\rpcss.dll
 Opens:
                        C:\WINDOWS\system32\MSCTF.dll
 Opens:
                        C:\WINDOWS\system32\npp
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Microsoft
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Microsoft\AddIns
                        C:\Documents and Settings\Admin\Application Data\Microsoft\Credentials
 Opens:
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-1003
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\CryptnetUrlCache
 Opens:
                        C:\Documents and Settings\Admin\Application
{\tt Data} \verb|\Microsoft| CryptnetUrl Cache \verb|\Content|
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\0797C381B2F87EB5A1D5573BD15BA4F4
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\CryptnetUrlCache\Content\135BD6A358680A7BF1CCEC7C0172393D
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\3130B1871A126520A8C47861EFE3ED4D
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\60E31627FDA0A46932B0E5948949F2A5
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\62B5AF9BE9ADC1085C3C56EC07A82BF6
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D49D759AD
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7396C420A8E1BC1DA97F1AF0D10BAD21
                        C:\Documents and Settings\Admin\Application
 Opens:
C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\8DFDF057024880D7A081AFBF6D26B92F
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015
                        C:\Documents and Settings\Admin\Application
 Opens:
C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\F482C95F83F1B59228F1B1E720F2EDF1
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\0797C381B2F87EB5A1D5573BD15BA4F4
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\135BD6A358680A7BF1CCEC7C0172393D
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497DD56F57004
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\3130B1871A126520A8C47861EFE3ED4D
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\60E31627FDA0A46932B0E5948949F2A5
 Opens:
                        C:\WINDOWS\win.ini
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\62B5AF9BE9ADC1085C3C56EC07A82BF6
 Opens:
                        C:\Users\
 Opens:
                        C:\Documents and Settings\Admin\Application Data\AceBIT\
 Opens:
                        C:\Documents and Settings\All Users\Application Data\AceBIT\
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application Data\AceBIT\
 Opens:
                        C:\WINDOWS\system32\pstorec.dll
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD
                        C:\WINDOWS\system32\atl.dll
 Opens:
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7396C420A8E1BC1DA97F1AF0D10BAD21
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7B2238AACCEDC3F1FFE8E7EB5F575EC9
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\8DFDF057024880D7A081AFBF6D26B92F
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\A44F4E7CB3133FF765C39A53AD8FCFDD
 Opens:
                        C:\Documents and Settings\Admin\Application
```

```
C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
  Opens:
1-5-21-1757981266-507921405-1957994488-1003
  Opens:
                                    {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Crypto\RSA\S-line(C))} \\
1-5-21-1757981266-507921405-1957994488-1003\6b29ae44e85efac3c72ff4d1865d73f1_fa860dc5-a965-4200-
a9d4-fb930ff1911b
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
1-5-21-1757981266-507921405-1957994488-1003\83aa4cc77f591dfc2374580bbd95f6ba_fa860dc5-a965-4200-
a9d4-fb930ff1911b
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer
                                    {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Internet}
  Opens:
Explorer\brndlog.bak
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\brndlog.txt
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Desktop.htt
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
  Opens:
Explorer\Quick Launch
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\desktop.ini
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
  Opens:
Explorer\Quick Launch\Show Desktop.scf
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Media Player
                                    {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\MMC}
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Office
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\Office\Excel12.pip
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Office\Recent
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\Office\Recent\Desktop.ini
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Protect
  Opens:
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\Protect\CREDHIST
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003
                                    \label{lem:c:Documents} C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-Relation\N-1-R
  Opens:
5-21-1757981266-507921405-1957994488-1003\3ea8a527-1704-4983-8596-ab49c663cca3
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
  Opens:
5-21-1757981266-507921405-1957994488-1003\4f5d6884-c60c-4cd3-906b-3d677949fac1
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\fe1a937a-0ac9-4cf1-978d-5d0742ed2858
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\Preferred
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Speech
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Speech\Files
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\Speech\Files\UserLexicons
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons\SP_6A65DB879F95470886BD7EFE4977B10E.dat
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\SystemCertificates
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\SystemCertificates\My\Certificates
  Opens:
                                    C:\Documents and Settings\Admin\Application
{\tt Data\Microsoft\SystemCertificates\My\CRLs}
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\SvstemCertificates\Mv\CTLs
                                    C:\Documents and Settings\Admin\Application Data\Google\Chrome\
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Templates
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Chrome\
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Windows
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\Windows\Themes
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\Windows\Themes\Custom.theme
                                    C:\Documents and Settings\All Users\Application Data\Google\Chrome\
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Chromium\
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Chromium\
                                    C:\Documents and Settings\All Users\Application Data\Chromium\
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Oracle
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\ChromePlus\
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Oracle\Java
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\ChromePlus\
```

Data\Microsoft\CryptnetUrlCache\MetaData\F482C95F83F1B59228F1B1E720F2EDF1

```
C:\Documents and Settings\All Users\Application Data\ChromePlus\
 Opens:
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Bromium\
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Oracle\Java\Uninstall
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application Data\Bromium\
                        {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Sun}
 Opens:
 Opens:
                        C:\Documents and Settings\All Users\Application Data\Bromium\
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Sun\Java
                        C:\Documents and Settings\Admin\Application Data\Nichrome\
 Opens:
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Sun\Java\AU
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Nichrome\
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment
 Opens:
                        C:\Documents and Settings\All Users\Application Data\Nichrome\
                        C:\Documents and Settings\Admin\Application Data\Comodo\
 Opens:
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application Data\Comodo\
 Opens:
                        C:\Documents and Settings\All Users\Application Data\Comodo\
 Opens:
                        C:\Documents and Settings\Admin\Application Data\RockMelt\
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\RockMelt\
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\0
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\1
                        C:\Documents and Settings\All Users\Application Data\RockMelt\
 Opens:
 Opens:
                        C:\Documents and Settings\Admin\Application
C:\Documents and Settings\Admin\Application Data\MapleStudio\ChromePlus\
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\MapleStudio\ChromePlus\
 Opens:
                        C:\Documents and Settings\All Users\Application
Data\MapleStudio\ChromePlus\
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\11
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\12
 Opens:
                        C:\Documents and Settings\Admin\Application
C:\Documents and Settings\Admin\Application Data\browser.yandex\
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\browser.yandex\
                        C:\Documents and Settings\All Users\Application Data\browser.yandex\
 Opens:
 Opens:
                        C:\Documents and Settings\Admin\Desktop
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171.idx
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\13
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\14
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\15
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\16
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17
 Opens:
                        C:\Documents and Settings\Admin\Application
Opens:
                        C:\Documents and Settings\Admin\Application
Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-6.0.lap
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\18
                        C:\Documents and Settings\Admin\Application
 Opens:
Data \S un \S ava \S eployment \S ache \S 6.0 \S 19
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1.idx
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-6.0.lap
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\2
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\20
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\21
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\22
 Opens:
                        C:\Documents and Settings\Admin\Application
```

Data\Sun\Java\Deployment\cache\6.0\23 Opens: C:\Documents		Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\24	anu	Settings (Admit (Application
Opens: C:\Documents	and	Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\25	and	Sottings\Admin\Annlication
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\26		Settings\Admin\Application
Opens: C:\Documents	and	${\tt Settings \LAdmin \LApplication}$
Data\Sun\Java\Deployment\cache\6.0\27		Cattings \ Admin \ Annlinetin
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\28		Settings\Admin\Application
Opens: C:\Documents		Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\29		
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\3	and	Settings\Admin\Application
	and	Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\30		
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\31	and	Settings\Admin\Application
	and	Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\32		
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\33	and	Settings\Admin\Application
	and	Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\34		
·		Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\35 Opens: C:\Documents		Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\36		
·		Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\37 Opens: C:\Documents		Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\38		500011185 W. W. W. W. P. P. T. C.
	and	Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\39 Opens: C:\Documents	and	Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\4	unu	Sectings wamin application
		Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\40 Opens: C:\Documents		Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\41	unu	Sectings (Main in Application
Opens: C:\Documents	and	Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\42	and	Settings\Admin\Annlication
		Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents	and	Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43	and \1ca	Settings\Admin\Application 2666b-2c59609d
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43	and \1cai	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents C:\Documents	and \1cai and \1cai and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44	and \1ca and \1ca and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44	and \1ca and \1ca and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents	and \1cai and \1cai and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46	and \1ca and \1ca and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46	and \1ca and \1ca and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents	and \1ca: and \1ca: and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents	and \1ca; and \1ca; and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents	and \1ca; and \1ca; and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents	and \1ca: and \1ca: and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents	and \1ca: and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents	and \1ca: and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents	and \\1ca_and \\	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50	and \\1ca:	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents	and \\1ca:	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents	and \1ca: and \1	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52	and land and and and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52	and land and and and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\54 Opens: C:\Documents	and land and and and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50	and land and and and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50	and land and and and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\55 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\56 Opens: C:\Documents	and land and and and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\56	and land and and and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\56	and land and and and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\53 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\55 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\56 Opens: C:\Documents	and land and and and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\43 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\46 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\55 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\56 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\56 Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\57	and land and and and and and and and and and	Settings\Admin\Application 2666b-2c59609d Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application 2666b-2c59609d.idx Settings\Admin\Application

```
Opens:
                         C:\Documents and Settings\Admin\Application
{\tt Data\Sun\Java\Deployment\cache\6.0\6}
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\60
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\61
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\62
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\63
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\7
                         C:\Documents and Settings\Admin\Application
 Opens:
C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\9
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\host
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\lastAccessed
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\muffin
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\tmp
                         C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\ext
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Sun\Java\Deployment\log}
 Opens:
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\security
                         C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\tmp
 Opens:
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\tmp\si
                         C:\Documents and Settings\Admin\Application Data\Sun\Java\jre1.7.0_02
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application Data
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Acrobat\9.0
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\deployment.properties
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\Acrobat\9.0\Cache
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Acrobat\9.0\Cache\Search
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Acrobat\9.0\Updater
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\Color
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Updater6
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Updater6\Install
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\CD Burning
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Credentials
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-1003
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\security\trusted.certs
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}^
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\FBANKAIW
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\G4DZ1I7H
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\J3XY1QNV
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\TLMHA51J
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer
                         C:\Documents and Settings\Admin\Local Settings\Application
```

Opens:

```
Data\Microsoft\Internet Explorer\Custom Settings
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Custom Settings\Custom0
 Opens:
                         C:\Documents and Settings\Admin\Cookies
                         C:\Documents and Settings\Admin\Cookies\admin@c1.microsoft[2].txt
 Opens:
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Internet Explorer\DOMStore
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\DOMStore\OWORJP5C
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\LQLIM8KB
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Recovery
                         C:\Documents\ and\ Settings\Admin\Cookies\admin@microsoft[1].txt
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Active
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Recovery\Last Active
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Services
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Media Player
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Office
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Microsoft\Office\12.0
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Office\14.0
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Silverlight
 Opens:
                         C:\Documents and Settings\Admin\Cookies\admin@rto.microsoft[1].txt
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Windows
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Windows Media\9.0
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application Data\Sun
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0
 Opens:
                         C:\Documents and Settings\Admin\Cookies\admin@search.microsoft[1].txt
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\0
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\1
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\10
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\11
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\12
                         C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt
 Opens:
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Sun\Java\Deployment\cache\6.0\13
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Sun\Java\Deployment\cache\6.0\14
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\15
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Sun\Java\Deployment\cache\6.0\16
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\17
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\18
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\19
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\2
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\20
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\21
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\22
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\23
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\24
                         C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[3].txt
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\25
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\26
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\27
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\28
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\29
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\3
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\30
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\31
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\32
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\33
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Sun\Java\Deployment\cache\6.0\34
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\36
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\38
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\39
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\4
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\40
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\41
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\42
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Sun\Java\Deployment\cache\6.0\43
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\44
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\45
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\46
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\47
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\48
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\49
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\50
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\51
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\52
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\53
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\54
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\55
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\56
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\57
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\58
                         C:\Documents and Settings\Admin\Favorites
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Sun\Java\Deployment\cache\6.0\59
```

```
Opens:
                         C:\Documents and Settings\Admin\Favorites\Desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\6
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
{\tt Data\Sun\Java\Deployment\cache\6.0\60}
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\61
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\62
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\63
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\7
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\8
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\9
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\host
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\muffin
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\tmp
                         C:\Documents and Settings\All Users\Application Data
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Adobe
 Opens:
                         {\tt C:\Documents\ and\ Settings\All\ Users\Application\ Data\Adobe\Acrobat}
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Links
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Adobe\Acrobat\9.0
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Links\desktop.ini
                         C:\Documents and Settings\All Users\Application
 Opens:
Data\Adobe\Acrobat\9.0\Replicate
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Adobe\Acrobat\9.0\Replicate\Security
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Adobe\Reader
                         C:\Documents and Settings\All Users\Application Data\Adobe\Reader\9.3
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Adobe\Reader\9.4
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Adobe\Reader\9.4\ARM
                         C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Links\Suggested Sites.url
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Favorites\Links\Web\ Slice\ Gallery.url}
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Favorites\Microsoft\ Websites\IE\ Add-on}
 Opens:
site.url
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Adobe\Updater6
                         C:\Documents and Settings\All Users\Application Data\Microsoft
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Crypto\DSS
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Crypto\DSS\MachineKeys
                         C:\Documents and Settings\All Users\Application
 Opens:
Data\Microsoft\Crypto\RSA
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Crypto\RSA\MachineKeys
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Crypto\RSA\S-1-5-18
                         C:\Documents and Settings\All Users\Application Data\Microsoft\HTML Help
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE site on
Microsoft.com.url
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Microsoft\Media
Index
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Microsoft\Media
Plaver
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Microsoft\Network
                         C:\Documents and Settings\All Users\Application
 Opens:
Data\Microsoft\Network\Connections
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Cm
                         {\tt C:\Documents\ and\ Settings\Admin\Favorites\Microsoft\ Websites\Microsoft\ }}
 Opens:
At Home.url
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Downloader
                         C:\Documents and Settings\All Users\Application Data\Microsoft\PlayReady
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Microsoft\User
Account Pictures
                         C:\Documents and Settings\All Users\Application Data\Microsoft\User
 Opens:
Account Pictures\Default Pictures
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Work.url
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Sun
```

```
C:\Documents and Settings\All Users\Application Data\Sun\Java
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Sun\Java\Java
Update
                         C:\Program Files\Whisper Technology\FTP Surfer\
 Opens:
                         C:\Documents and Settings\Admin\Application Data\FTPGetter\
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application Data\FTPGetter\
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\FTPGetter\
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Estsoft\ALFTP\
                         C:\Documents and Settings\All Users\Application Data\Estsoft\ALFTP\
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Estsoft\ALFTP\
 Opens:
                         C:\Documents and Settings\Admin\Application Data\BlazeFtp\
 Opens:
                         C:\Documents and Settings\All Users\Application Data\BlazeFtp\
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\BlazeFtp\
                         C:\Documents and Settings\Admin\Application Data\3D-FTP\
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application Data\3D-FTP\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application Data\3D-FTP\
 Opens:
                         C:\Documents and Settings\Admin\Application Data\SiteDesigner\
 Opens:
                         C:\Documents and Settings\All Users\Application Data\SiteDesigner\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\SiteDesigner\
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
Store.url
                         C:\Documents and Settings\Admin\Favorites\MSN.com.url
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Radio Station Guide.url
 Opens:
                         C:\Documents and Settings\Admin\IECompatCache
                         C:\Documents and Settings\Admin\IECompatCache\index.dat
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\IETldCache
 Opens:
                         C:\Documents and Settings\Admin\IETldCache\index.dat
                         C:\Documents and Settings\Admin\Local Settings
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Adobe\Acrobat\9.0\Cache\AcroFnt09.1st
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Updater\updater.log
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Color\ACECache10.lst
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Updater6\aum.log
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\Updater6\aumLib.log
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\GDIPFONTCACHEV1.DAT
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\IconCache.db
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Feeds\FeedsStore.feedsdb-ms
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Suggested Sites~.feed-ms
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds\\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-
ms
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Microsoft\Feeds Cache\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\FBANKAIW\desktop.ini
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Feeds Cache\FBANKAIW\fwlink[1]
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\G4DZ1I7H\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\G4DZ1I7H\fwlink[1]
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Feeds Cache\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\J3XY1QNV\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY1QNV\fwlink[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\TLMHA51J\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\TLMHA51J\ieonline.microsoft[1]
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\brndlog.bak
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\brndlog.txt
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Custom Settings\Custom0\install.ins
```

```
Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK\www.microsoft[1].xml
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\index.dat
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\frameiconcache.dat
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Active\{49831954-C276-11E3-AE24-08002733366F}.dat
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{80236AC0-AAD6-11E3-AE20-
08002733366F}.dat
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\rsoplog.bak
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\rsoplog.txt
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Silverlight\mssl.lck
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Windows\UsrClass.dat
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Windows\UsrClass.dat.LOG
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc.idx
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\47\15572e2f-21932044
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\7\2bbaaf87-5ca9d237.idx
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\lastAccessed
                        C:\Documents and Settings\Admin\Local Settings\desktop.ini
 Opens:
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\History
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
                        C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\desktop.ini
                        C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\index.dat
 Opens:
                        C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014031220140313
 Opens:
                        C:\Documents and Settings\Admin\Local
Settings \verb|\History\History\IE5\MSHist012014031220140313\lindex.dat
                        C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014033120140407
                        C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407\index.dat
 Opens:
                        C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413
                        C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014041220140413\index.dat
                        C:\Documents and Settings\Admin\Local Settings\Temp
 Opens:
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Temp\296c0.msp
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Temp\AdobeARM.log
 Opens:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\AdobeARM_NotLocked.log
 Opens:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\ASPNETSetup_00000.log
                        C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ASPNETSetup_00001.log
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Temp\AUCHECK_PARSER.txt
 Opens:
                        {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Compatibility\ Pack}
for the 2007 Office system (0).log
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Temp\dd_clwireg.txt
                        C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_depcheck_NETFX_EXP_35.txt
                        C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_dotnetfx35error.txt
 Opens:
                        C:\Documents and Settings\Admin\Local
```

```
Settings\Temp\dd_dotnetfx35install.txt
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_NET_Framework20_Setup164F.txt
                         C:\Documents and Settings\Admin\Local
 Opens:
{\tt Settings\Temp\dd\_NET\_Framework30\_Setup16AE.txt}
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework35_MSI16E2.txt
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_NET_Framework35_MSI63E0.txt
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_RGB9RAST_x86.msi601E.txt
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA2A49.txt
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA3565.txt
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA35A0.txt
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_XPS.txt
                         C:\Documents and Settings\Admin\Local Settings\Temp\gen_py
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\gen_py\2.7
 Opens:
                         \label{lem:local_Settings} C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\gen\_py\2.7\dicts.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
                           _init__.py
Settings\Temp\gen_py\2.7\_
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\JAUReg.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\java_install.log
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\java_install_reg.log
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\jusched.log
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Microsoft\ PowerPoint}
 Opens:
Viewer (0).log
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_10.0.30319
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20131223_035827352-MSI_vc_red.msi.txt
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Opens:
2010 x86 Redistributable Setup_20131223_035827352.html
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_152314679-MSI_vc_red.msi.txt
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Opens:
2010 x86 Redistributable Setup_20140312_152314679.html
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Opens:
2010 x86 Redistributable Setup_20140312_152634747-MSI_vc_red.msi.txt
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Opens:
2010 x86 Redistributable Setup_20140312_152634747.html
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Opens:
2010 x86 Redistributable Setup_20140312_154212618-MSI_vc_red.msi.txt
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Opens:
2010 x86 Redistributable Setup_20140312_154212618.html
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\pywin32_postinstall.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\setup.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\SilverlightO.log
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\SilverlightMSI.log
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\uxeventlog.txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\AntiPhishing
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\AntiPhishing\2CEDBFBC-DBA8-43AA-B1FD-CC8E6316E3E2.dat
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\300lo[1].json
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\300lo[2].json
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\88666cc6-d578-45c8-baf0-89d3837f41c3_89[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\93e33485-fea3-4687-a642-2c5dd233522f_12[1].eot
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[1].txt
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[2].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files \verb|\| Content.IE5 \verb|\| CXCXW1MR \verb|\| ADSAdClient31[3].txt \\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[4].txt
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[5].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\adServer[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\auth016[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\CXCXW1MR\bimapping[2].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\broker[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CA9ATUDW.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\CAMLW29Z.jsx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CATM568T.jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\CAVLZJ9D.jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\core114[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\core114[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\css[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\css[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\css[3].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\DataList[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\e64030e7-ad8c-4be8-a45a-b69a2df3caef_13[1].eot
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\event[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[2].js
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\CXCXW1MR\event[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\event[5].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\false[1].htm
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\General[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\General[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\georedirect[1].htm
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\georedirect[2].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\georedirect[3].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\georedirect[4].htm
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\install[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\js[2].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\LoginStatus[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\Nebula[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\omnibase[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomBlade[2].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\onemscomfooter[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[3].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\request[1].php
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\ScriptResource[1].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\ScriptResource[2].axd
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[3].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\ScriptResource[4].axd
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[5].axd
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\script[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\script[1].jsx
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\script[2].jsx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\true[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\true[2].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\views[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\WebResource[1].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\wtid[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\wt_capi[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\736e3781-6a19-4119-b717-e61f0d8982c0_12[1].eot
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\ADSAdClient31[1].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\ADSAdClient31[2].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\auth016[1].js
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\ONWV4FIP\auth016[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\bing[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\broker-config_s1[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\broker-config_s1[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\broker-config_s1[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\CA39W67Q.jsx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\CAANG12B.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\CAU35S9Y.jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\ChangePassword[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\ClickToInstall[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\ClientBiSettings.Wol[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\confirmation[1].aspx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\core114[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\counter017[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\counter017[2].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\css[1].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\css[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\css[2].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\details[1].htm
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\details[21.htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\event[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\event[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\event[6].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\General[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\gl_social[1].svg
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\Install[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\ONWV4FIP\js[1].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[2].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[3].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[4].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\Login[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\modernizr.wol[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\nb-no[2].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\omniture_s_code[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\onemscomfooter[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\onemscomsearch[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\oneMscomSocial[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\PasswordRecovery[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\ScriptResource[1].axd
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\ONWV4FIP\ScriptResource[2].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\script[2].jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\SearchMSStoreClient[2].js
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\ONWV4FIP\serverComponent[1].php
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\ONWV4FIP\siteresource[1].ashx
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\ONWV4FIP\siteresource[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\style[1].cssx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files \verb|\Content.IE5| ONWV4FIP \verb|\Tracker[1].js| \\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\true[1].htm
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\wol.common[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\wt_capi[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\08ce8e54-41ba-4695-9963-a7669022faec_12[1].eot
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\15d2470f-0fcf-45e9-bf5b-c943236a61cf_27[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\300lo[1].json
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\67706439-4969-4bc3-9e3b-50770f40b20e_36[1].js
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\QXMNQBKF\ADSAdClient31[1].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ADSAdClient31[2].txt
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\auth016[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\broker-config_s1[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\broker-config_s1[2].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\broker-config_s1[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\broker-config_s2[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\CA9P88JQ.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\core114[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\counter017[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\counter017[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\css[1].ashx
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\css[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\css[2].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\css[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\DetailsView[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\event[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\event[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\feedback[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\FormView[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\GlobalResources[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\gl_site[1].svg
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\Import[1].css
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\QXMNQBKF\Install[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\js[1].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\js[2].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\js[3].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\js[4].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\Menu[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\omnibase[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\oneMscomBlade[2].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\oneMscomComponents[2].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\oneMscomNav[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\onemscomsearch[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\oneMscomSocial[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\ScriptResource[1].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\script[1].jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\script[2].jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\SilverlightAtlas-MSCOM-Tracking[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\Silverlight[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\styles[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\uninstall-arp-win[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files \verb|\| Content.IE5 \verb|\| QXMNQBKF \verb|\| WebResource[1].axd \\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\OXMNOBKF\welcome[11.htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\windows8_site_ltr[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\300lo[1].json
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\300lo[2].json
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\ADSAdClient31[1].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\adServer[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

Opens:

```
Files\Content.IE5\UH4D6D6X\auth016[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\background_gradient[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bimapping[2].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\broker-config_s1[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\broker-config_s1[3].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[4].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\broker-config_s1[5].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\broker[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\broker[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\CA01EFSH.isx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\CA7GG9IO.css
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\UH4D6D6X\CA8VUH6F.css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CAI7MNGV.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\CallingControl[1].aspx
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\UH4D6D6X\confirmation[1].aspx
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\UH4D6D6X\confirmation[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\Cookies[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\core114[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\counter017[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CreateUserWizard[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\css[1].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files \verb|\Content.IE5\UH4D6D6X\css[1].css|
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\css[2].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\desktop.ini
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\UH4D6D6X\details-social[2].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\enable[2].htm
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\event[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\event[5].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\GridView[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\info_48[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\InstallPageReskin[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\Install[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\internet-explorer-8-details[1].htm
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\js[1].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\js[2].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\js[3].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\Marquee[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\mbox[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\MicrosoftAjax[1].js
```

```
C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\ms[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\navcancl[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files \verb|\Content.IE5>UH4D6D6X\verb|\comComponents[1].css|
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\oneMscomListLayout[2].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\oneMscomListLayout[3].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\oneMscomNav[2].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\pre_broker[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ScriptResource[1].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\ScriptResource[2].axd
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\script[2].jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\serverComponent[1].php
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\silverlight[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\TreeView[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\webtrends[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\wt[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.MSO
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\My Documents
 Opens:
                         C:\Documents and Settings\Admin\My Documents\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\My Documents\My Music
                         C:\Documents and Settings\Admin\My Documents\My Music\Desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\My Documents\My Music\Sample Music.lnk
 Opens:
                         C:\Documents and Settings\Admin\My Documents\My Pictures
                         C:\Documents and Settings\Admin\My Documents\My Pictures\Desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\My Documents\My Pictures\Sample
Pictures.lnk
                         C:\Documents and Settings\Admin\NetHood
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\NTUSER.DAT
 Opens:
                         C:\Documents and Settings\Admin\NTUSER.DAT.LOG
 Opens:
                         C:\Documents and Settings\Admin\ntuser.ini
 Opens:
                         C:\Documents and Settings\Admin\PrintHood
                         C:\Documents and Settings\Admin\PrivacIE
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\PrivacIE\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Recent
 Opens:
                         C:\Documents and Settings\Admin\Recent\Desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Recent\fp_11.0.1.152_archive.lnk
 Opens:
                         C:\Documents and Settings\Admin\SendTo
 Opens:
                         C:\Documents and Settings\Admin\SendTo\Compressed (zipped)
Folder.ZFSendToTarget
                         C:\Documents and Settings\Admin\SendTo\Desktop (create
 Opens:
shortcut).DeskLink
                         C:\Documents and Settings\Admin\SendTo\desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\SendTo\Mail Recipient.MAPIMail
 Opens:
                         C:\Documents and Settings\Admin\SendTo\My Documents.mydocs
 Opens:
                         C:\Documents and Settings\Admin\Start Menu
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility
 Opens:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
                         C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Address
 Opens:
Book.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Command
Prompt.lnk
                         C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\desktop.ini
```

```
Opens:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment
 Opens:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
                         C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Notepad.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Program
Compatibility Wizard.lnk
                         C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\Synchronize.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\System
Tools
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\System
Tools\Internet Explorer (No Add-ons).lnk
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Tour
 Opens:
Windows XP.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Windows
Explorer.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Internet
Explorer.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Outlook Express.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Remote
Assistance.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Startup
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Startup\desktop.ini
                         C:\Documents and Settings\Admin\Start Menu\Programs\Windows Media
 Opens:
Player.lnk
 Opens:
                         C:\Documents and Settings\Admin\Templates
                         C:\Documents and Settings\Admin\Templates\amipro.sam
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Templates\lotus.wk4
 Opens:
                         C:\Documents and Settings\Admin\Templates\presenta.shw
                         {\tt C:\Documents\ and\ Settings\Admin\Templates\quattro.wb2}
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Templates\wordpfct.wpd
 Opens:
                         C:\Documents and Settings\Admin\Templates\wordpfct.wpg
                         C:\Documents and Settings\Administrator
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Application Data
 Opens:
                         C:\Documents and Settings\Administrator\Application Data\desktop.ini
                         {\tt C:\Documents\ and\ Settings\Administrator\Application\ Data\Microsoft}
 Opens:
                         C:\Documents and Settings\Administrator\Application
 Opens:
Data\Microsoft\Credentials
                         C:\Documents and Settings\Administrator\Application
 Opens:
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-500
                         C:\Documents and Settings\Administrator\Application
 Opens:
Data\Microsoft\Internet Explorer
                         C:\Documents and Settings\Administrator\Application
Data\Microsoft\Internet Explorer\brndlog.bak
 Opens:
                         C:\Documents and Settings\Administrator\Application
Data\Microsoft\Internet Explorer\brndlog.txt
                         C:\Documents and Settings\Administrator\Application Data\Microsoft\Media
 Opens:
Player
 Opens:
                         C:\Documents and Settings\Administrator\Application
Data\Microsoft\SystemCertificates
 Opens:
                         C:\Documents and Settings\Administrator\Application
Data\Microsoft\SystemCertificates\My
                         C:\Documents and Settings\Administrator\Application
 Opens:
Data\Microsoft\SystemCertificates\My\Certificates
                         C:\Documents and Settings\Administrator\Application
 Opens:
Data\Microsoft\SystemCertificates\My\CRLs
 Opens:
                         C:\Documents and Settings\Administrator\Application
Data\Microsoft\SystemCertificates\My\CTLs
                         C:\Documents and Settings\Administrator\Cookies
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Cookies\index.dat
 Opens:
                         C:\Documents and Settings\Administrator\Desktop
 Opens:
                         C:\Documents and Settings\Administrator\Favorites
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Application Data
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft
                         C:\Documents and Settings\Administrator\Local Settings\Application
 Opens:
Data\Microsoft\Credentials
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-500
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Media Player
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Windows
                         C:\Documents and Settings\Administrator\Local Settings\Application
 Opens:
```

Data\Microsoft\Windows\UsrClass.dat

```
Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat.LOG
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Windows Media
                         C:\Documents and Settings\Administrator\Local Settings\Application
 Opens:
Data\Microsoft\Windows Media\9.0
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML
                         C:\Documents and Settings\Administrator\Local Settings\desktop.ini
 Opens:
 Opens:
                         {\tt C:\Documents\ and\ Settings\Administrator\Local\ Settings\History}
 Opens:
                         C:\Documents and Settings\Administrator\Local
Settings\History\desktop.ini
                         C:\Documents and Settings\Administrator\Local
 Opens:
Settings\History\History.IE5
                         C:\Documents and Settings\Administrator\Local
 Opens:
Settings\History\History.IE5\desktop.ini
                         C:\Documents and Settings\Administrator\Local
 Opens:
Settings\History\History.IE5\index.dat
                         C:\Documents and Settings\Administrator\Local Settings\Temp
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\Content.IE5
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\Content.IE5\CXCXW1MR
                         {\tt C:\Documents\ and\ Settings\backslash Administrator\backslash Local\ Settings\backslash Temporary}
 Opens:
Internet Files\Content.IE5\CXCXW1MR\desktop.ini
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\Content.IE5\desktop.ini
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\Content.IE5\index.dat
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\Content.IE5\ONWV4FIP
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\Content.IE5\ONWV4FIP\desktop.ini
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\Content.IE5\QXMNQBKF
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\Content.IE5\QXMNQBKF\desktop.ini
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\Content.IE5\UH4D6D6X
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\Content.IE5\UH4D6D6X\desktop.ini
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\desktop.ini
 Opens:
                         C:\Documents and Settings\Administrator\My Documents
 Opens:
                         C:\Documents and Settings\Administrator\NetHood
 Opens:
                         C:\Documents and Settings\Administrator\NTUSER.DAT
                         C:\Documents and Settings\Administrator\NTUSER.DAT.LOG
 Opens:
                         C:\Documents and Settings\Administrator\ntuser.ini
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\PrintHood
                         C:\Documents and Settings\Administrator\Recent
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\SendTo
 Opens:
                         C:\Documents and Settings\Administrator\SendTo\Compressed (zipped)
Folder.ZFSendToTarget
                         C:\Documents and Settings\Administrator\SendTo\Desktop (create
 Opens:
shortcut).DeskLink
                         C:\Documents and Settings\Administrator\SendTo\desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\SendTo\Mail Recipient.MAPIMail
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu
                         C:\Documents and Settings\Administrator\Start Menu\desktop.ini
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu\Programs
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories
                         C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Accessibility
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
                         C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Command Prompt.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\desktop.ini
                         C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Entertainment
```

```
C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Entertainment\desktop.ini
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
                         C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Notepad.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Program Compatibility Wizard.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Synchronize.lnk
                         C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Tour Windows XP.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Windows Explorer.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini
                         C:\Documents and Settings\Administrator\Start Menu\Programs\Remote
 Opens:
Assistance.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu\Programs\Startup
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Startup\desktop.ini
                         C:\Documents and Settings\Administrator\Start Menu\Programs\Windows
 Opens:
Media Player.lnk
                         C:\Documents and Settings\Administrator\Templates
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Templates\amipro.sam
 Opens:
                         C:\Documents and Settings\Administrator\Templates\lotus.wk4
 Opens:
                         C:\Documents and Settings\Administrator\Templates\presenta.shw
 Opens:
                         {\tt C:\Documents\ and\ Settings\Administrator\Templates\quattro.wb2}
 Opens:
                         C:\Documents and Settings\Administrator\Templates\wordpfct.wpd
 Opens:
                         C:\Documents and Settings\Administrator\Templates\wordpfct.wpg
 Opens:
                         C:\Documents and Settings\All Users
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Adobe\Acrobat\9.0\Replicate\Security\directories.acrodata
                         C:\Documents and Settings\All Users\Application
 Opens:
Data\Adobe\Reader\9.4\ARM\AdbeRdrUpd951_all_incr.msp
                         C:\WINDOWS\system32\Packet.dll
 Writes to:
 Writes to:
                         C:\WINDOWS\system32\wpcap.dll
 Writes to:
                         C:\WINDOWS\system32\drivers\npf.sys
 Reads from:
                         C:\WINDOWS\Temp\752d6fe81122349daf998a56f48e0b38.exe
 Reads from:
                         C:\AUTOEXEC.BAT
 Reads from:
                         C:\boot.ini
                         C:\CONFIG.SYS
 Reads from:
                         C:\Documents and Settings\Admin\Application
 Reads from:
Data\Adobe\Acrobat\9.0\AdobeCMapFnt09.1st
                         C:\Documents and Settings\Admin\Application
 Reads from:
Data\Adobe\Acrobat\9.0\AdobeSysFnt09.1st
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts\glob.js
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts\glob.settings.js
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\SharedDataEvents
                         C:\Documents and Settings\Admin\Application
 Reads from:
Data\Adobe\Acrobat\9.0\UserCache.bin
                         C:\Documents and Settings\Admin\Application Data\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\0797C381B2F87EB5A1D5573BD15BA4F4
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\135BD6A358680A7BF1CCEC7C0172393D
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\3130B1871A126520A8C47861EFE3ED4D
                         {\tt C:\Documents\ and\ Settings\Admin\Application}
 Reads from:
Data\Microsoft\CryptnetUrlCache\Content\60E31627FDA0A46932B0E5948949F2A5
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\62B5AF9BE9ADC1085C3C56EC07A82BF6
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D49D759AD
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7396C420A8E1BC1DA97F1AF0D10BAD21
 Reads from:
                         C:\Documents and Settings\Admin\Application
Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\8DFDF057024880D7A081AFBF6D26B92F
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\A44F4E7CB3133FF765C39A53AD8FCFDD
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\F482C95F83F1B59228F1B1E720F2EDF1
```

C:\Documents and Settings\Admin\Application

Reads from:

```
Data\Microsoft\CryptnetUrlCache\MetaData\0797C381B2F87EB5A1D5573BD15BA4F4
                                              C:\Documents and Settings\Admin\Application
   Reads from:
\label{lem:decomp} Data \\ \mbox{Microsoft} \\ \mbox{CryptnetUrlCache} \\ \mbox{MetaData} \\ \mbox{135BD6A358680A7BF1CCEC7C0172393D} \\ \mbox{CryptnetUrlCache} \\ \mbox{MetaData} \\ \mbox{MetaData}
                                              C:\Documents and Settings\Admin\Application
   Reads from:
Data\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497DD56F57004
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\3130B1871A126520A8C47861EFE3ED4D
                                              C:\Documents and Settings\Admin\Application
   Reads from:
\label{lem:decomp} Data \\ \mbox{Microsoft} \\ \mbox{CryptnetUrlCache} \\ \mbox{MetaData} \\ \mbox{60E31627FDA0A46932B0E5948949F2A5} \\ \mbox{Microsoft} \\ \mbox{CryptnetUrlCache} \\ \mbox{MetaData} \\ \mbox{MetaData
   Reads from:
                                              C:\WINDOWS\win.ini
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\62B5AF9BE9ADC1085C3C56EC07A82BF6
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7396C420A8E1BC1DA97F1AF0D10BAD21
                                              C:\Documents and Settings\Admin\Application
   Reads from:
Data\Microsoft\CryptnetUrlCache\MetaData\7B2238AACCEDC3F1FFE8E7EB5F575EC9
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\8DFDF057024880D7A081AFBF6D26B92F
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\A44F4E7CB3133FF765C39A53AD8FCFDD
                                              C:\Documents and Settings\Admin\Application
   Reads from:
C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
   Reads from:
1-5-21-1757981266-507921405-1957994488-1003\6b29ae44e85efac3c72ff4d1865d73f1_fa860dc5-a965-4200-
a9d4-fb930ff1911b
   Reads from:
                                              {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Crypto\RSA\S-line(C))} \\
1-5-21-1757981266-507921405-1957994488-1003\83aa4cc77f591dfc2374580bbd95f6ba_fa860dc5-a965-4200-
a9d4-fb930ff1911b
                                              {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Internet}
   Reads from:
Explorer\brndlog.bak
                                              C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
   Reads from:
Explorer\brndlog.txt
                                              C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
   Reads from:
Explorer\Desktop.htt
                                              C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
   Reads from:
Explorer\Quick Launch\desktop.ini
                                              {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Internet}
   Reads from:
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
                                             C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
   Reads from:
Explorer\Quick Launch\Show Desktop.scf
                                              C:\Documents and Settings\Admin\Application
   Reads from:
Data\Microsoft\Office\Excel12.pip
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\Office\Recent\Desktop.ini
                                              C:\Documents and Settings\Admin\Application
   Reads from:
Data\Microsoft\Protect\CREDHIST
                                              C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\3ea8a527-1704-4983-8596-ab49c663cca3
   Reads from:
                                              C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\4f5d6884-c60c-4cd3-906b-3d677949fac1
                                             C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
   Reads from:
5-21-1757981266-507921405-1957994488-1003\fe1a937a-0ac9-4cf1-978d-5d0742ed2858
                                              C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
   Reads from:
5-21-1757981266-507921405-1957994488-1003\Preferred
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons\SP_6A65DB879F95470886BD7EFE4977B10E.dat
                                             C:\Documents and Settings\Admin\Application
   Reads from:
Data\Microsoft\Windows\Themes\Custom.theme
                                              C:\Documents and Settings\Admin\Application
   Reads from:
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171.idx
                                             C:\Documents and Settings\Admin\Application
   Reads from:
Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c.idx
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-6.0.lap
                                             C:\Documents and Settings\Admin\Application
   Reads from:
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1.idx
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-6.0.lap
                                             C:\Documents and Settings\Admin\Application
   Reads from:
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d
   Reads from:
                                              C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d.idx
   Reads from:
                                              C:\Documents and Settings\Admin\Application
```

```
Data\Sun\Java\Deployment\cache\6.0\lastAccessed
                         C:\Documents and Settings\Admin\Application
 Reads from:
Data\Sun\Java\Deployment\deployment.properties
                         C:\Documents and Settings\Admin\Application
 Reads from:
Data\Sun\Java\Deployment\security\trusted.certs
 Reads from:
                         C:\Documents and Settings\Admin\Cookies\admin@c1.microsoft[2].txt
                         C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt
 Reads from:
                         C:\Documents and Settings\Admin\Cookies\admin@rto.microsoft[1].txt
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Cookies\admin@search.microsoft[1].txt
 Reads from:
                         C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt
 Reads from:
                         \label{lem:cokies-admin@www.microsoft[3].txt} C:\Documents\ and\ Settings\Admin\Cookies\admin@www.microsoft[3].txt
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Cookies\index.dat}\\
 Reads from:
                         C:\Documents and Settings\Admin\Favorites\Desktop.ini
                         {\tt C:\Documents\ and\ Settings\Admin\Favorites\Links\desktop.ini}
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url
 Reads from:
                         C:\Documents and Settings\Admin\Favorites\Links\Suggested Sites.url
                         C:\Documents and Settings\Admin\Favorites\Links\Web Slice Gallery.url
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE Add-on
site.url
 Reads from:
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE site on
Microsoft.com.url
 Reads from:
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Home.url
 Reads from:
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Work.url
 Reads from:
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
Store.url
 Reads from:
                         C:\Documents and Settings\Admin\Favorites\MSN.com.url
 Reads from:
                         C:\Documents and Settings\Admin\Favorites\Radio Station Guide.url
 Reads from:
                         C:\Documents and Settings\Admin\IECompatCache\index.dat
 Reads from:
                         C:\Documents and Settings\Admin\IETldCache\index.dat
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Reads from:
Data\Adobe\Acrobat\9.0\Cache\AcroFnt09.lst
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Reads from:
Data\Adobe\Acrobat\9.0\Updater\updater.log
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Adobe\Color\ACECache10.lst
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Adobe\Updater6\aum.log
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Adobe\Updater6\aumLib.log
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\GDIPFONTCACHEV1.DAT
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\IconCache.db
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Feeds\FeedsStore.feedsdb-ms
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Suggested Sites~.feed-ms
                         C:\Documents and Settings\Admin\Local Settings\Application
C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Feeds Cache\FBANKAIW\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\FBANKAIW\fwlink[1]
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\G4DZ1I7H\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\G4DZ1I7H\fwlink[1]
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\index.dat
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY1QNV\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY1QNV\fwlink[1]
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Feeds Cache\TLMHA51J\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\TLMHA51J\ieonline.microsoft[1]
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\brndlog.bak
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Internet Explorer\brndlog.txt
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Custom Settings\CustomO\install.ins
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
```

```
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK\www.microsoft[1].xml
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Internet Explorer\DOMStore\index.dat
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Internet Explorer\frameiconcache.dat
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Internet Explorer\Recovery\Active\{49831954-C276-11E3-AE24-08002733366F}.dat
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{80236AC0-AAD6-11E3-AE20-
08002733366F}.dat
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\rsoplog.bak
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\rsoplog.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Silverlight\mssl.lck
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML
                        {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Reads from:
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc.idx
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
{\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Reads from:
Data\Sun\Java\Deployment\cache\6.0\47\15572e2f-21932044.idx
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\7\2bbaaf87-5ca9d237
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\lastAccessed
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\desktop.ini
                        C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Reads from:
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\desktop.ini
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\History\History.IE5\index.dat
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014031220140313\index.dat
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\History\History.IE5\MSHist012014033120140407\index.dat
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\History\History.IE5\MSHist012014041220140413\index.dat
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Temp\296c0.msp
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Temp\AdobeARM.log
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\AdobeARM_NotLocked.log
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\ASPNETSetup_00000.log
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\ASPNETSetup_00001.log
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Temp\AUCHECK_PARSER.txt
 Reads from:
                        {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Compatibility\ Pack}
for the 2007 Office system (0).log
                        C:\Documents and Settings\Admin\Local Settings\Temp\dd_clwireg.txt
 Reads from:
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\dd_depcheck_NETFX_EXP_35.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local
{\tt Settings\Temp\dd\_dotnetfx35error.txt}
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\dd dotnetfx35install.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework20_Setup164F.txt
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\dd_NET_Framework30_Setup16AE.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework35_MSI16E2.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework35_MSI63E0.txt
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\dd_RGB9RAST_x86.msi601E.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA2A49.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA3565.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA35A0.txt
```

```
C:\Documents and Settings\Admin\Local Settings\Temp\dd_XPS.txt
 Reads from:
                         \label{local_continuous} C: \Documents \ and \ Settings \Admin\Local \ Settings \Temp\gen\_py\2.7 \dicts.dat
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\gen_py\2.7\__init__.py
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\JAUReg.log
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\java_install.log
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\java_install_reg.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\jusched.log
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft PowerPoint
Viewer (0).log
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Microsoft\ Visual\ C++}
2010 x86 Redistributable Setup_20131223_035827352-MSI_vc_red.msi.txt
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20131223_035827352.html
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_152314679-MSI_vc_red.msi.txt
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Microsoft\ Visual\ C++}
2010 x86 Redistributable Setup_20140312_152314679.html
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_152634747-MSI_vc_red.msi.txt
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_152634747.html
                         \hbox{C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft\ Visual\ C++}
 Reads from:
2010 x86 Redistributable Setup_20140312_154212618-MSI_vc_red.msi.txt
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_154212618.html
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\pywin32 postinstall.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\setup.log
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\SilverlightO.log
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\SilverlightMSI.log
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\uxeventlog.txt}
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\AntiPhishing\2CEDBFBC-DBA8-43AA-B1FD-CC8E6316E3E2.dat
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\CXCXW1MR\300lo[1].json
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\300lo[2].json
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\88666cc6-d578-45c8-baf0-89d3837f41c3_89[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\93e33485-fea3-4687-a642-2c5dd233522f_12[1].eot
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\CXCXW1MR\ADSAdClient31[1].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[2].txt
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[3].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\ADSAdClient31[4].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\ADSAdClient31[5].txt
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\adServer[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\auth016[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\bimapping[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\broker[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\CA9ATUDW.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\CAMLW29Z.isx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CATM568T.jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\CAVLZJ9D.jsx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\core114[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\core114[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\css[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\css[2].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\css[3].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\DataList[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\CXCXW1MR\e64030e7-ad8c-4be8-a45a-b69a2df3caef_13[1].eot
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\event[1].js
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[2].js
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[3].js
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[5].js
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\false[1].htm
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\General[1].css
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\General[1].js
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\georedirect[1].htm
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\georedirect[2].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\georedirect[3].htm
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\georedirect[4].htm
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\install[1].css
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\CXCXW1MR\js[2].ashx
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\LoginStatus[1].css
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\Nebula[1].js
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\CXCXW1MR\omnibase[2].css
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\oneMscomBlade[2].css
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\onemscomfooter[2].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\| Content.IE5 \verb|\| CXCXW1MR \verb|\| oneMscomJsCssLoader[3].js
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\request[1].php
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[1].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\| Content.IE5 \verb|\| CXCXW1MR \verb|\| ScriptResource[2].axd \\
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[3].axd
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[4].axd
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[5].axd
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\script[1].js
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\script[1].jsx
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\script[2].jsx
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\true[1].htm
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\true[2].htm
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\views[1]
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\WebResource[1].axd
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\wtid[1].js
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\wt_capi[2].js
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\desktop.ini
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\736e3781-6a19-4119-b717-e61f0d8982c0_12[1].eot
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\ADSAdClient31[1].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\ADSAdClient31[2].txt
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\auth016[1].js
```

```
Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\auth016[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\bing[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\broker-config_s1[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\broker-config_s1[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\broker-config_s1[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\CA39W67Q.jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\CAANG12B.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\CAU35S9Y.jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\ChangePassword[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\ClickToInstall[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\ClientBiSettings.Wol[1].js
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\ONWV4FIP\confirmation[1].aspx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\Content.IE5| ONWV4FIP \verb|\core114[1].js| \\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\counter017[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\counter017[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\css[1].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\css[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\css[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\details[1].htm
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\details[2].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\event[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\event[3].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\event[6].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\General[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\gl_social[1].svg
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\Install[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\js[1].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[2].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[3].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\js[4].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\Login[11.css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\modernizr.wol[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\Content.IE5|ONWV4FIP| nb-no[2].css|
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\ONWV4FIP\omniture_s_code[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\onemscomfooter[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\onemscomsearch[2].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\oneMscomSocial[2].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\PasswordRecovery[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\ScriptResource[1].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\ScriptResource[2].axd
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\ONWV4FIP\script[2].jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\SearchMSStoreClient[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\serverComponent[1].php
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\siteresource[1].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\siteresource[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\style[1].cssx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\Tracker[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\true[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\wol.common[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\wt_capi[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\08ce8e54-41ba-4695-9963-a7669022faec_12[1].eot
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\0XMN0BKF\15d2470f-0fcf-45e9-bf5b-c943236a61cf 27[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\300lo[1].json
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\67706439-4969-4bc3-9e3b-50770f40b20e_36[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\OXMNOBKF\ADSAdClient31[1].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\ADSAdClient31[2].txt
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\QXMNQBKF\auth016[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\broker-config_s1[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\broker-config_s1[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\broker-config_s1[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\broker-config_s2[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[1]
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\CA9P88JQ.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\Content.IE5| QXMNQBKF \verb|\core114[1].js|
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\counter017[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\counter017[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\css[1].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\css[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\css[2].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\css[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\DetailsView[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\event[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\event[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\feedback[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\FormView[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\GlobalResources[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\gl_site[1].svg
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\Import[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
```

Files\Content.IE5\QXMNQBKF\Install[1].css

```
Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\js[1].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\js[2].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\js[3].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\js[4].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\Menu[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\omnibase[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\oneMscomBlade[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\oneMscomComponents[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\oneMscomNav[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\onemscomsearch[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\oneMscomSocial[2].css
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\QXMNQBKF\ScriptResource[1].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\script[1].jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\script[2].jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\SilverlightAtlas-MSCOM-Tracking[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\Silverlight[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\styles[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\uninstall-arp-win[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\WebResource[1].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\welcome[1].htm
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\windows8_site_ltr[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\300lo[1].json
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\300lo[2].json
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ADSAdClient31[1].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\adServer[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\auth016[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\background_gradient[1]
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\UH4D6D6X\bimapping[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\broker-config[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\broker-config_s1[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\broker-config_s1[3].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[4].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\broker-config_s1[5].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\CA01EFSH.jsx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA7GG9IO.css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA8VUH6F.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\CAI7MNGV.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\CallingControl[1].aspx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\UH4D6D6X\confirmation[1].aspx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\confirmation[1].htm
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\Cookies[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\core114[1].js
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\UH4D6D6X\counter017[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CreateUserWizard[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\css[1].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\css[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\css[2].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\details-social[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\Content.IE5\UH4D6D6X\enable[2].htm|
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\UH4D6D6X\event[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\event[5].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\GridView[1].css
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\UH4D6D6X\info_48[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\InstallPageReskin[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\Install[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\internet-explorer-8-details[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\js[1].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\js[2].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\js[3].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\Marquee[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\mbox[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\MicrosoftAjax[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\ms[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\navcancl[2]
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\oneMscomComponents[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\oneMscomListLayout[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\oneMscomListLayout[3].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\oneMscomNav[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\pre_broker[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ScriptResource[1].axd
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ScriptResource[2].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\script[2].jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\serverComponent[1].php
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\silverlight[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\TreeView[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\webtrends[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\wt[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\desktop.ini
```

```
C:\Documents and Settings\Admin\My Documents\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\My Documents\My Music\Desktop.ini
                         C:\Documents and Settings\Admin\My Documents\My Music\Sample Music.lnk
 Reads from:
                         C:\Documents and Settings\Admin\My Documents\My Pictures\Desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\My Documents\My Pictures\Sample
Pictures.lnk
                         C:\Documents and Settings\Admin\ntuser.ini
 Reads from:
                         C:\Documents and Settings\Admin\PrivacIE\index.dat
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Recent\Desktop.ini
                         C:\Documents and Settings\Admin\Recent\fp_11.0.1.152_archive.lnk
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\SendTo\Compressed (zipped)
{\tt Folder.ZFS} end {\tt ToTarget}
 Reads from:
                         C:\Documents and Settings\Admin\SendTo\Desktop (create
shortcut).DeskLink
 Reads from:
                         C:\Documents and Settings\Admin\SendTo\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\SendTo\Mail Recipient.MAPIMail
                         C:\Documents and Settings\Admin\SendTo\My Documents.mydocs
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start
C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Address
Book.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Command
Prompt.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\desktop.ini
                         {\tt C:\Documents\ and\ Settings\Admin\Start}
 Reads from:
Menu\Programs\Accessories\Entertainment\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
                         C:\Documents and Settings\Admin\Start
 Reads from:
Menu\Programs\Accessories\Notepad.lnk
                         \verb|C:\Documents| and Settings\Admin\Start Menu\Programs\Accessories\Program| \\
 Reads from:
Compatibility Wizard.lnk
                         C:\Documents and Settings\Admin\Start
 Reads from:
Menu\Programs\Accessories\Synchronize.lnk
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\System
 Reads from:
Tools\Internet Explorer (No Add-ons).lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Tour
Windows XP.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Windows
Explorer.lnk
                         C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Internet
Explorer.lnk
                         C:\Documents and Settings\Admin\Start Menu\Programs\Outlook Express.lnk
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Remote
Assistance.lnk
                         C:\Documents and Settings\Admin\Start Menu\Programs\Startup\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Windows Media
 Reads from:
Player.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Templates\amipro.sam
 Reads from:
                         C:\Documents and Settings\Admin\Templates\lotus.wk4
                         {\tt C:\Documents\ and\ Settings\Admin\Templates\presenta.shw}
 Reads from:
                         C:\Documents and Settings\Admin\Templates\quattro.wb2
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Templates\wordpfct.wpd
 Reads from:
                         C:\Documents and Settings\Admin\Templates\wordpfct.wpg
                         C:\Documents and Settings\Administrator\Application Data\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Administrator\Application
Data\Microsoft\Internet Explorer\brndlog.bak
 Reads from:
                         C:\Documents and Settings\Administrator\Application
Data\Microsoft\Internet Explorer\brndlog.txt
                         C:\Documents and Settings\Administrator\Cookies\index.dat
 Reads from:
                         C:\Documents and Settings\Administrator\Local Settings\Application
 Reads from:
Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb
 Reads from:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat
 Reads from:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat.LOG
                         C:\Documents and Settings\Administrator\Local Settings\Application
 Reads from:
Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD
 Reads from:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML
 Reads from:
                         C:\Documents and Settings\Administrator\Local Settings\desktop.ini
 Reads from:
                         C:\Documents and Settings\Administrator\Local
```

```
Settings\History\desktop.ini
 Reads from:
                         C:\Documents and Settings\Administrator\Local
Settings\History\History.IE5\desktop.ini
                         C:\Documents and Settings\Administrator\Local
 Reads from:
Settings\History\History.IE5\index.dat
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Administrator\Local\ Settings\Temporary}
Internet Files\Content.IE5\CXCXW1MR\desktop.ini
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Reads from:
Internet Files\Content.IE5\desktop.ini
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Reads from:
Internet Files\Content.IE5\index.dat
 Reads from:
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\ONWV4FIP\desktop.ini
                         {\tt C:\Documents\ and\ Settings\backslash Administrator\backslash Local\ Settings\backslash Temporary}
 Reads from:
Internet Files\Content.IE5\QXMNQBKF\desktop.ini
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Reads from:
Internet Files\Content.IE5\UH4D6D6X\desktop.ini
 Reads from:
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\desktop.ini
 Reads from:
                         C:\Documents and Settings\Administrator\NTUSER.DAT
 Reads from:
                         C:\Documents and Settings\Administrator\NTUSER.DAT.LOG
 Reads from:
                         C:\Documents and Settings\Administrator\ntuser.ini
 Reads from:
                         C:\Documents and Settings\Administrator\SendTo\Compressed (zipped)
Folder.ZFSendToTarget
 Reads from:
                         C:\Documents and Settings\Administrator\SendTo\Desktop (create
shortcut).DeskLink
 Reads from:
                         C:\Documents and Settings\Administrator\SendTo\desktop.ini
 Reads from:
                         C:\Documents and Settings\Administrator\SendTo\Mail Recipient.MAPIMail
 Reads from:
                         C:\Documents and Settings\Administrator\Start Menu\desktop.ini
 Reads from:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Command Prompt.lnk
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\desktop.ini
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Entertainment\desktop.ini
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Notepad.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Program Compatibility Wizard.lnk
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Synchronize.lnk
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Tour Windows XP.lnk
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Windows Explorer.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini
 Reads from:
                         C:\Documents and Settings\Administrator\Start Menu\Programs\Remote
Assistance.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Startup\desktop.ini
                         C:\Documents and Settings\Administrator\Start Menu\Programs\Windows
 Reads from:
Media Player.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Templates\amipro.sam
 Reads from:
                         C:\Documents and Settings\Administrator\Templates\lotus.wk4
 Reads from:
                         C:\Documents and Settings\Administrator\Templates\presenta.shw
 Reads from:
                         C:\Documents and Settings\Administrator\Templates\quattro.wb2
 Reads from:
                         C:\Documents and Settings\Administrator\Templates\wordpfct.wpd
 Reads from:
                         C:\Documents and Settings\Administrator\Templates\wordpfct.wpg
 Reads from:
                         C:\Documents and Settings\All Users\Application
Data\Adobe\Acrobat\9.0\Replicate\Security\directories.acrodata
                         C:\Documents and Settings\All Users\Application
 Reads from:
Data\Adobe\Reader\9.4\ARM\AdbeRdrUpd951_all_incr.msp
                         C:\WINDOWS\Temp\tmp.exe
```

#### Network Events

Network Events		
Connects to:	127.0.0.1:1040	
Connects to:	113.255.164.198:80	
Connects to:	127.0.0.1:1043	
Connects to:	114.24.138.24:80	
Connects to:	127.0.0.1:1046	

Connects to:	212.8.43.26:80
Connects to: Connects to:	127.0.0.1:1049 91.219.62.29:80
Connects to:	127.0.0.1:1052
Connects to:	109.200.236.29:80
Connects to:	127.0.0.1:1055
Connects to:	2.143.35.31:80
Connects to:	127.0.0.1:1058
Connects to:	2.135.63.24:80
Connects to:	127.0.0.1:1061
Connects to:	83.213.85.32:80
Connects to:	127.0.0.1:1064
Connects to:	46.119.251.8:80
Connects to: Connects to:	127.0.0.1:1067 178.89.23.9:80
Connects to:	127.0.0.1:1070
Connects to:	93.79.238.9:80
Connects to:	127.0.0.1:1073
Connects to:	122.121.201.46:80
Connects to:	127.0.0.1:1076
Connects to:	194.27.111.48:80
Connects to:	127.0.0.1:1079
Connects to:	93.170.35.49:80
Connects to:	127.0.0.1:1082
Connects to:	113.255.17.46:80 127.0.0.1:1085
Connects to: Connects to:	127.0.0.1:1085
Connects to:	127.0.0.1:1088
Connects to:	93.79.131.49:80
Connects to:	127.0.0.1:1091
Connects to:	46.185.29.50:80
Connects to:	127.0.0.1:1094
Connects to:	89.38.112.51:80
Connects to:	127.0.0.1:1097
Connects to:	37.19.78.18:80
Connects to:	77.122.165.42:80
Sends data to:	127.0.0.1:1040
Sends data to: Sends data to:	113.255.164.198:80 127.0.0.1:1043
Sends data to:	114.24.138.24:80
Sends data to:	127.0.0.1:1046
Sends data to:	212.8.43.26:80
Sends data to:	127.0.0.1:1049
Sends data to:	91.219.62.29:80
Sends data to:	127.0.0.1:1052
Sends data to:	109.200.236.29:80
Sends data to:	127.0.0.1:1055
Sends data to:	2.143.35.31:80
Sends data to: Sends data to:	127.0.0.1:1058
Sends data to:	2.135.63.24:80 127.0.0.1:1061
Sends data to:	83.213.85.32:80
Sends data to:	127.0.0.1:1064
Sends data to:	46.119.251.8:80
Sends data to:	127.0.0.1:1067
Sends data to:	178.89.23.9:80
Sends data to:	127.0.0.1:1070
Sends data to:	93.79.238.9:80
Sends data to:	127.0.0.1:1073
Sends data to: Sends data to:	122.121.201.46:80 127.0.0.1:1076
Sends data to: Sends data to:	127.0.0.1:1076 194.27.111.48:80
Sends data to:	127.0.0.1:1079
Sends data to:	93.170.35.49:80
Sends data to:	127.0.0.1:1082
Sends data to:	113.255.17.46:80
Sends data to:	127.0.0.1:1085
Sends data to:	109.254.96.49:80
Sends data to:	127.0.0.1:1088
Sends data to:	93.79.131.49:80
Sends data to: Sends data to:	127.0.0.1:1091 46.185.29.50:80
Sends data to: Sends data to:	46.185.29.50:80 127.0.0.1:1094
Sends data to:	89.38.112.51:80
Sends data to:	127.0.0.1:1097
Sends data to:	37.19.78.18:80
Sends data to:	77.122.165.42:80
Receives data from:	127.0.0.1:1041
Receives data from:	113.255.164.198:80
Receives data from:	127.0.0.1:1044
Receives data from:	114.24.138.24:80
Receives data from: Receives data from:	127.0.0.1:1047 212.8.43.26:80
Receives data ITUIII,	212.0.73.20.00

Receives data from: 127.0.0.1:1050 Receives data from: 91.219.62.29:80 Receives data from: 127.0.0.1:1053 Receives data from: 109.200.236.29:80 Receives data from: 127.0.0.1:1056 Receives data from: 2.143.35.31:80 Receives data from: 127.0.0.1:1059 Receives data from: 2.135.63.24:80 Receives data from: 127.0.0.1:1062 Receives data from: 83.213.85.32:80 Receives data from: 127.0.0.1:1065 Receives data from: 46.119.251.8:80 Receives data from: 127.0.0.1:1068 Receives data from: 127.0.0.1:1071 Receives data from: 127.0.0.1:1074 Receives data from: 127.0.0.1:1077 Receives data from: 127.0.0.1:1080 Receives data from: 93.170.35.49:80 Receives data from: 127.0.0.1:1083 Receives data from: 127.0.0.1:1086 Receives data from: 109.254.96.49:80 Receives data from: 127.0.0.1:1089 93.79.131.49:80 Receives data from: Receives data from: 127.0.0.1:1092 Receives data from: 46.185.29.50:80 Receives data from: 127.0.0.1:1095 Receives data from: 127.0.0.1:1098

options\oleaut32.dll

Opens key: options\iertutil.dll

Opens key:

Windows Registry Events				
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings			
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters			
Creates key:	HKCU\software\microsoft\internet explorer\main			
Creates key:	HKLM\software\microsoft\windows\currentversion\run			
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\user shell			
folders				
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\shell folders</pre>			
Creates key:	HKLM\software\microsoft\windows\currentversion\explorer\user shell			
folders				
Creates key:	<pre>HKLM\software\microsoft\windows\currentversion\explorer\shell folders</pre>			
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\752d6fe81122349d	laf998a56f48e0b38.exe			
Opens key:	HKLM\system\currentcontrolset\control\terminal server			
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option			
Opens key:	<pre>HKLM\software\policies\microsoft\windows\safer\codeidentifiers</pre>			
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers			
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution			
options\msvcrt.dll	•			
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\advapi32.dll				
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\winlogon</pre>			
Opens key:	HKLM\			
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\diagnostics</pre>			
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\secur32.dll				
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\rpcrt4.dll				
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\wmdmps.dll				
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\user32.dll				
Opens key:	HKLM\system\currentcontrolset\control\session manager			
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\imm32.dll				
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\ntdll.dll				
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\kernel32.dll				
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\comcat.dll				
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\gdi32.dll				
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>			
options\shlwapi.dll				
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution			
options\normaliz.dll				
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution			
options\ole32.dll				
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution			

 $\label{thm:local_hammon} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\sc mage file execution} \\$ 

HKLM\software\microsoft\windows nt\currentversion\image file execution

```
options\urlmon.dll
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
                                        HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:
  Opens key:
                                        HKLM\system\currentcontrolset\control\error message instrument
  Opens key:
                                        \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre\_initialize
                                        HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\windows
                                        HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:
  Opens key:
                                        HKLM\software\microsoft\ole
  Opens key:
                                        HKCR\interface
  Opens key:
                                        HKCR\interface\{00020400-0000-0000-c000-00000000046}
                                        HKLM\software\microsoft\oleaut
  Opens key:
                                        HKLM\software\microsoft\oleaut\userera
  Opens key:
  Opens key:
                                        HKCU\software\policies\microsoft\control panel\desktop
  Opens kev:
  Opens key:
                                        HKCU\control panel\desktop
  Opens key:
Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:
                                        HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:
                                        HKCU\software\classes\
  Opens key:
                                        HKCU\software\classes\protocols\name-space handler\
  Opens key:
                                        HKCR\protocols\name-space handler
  Opens key:
                                        HKCU\software\classes\protocols\name-space handler
  Opens key:
                                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:
                                        HKLM\software\microsoft\windows\currentversion\internet settings
                                        HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings
  Opens key:
                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:
                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
                                       HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\
  Opens key:
                                        HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
                                        HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:
  Opens key:
                                        HKLM\software\microsoft\internet explorer\main\featurecontrol
  Opens key:
                                        HKCU\software\microsoft\internet explorer\main\featurecontrol
                                        HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
                                        HKLM\software\microsoft\internet
  Opens key:
explorer \verb|\main| featurecontrol| feature\_ignore\_policies\_zonemap\_if\_esc\_enabled\_kb918915
  Opens key:
                                        \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zonemap\domains\
                                        \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
  Opens key:
settings\zonemap\domains\
                                        HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\ranges\
  Opens key:
                                        \label{lem:hkcu} \verb+KCU\software\policies\microsoft\windows\currentversion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currenters
settings\zonemap\ranges\
                                        HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:
                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:
                                        HKLM\system\currentcontrolset\control\wmi\security
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
```

options\ws2\_32.dll

HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key:

options\dnsapi.dll

Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters HKLM\software\policies\microsoft\windows nt\dnsclient Opens key:

Opens key: HKLM\system\setup

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

 $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key:

options\iphlpapi.dll

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

Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces

Opens kev: HKLM\system\currentcontrolset\services\netbt\parameters

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\mswsock.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\psapi.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\shell32.dll

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9

Opens kev:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog 9 \setminus 00000004$ 

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries
Opens kev:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol\_catalog 9 \catalog\_entries \000000000010 \parameters \end{substitute} Opens \end{substitute} key:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000011
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000004

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:

options\hnetcfg.dll

Opens key: HKLM\software\microsoft\rpc\pagedbuffers

Opens key: HKLM\software\microsoft\rpc

Opens key:  ${\tt HKLM \setminus software \setminus microsoft \setminus windows\ nt \setminus current version \setminus image\ file\ execution}$ 

options\752d6fe81122349daf998a56f48e0b38.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\microsoft\rpc\securityservice

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wshtcpip.dll

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\access
Opens key: HKCU\software\adobe\acrobat reader\9.0\accessibility
Opens key: HKCU\software\adobe\acrobat reader\9.0\adobe\viewer
Opens key: HKCU\software\adobe\acrobat reader\9.0\annots

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\autosavedocs

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
                          HKCU\software\adobe\acrobat
 Opens kev:
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
                          HKCU\software\adobe\acrobat reader\9.0\formsprefs
 Opens key:
                          HKCU\software\adobe\acrobat reader\9.0\formsprefs\crequiredfieldhlcolor
 Opens key:
 Opens key:
                          HKCU\software\adobe\acrobat reader\9.0\formsprefs\cruntimebgidlecolor
 Opens key:
                          HKCU\software\adobe\acrobat reader\9.0\fullscreen
                          HKCU\software\adobe\acrobat reader\9.0\handtool
 Opens key:
 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\jsprefs
 Opens key:
                          HKCU\software\adobe\acrobat reader\9.0\language
 Opens kev:
                          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\optionalcontent
 Opens key:
                          HKCU\software\adobe\acrobat reader\9.0\originals
 Opens kev:
                          HKCU\software\adobe\acrobat reader\9.0\prefsdialog
 Opens key:
                          HKCU\software\adobe\acrobat reader\9.0\rememberedviews
 Opens key:
                          HKCU\software\adobe\acrobat reader\9.0\sdi
                          HKCU \ software \ adobe\ acrobat\ reader \ \ 9.0 \ selection
 Opens key:
 Opens key:
                          HKCU\software\adobe\acrobat reader\9.0\usagemeasurement
 Opens key:
                          HKCU\software\adobe\adobe acrobat
                          HKCU\software\adobe\adobe acrobat\9.0
 Opens key:
 Opens key:
                          HKCU\software\adobe\adobe acrobat\9.0\diskcabs
 Opens key:
                          HKCU\software\adobe\adobe arm
                          HKCU\software\adobe\adobe arm\1.0
 Opens key:
 Opens key:
                          HKCU\software\adobe\adobe arm\1.0\arm
 Opens key:
                          HKCU\software\adobe\adobe synchronizer
                          HKCU\software\adobe\adobe synchronizer\9.0
 Opens key:
                          \label{local-composition} \mbox{HKCU\software\adobe\adobe\ synchronizer\9.0\acrobat.com} \mbox{}
 Opens key:
 Opens key:
                          HKCU\software\adobe\commonfiles
 Opens key:
                          HKCU\software\adobe\commonfiles\usage
 Opens key:
                          HKCU\software\adobe\commonfiles\usage\demographic
 Opens key:
                          HKCU\software\adobe\commonfiles\usage\reader 9
                          HKCU\software\intel
 Opens key:
 Opens key:
                          HKCU\software\intel\indeo
                          HKCU\software\intel\indeo\4.1
 Opens kev:
 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\prefs
 Opens key:
                          HKCU\software\macromedia
 Opens kev:
                          HKCU\software\macromedia\flashplaver
 Opens key:
                          HKCU\software\macromedia\flashplayerupdate
```

Opens key: HKCU\software\microsoft

Opens key: HKCU\software\microsoft\active setup

Opens key: HKCU\software\microsoft\active setup\installed components

Opens key: HKCU\software\microsoft\active setup\installed components\<{12d0ed0d-

0ee0-4f90-8827-78cefb8f4988}

Opens key: HKCU\software\microsoft\active setup\installed components\>{26923b43-

4d38-484f-9b9e-de460746276c}

HKCU\software\microsoft\active setup\installed components\>{60b49e34-Opens key:

c7cc-11d0-8953-00a0c90347ff}

HKCU\software\microsoft\active setup\installed components\>{60b49e34-Opens key:

c7cc-11d0-8953-00a0c90347ff}micros

Opens key:

3dcf-431b-b061-f3f88e8be88a} HKCU\software\microsoft\active setup\installed components\{2179c5d3-Opens kev:

ebff-11cf-b6fd-00aa00b4e220}

HKCU\software\microsoft\active setup\installed components\{22d6f312-Opens key: b0f6-11d0-94ab-0080c74c7e95}

Opens key:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \active setup \slightly installed components \cite{Components} \cite{Comp$ 2b09-4501-b3f3-f3508c9228ed}

Opens key: HKCU\software\microsoft\active setup\installed components\{44bba840-

cc51-11cf-aafa-00aa00b6015c} Opens key:

cc51-11cf-aafa-00aa00b6015b}

Opens key: HKCU\software\microsoft\active setup\installed components\{44bba848cc51-11cf-aafa-00aa00b6015c}

Opens key: HKCU\software\microsoft\active setup\installed components\{4b218e3e-

bc98-4770-93d3-2731b9329278}

Opens key: HKCU\software\microsoft\active setup\installed components\{5945c046-

1e7d-11d1-bc44-00c04fd912be}

Opens key: HKCU\software\microsoft\active setup\installed components\{6bf52a52-

394a-11d3-b153-00c04f79faa6}

Opens key: HKCU\software\microsoft\active setup\installed components\{7790769c-

0471-11d2-af11-00c04fa35d02}

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:  $\label{lem:hamilton} HKCU\software\microsoft\active\ setup\installed\ components\{89b4c1cd-b018-4511-b0a1-5476dbf70820\}}$ 

Opens key: HKCU\software\microsoft\activemovie
Opens key: HKCU\software\microsoft\activemovie\devenum

Opens key: HKCU\software\microsoft\activemovie\devenum\{083863f1-70de-11d0-bd40-

00a0c911ce86}

Opens key: HKCU\software\microsoft\activemovie\devenum\{083863f1-70de-11d0-bd40-

00a0c911ce86}\{31345649-0000-0010-8000-00aa00389b71}

Opens key: HKCU\software\microsoft\activemovie\devenum\{083863f1-70de-11d0-bd40-

 $00a0c911ce86\} \setminus \{a2551f60-705f-11cf-a424-00aa003735be\}$ 

Opens key: HKCU\software\microsoft\advanced inf setup

Opens key: HKCU\software\microsoft\advanced inf setup\ie userdata nt

Opens key: HKCU\software\microsoft\advanced inf setup\ie userdata nt\regbackup
Opens key: HKCU\software\microsoft\advanced inf setup\ie userdata nt\regbackup\0

Opens key: HKCU\software\microsoft\advanced inf setup\ie userdata

nt\regbackup\0.map

Opens key: HKCU\software\microsoft\advanced inf setup\ie.hkcuzoneinfo

Opens key: HKCU\software\microsoft\advanced inf setup\ie.hkcuzoneinfo\regbackup
Opens key: HKCU\software\microsoft\advanced inf setup\ie.hkcuzoneinfo\regbackup\0

Opens key: HKCU\software\microsoft\advanced inf

setup\ie.hkcuzoneinfo\regbackup\0.map

Opens key: HKCU\software\microsoft\advanced inf setup\ie40.useragent

Opens key: HKCU\software\microsoft\advanced inf setup\ie40.useragent\regbackup Opens key: HKCU\software\microsoft\advanced inf setup\ie40.useragent\regbackup\0

Opens key: HKCU\software\microsoft\advanced inf

setup\ie40.useragent\regbackup\0.map

Opens key: HKCU\software\microsoft\advanced inf setup\iehomepageinfo

Opens key: HKCU\software\microsoft\advanced inf setup\iehomepageinfo\regbackup
Opens key: HKCU\software\microsoft\advanced inf setup\iehomepageinfo\regbackup\0

Opens key: HKCU\software\microsoft\advanced inf

setup\iehomepageinfo\regbackup\0.map

Opens key: HKCU\software\microsoft\clock

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\compartment

 $Opens~key: \\ HKCU \setminus software \setminus t(544d6a63-e2e8-4752-bbd1-e2e8-47$ 

000960bca083}

Opens key: HKCU\software\microsoft\ctf\langbar
Opens key: HKCU\software\microsoft\ctf\msutb
Opens key: HKCU\software\microsoft\ctf\sapilayr
Opens key: HKCU\software\microsoft\ctf\tip

 $Opens \ key: \\ HKCU \ software \ microsoft \ ctf \ tip \ \{dcbd6fa8-032f-11d3-b5b1-00c04fc324a1\}$ 

Opens key: HKCU\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-

00c04fc324a1}\languageprofile

Opens key: HKCU\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-

00c04fc324a1}\languageprofile\0x00000409

Opens key: HKCU\software\microsoft\direct3d

Opens key:  ${\tt HKCU \setminus software \setminus microsoft \setminus direct 3d \setminus most recent application}$ 

Opens key: HKCU\software\microsoft\eventsystem

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

00805fc79216}

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

00805fc79216}\subscriptions

Opens key: HKCU\software\microsoft\feeds
Opens key: HKCU\software\microsoft\file manager

Opens key: HKCU\software\microsoft\file manager\settings

Opens key: HKCU\software\microsoft\ftp
Opens key: HKCU\software\microsoft\gdiplus
Opens key: HKCU\software\microsoft\ieak

Opens key:  ${\sf HKCU \backslash software \backslash microsoft \backslash ieak \backslash grouppolicy}$ 

Opens key: HKCU\software\microsoft\imemip

Opens key: HKCU\software\microsoft\imemip\0x0409

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\caretbrowsing

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

Opens key: HKCU\software\microsoft\internet explorer\desktop\components
Opens key: HKCU\software\microsoft\internet explorer\desktop\components\0
Opens key: HKCU\software\microsoft\internet explorer\desktop\general
Opens key: HKCU\software\microsoft\internet explorer\desktop\old workareas
Opens key: HKCU\software\microsoft\internet explorer\desktop\safemode
Opens key: HKCU\software\microsoft\internet explorer\desktop\safemode
HKCU\software\microsoft\internet explorer\desktop\safemode\general

Opens key: HKCU\software\microsoft\internet explorer\desktop\scheme
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:  $\label{lem:hkcusoftwaremicrosoft} \mbox{hkcusoftwaremicrosoft} \mbox{internet explorer} \mbox{download}$ 

```
HKCU\software\microsoft\internet explorer\extensions
   Opens key:
                                              HKCU\software\microsoft\internet explorer\extensions\cmdmapping
   Opens key:
                                              HKCU\software\microsoft\internet explorer\help_menu_urls
   Opens kev:
   Opens key:
                                              HKCU\software\microsoft\internet explorer\ietld
   Opens kev:
                                              HKCU\software\microsoft\internet explorer\ietld\lowmic
   Opens key:
                                              \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ internet\ explorer\+ information bar
                                              HKCU\software\microsoft\internet explorer\international
   Opens key:
                                              HKCU\software\microsoft\internet explorer\international\scripts
   Opens key:
   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 \setminus software \setminus microsoft \setminus internet \ explorer \setminus international \setminus scripts \setminus 13
   Opens key:
                                              HKCU\software\microsoft\internet explorer\international\scripts\14
                                              HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus international \setminus scripts \setminus 15
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\internet explorer\international\scripts\16
                                              HKCU\software\microsoft\internet explorer\international\scripts\17
   Opens key:
   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
                                              HKCU\software\microsoft\internet explorer\international\scripts\23
   Opens key:
                                              HKCU\software\microsoft\internet explorer\international\scripts\24
   Opens kev:
   Opens key:
                                              HKCU\software\microsoft\internet explorer\international\scripts\25
   Opens key:
                                              HKCU\software\microsoft\internet explorer\international\scripts\26
                                              \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc internet explorer\international\sc ripts\27} \\
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\internet explorer\international\scripts\28
   Opens key:
                                              HKCU\software\microsoft\internet explorer\international\scripts\29
                                              Opens kev:
   Opens key:
                                              HKCU\software\microsoft\internet explorer\international\scripts\30
   Opens key:
                                              HKCU\software\microsoft\internet explorer\international\scripts\34
   Opens key:
                                              HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus international \setminus scripts \setminus 35
   Opens key:
                                              Opens key:
                                              HKCU\software\microsoft\internet explorer\international\scripts\38
                                              \label{thm:hkcu} \mbox{HKCU\software\mbox{\sc internet explorer\international\sc ipts\sc 39}} \label{thm:hkcu}
   Opens key:
   Opens key:
                                              \label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| internet explorer expl
   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
                                              \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\international\sc ripts\9} \\
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\internet explorer\internetregistry
   Opens key:
                                              HKCU\software\microsoft\internet explorer\linksbar
                                              HKCU\software\microsoft\internet explorer\linksbar\itemcache
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\internet explorer\linksbar\itemcache\0
   Opens key:
                                              HKCU\software\microsoft\internet explorer\linksbar\itemcache\1
                                              HKCU\software\microsoft\internet explorer\lowregistry
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\internet explorer\lowregistry\domstorage
   Opens key:
                                              HKCU\software\microsoft\internet explorer\lowregistry\domstorage\total
                                              HKCU\software\microsoft\internet explorer\lowregistry\extensions
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\internet
explorer\lowregistry\extensions\cmdmapping
                                              HKCU\software\microsoft\internet explorer\main
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\internet explorer\main\default feeds
   Opens key:
                                              HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus internet \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \setminus microsoft \ explorer \setminus main \setminus default \ feeds \setminus \{292f3d25-microsoft \ explorer \setminus microsoft \ explorer \ explorer \setminus microsoft \ explorer \ 
c7e7-48ac-bfba-7b9c1f5b42a7}
                                              HKCU\software\microsoft\internet explorer\main\default feeds\{8dd206d8-
   Opens key:
e6a9-4797-bfe9-b6a7783eb157}
                                              HKCU\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_localmachine_lockdown
   Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown\settings
   Opens key:
                                              \label{lem:hkcu} \verb+KKCU\+ software\+ internet explorer\+ main\+ windows search
   Opens key:
                                              HKCU\software\microsoft\internet explorer\new windows
   Opens key:
                                              HKCU\software\microsoft\internet explorer\new windows\allow
   Opens key:
                                              HKCU\software\microsoft\internet explorer\phishingfilter
   Opens key:
                                              HKCU\software\microsoft\internet explorer\privacy
                                              \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ internet\ explorer\+ recovery
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\internet explorer\recovery\active
   Opens key:
                                              HKCU\software\microsoft\internet explorer\searchscopes
                                              Opens key:
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\security\p3global
   Opens key:
                                              HKCU\software\microsoft\internet explorer\security\p3sites
   Opens key:
                                              HKCU\software\microsoft\internet explorer\services
   Opens key:
                                              HKCU\software\microsoft\internet explorer\settings
                                              HKCU\software\microsoft\internet explorer\sqm
   Opens kev:
   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\explorer
     Opens key:
                                                                       HKCU\software\microsoft\internet explorer\toolbar\shellbrowser
                                                                       HKCU\software\microsoft\internet explorer\toolbar\webbrowser
     Opens key:
     Opens key:
                                                                       HKCU\software\microsoft\internet explorer\typedurls
     Opens key:
                                                                       HKCU\software\microsoft\internet explorer\urlsearchhooks
                                                                       HKCU\software\microsoft\internet explorer\user preferences
     Opens key:
     Opens key:
                                                                       HKCU\software\microsoft\internet explorer\zoom
     Opens key:
                                                                       HKCU\software\microsoft\java vm
     Opens key:
                                                                       HKCU\software\microsoft\keyboard
     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\battery
     Opens key:
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets
                                                                       \label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \mediap layer \battery \presets \bright sphere \end{tabular}
     Opens kev:
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\brightsphere\currentshiftinfo
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\brightsphere\preshiftinfo
     Opens key:
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\circledance
     Opens kev:
HKCU\software\microsoft\mediaplayer\battery\presets\circledance\currentshiftinfo
    Opens key:
\label{lem:hkcu} \begin{tabular}{l} HKCU \software \microsoft \mediaplayer \battery \presets \circled ance \postshift in for the limit of the latest substitution of the latest subst
HKCU\software\microsoft\mediaplayer\battery\presets\circledance\preshiftinfo
     Opens key:
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\cominatya
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\cominatya\currentshiftinfo
     Opens key:
HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ cominaty a \ preshift in fooling \ mediaplayer \ battery \ presets \ cominaty \ and \ preshift in fooling \ preshift \ presets \ preshift \ presets \ preshift \ pres
                                                                       HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ cotton star
     Opens key:
     Opens key:
\label{thm:linear} \verb+KCU \+ software \+ microsoft \+ mediaplayer \+ battery \+ presets \+ cotton star \+ current shift info
    Opens kev:
\label{lem:hkcu} \verb+KKCU \software \microsoft \mediaplayer \mbox{\verb+battery \presets \cottonstar \preshiftinfo}
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\dandelionaid
     Opens key:
     Opens key:
HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ dandelionaid \ currents hiftinfo
     Opens key:
\label{thm:linear} HKCU \software \microsoft \mediaplayer \battery \presets \dandelion aid \postshift in formula and \mediaplayer \presets \presets \mediaplayer \presets \prese
    Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\dandelionaid\preshiftinfo
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\drowningflower
     Opens key:
     Opens key:
HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ drowning flower \ currents hiftinfollower \ microsoft \ mediaplayer \ battery \ presets \ drowning flower \ currents \ hiftinfollower \ microsoft \ mediaplayer \ battery \ presets \ drowning flower \ currents \ hiftinfollower \ microsoft \ mediaplayer \ battery \ presets \ drowning flower \ currents \ hiftinfollower \ microsoft \ mediaplayer \ battery \ presets \ drowning flower \ microsoft \ mediaplayer \ hiftinfollower \ mediaplayer \ hiftinfollower \ microsoft \ mediaplayer \ hiftinfollower \ hif
    Opens kev:
Opens kev:
HKCU\software\microsoft\mediaplayer\battery\presets\drowningflower\preshiftinfo
     Opens key:
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\eletriarnation
     Opens key:
HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ eletriar nation \ currents \ hiftinfo
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\eletriarnation\postshiftinfo
    Opens kev:
HKCU \ software \ \ icrosoft \ \ mediaplayer \ \ battery \ \ presets \ \ eletriar nation \ \ \ preshiftin fo
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\eventhorizon
     Opens key:
     Opens key:
HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ eventhorizon \ currents \ hiftinfo
     Opens key:
HKCU\software\microsoft\mediaplayer\batterv\presets\eventhorizon\postshiftinfo
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\eventhorizon\preshiftinfo
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick ascii
     Opens key:
    Opens key:
                                                                       ascii\currentshiftinfo
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick
    Opens kev:
ascii\postshiftinfo
    Opens key:
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick
ascii\preshiftinfo
     Opens key:
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\gemstone matrix
     Opens key:
                                                                       \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ mediaplayer\+ battery\+ presets\+ gemstone
matrix\currentshiftinfo
    Opens key:
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\gemstone
matrix\preshiftinfo
                                                                       HKCU\software\microsoft\mediaplayer\battery\presets\grooveswirl
    Opens kev:
     Opens key:
Opens key:
```

Opens key:  $HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ grooves wirl \ preshift in formula and the sum of the s$ Opens kev: HKCU\software\microsoft\mediaplayer\battery\presets\illuminator Opens key:  $HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ illuminator \ currents \ hiftinfo$ Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\illuminator\postshiftinfo Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\illuminator\preshiftinfo Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\iseethetruth Opens kev:  $HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ is eethet ruth \ currents hiftinfo$ Opens key:  $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \mediap layer \battery \presets \see the truth \preshift info$ Opens key: Opens key:

HKCU\software\microsoft\mediaplayer\battery\presets\kaleidoscope

 $HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ kale idoscope \ currents hiftinfo$ 

Opens key:

HKCU\software\microsoft\mediaplayer\battery\presets\kaleidoscope\postshiftinfo

Opens key:

HKCU\software\microsoft\mediaplayer\battery\presets\kaleidoscope\preshiftinfo

Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\khemicalnova

Opens kev:

 $HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus khemical nova \setminus currents hiftinfo$ 

Opens key:

HKCU\software\microsoft\mediaplayer\battery\presets\khemicalnova\preshiftinfo

Opens kev: HKCU\software\microsoft\mediaplayer\battery\presets\lotus

Opens key:

HKCU\software\microsoft\mediaplayer\battery\presets\lotus\currentshiftinfo

HKCU\software\microsoft\mediaplayer\battery\presets\lotus\postshiftinfo Opens key: Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\lotus\preshiftinfo Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\nerds are cool  $\label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \mbox{$\mbox{microsoft} \mbox{$\mbox{mediaplayer} \mbox{$\mbox{$\mbox{$hot$} $}$} are \end{tabular}$ Opens key:

cool\currentshiftinfo

Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\nerds are

cool\postshiftinfo

HKCU\software\microsoft\mediaplayer\battery\presets\nerds are Opens key:

cool\preshiftinfo

Opens key:  $HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus relatively calm = microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus mediaplayer \setminus battery \setminus mediaplayer \setminus$ 

Opens key:

HKCU\software\microsoft\mediaplayer\battery\presets\relativelycalm\currentshiftinfo Opens key:

 $HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ relatively calm \ postshift infonce \ microsoft \ mediaplayer \ battery \ presets \ relatively \ calm \ postshift \ infonce \ presets \ relatively \ calm \ postshift \ infonce \ presets \ relatively \ calm \ postshift \ infonce \ presets \ relatively \ presets \ relatively \ presets \ relatively \ presets \ p$ 

Opens key:

 $HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ relatively calm \ preshift info$ 

 $\label{lem:hkcu} \verb+KCU \software \microsoft \mediaplayer \mbox{} battery \mbox{} presets \mbox{} \mbox{} sleepy spray \mbox{} and \mbox{} battery \mbox{} \mbox{} presets \mbox{} \m$ Opens key:

Opens key:

HKCU\software\microsoft\mediaplayer\battery\presets\sleepyspray\currentshiftinfo

Opens kev:

Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\smoke or water HKCU\software\microsoft\mediaplayer\battery\presets\smoke or Opens key:

water\currentshiftinfo

Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\smoke or

water\preshiftinfo

HKCU\software\microsoft\mediaplayer\battery\presets\spiderslastmoment Opens kev: Opens kev:

Opens key:

 $\label{lem:hccu} \begin{tabular}{l} HKCU \software \microsoft \mediaplayer \battery \presets \spiders \mbox{last moment \postshift info} \end{tabular}$  $\label{lem:hkcu} \begin{tabular}{l} HKCU \software \microsoft \mediap layer \battery \presets \strawberry aid \end{tabular}$ 

Opens key: Opens kev:

 $HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ strawberry aid \ currents hiftinfollowed by the software \ microsoft \ mediaplayer \ battery \ presets \ strawberry \ aid \ currents \ hiftinfollowed by the software \ microsoft \ mediaplayer \ battery \ presets \ strawberry \ aid \ currents \ hiftinfollowed \ battery \$ 

Opens kev:

Opens key:

 $\label{thm:linear} HKCU \ software \ \ icrosoft \ \ \ battery \ \ \ strawberry aid \ \ preshift in fo$ 

Opens kev: HKCU\software\microsoft\mediaplayer\batterv\presets\the world Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\the

world\currentshiftinfo

Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\the

world\preshiftinfo

Opens key:  $HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus tornado$ 

Opens kev:

 $HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ tornado \ currents hiftinfo$ Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\tornado\preshiftinfo Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\what is an egab Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\what is an

egab\currentshiftinfo

Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\what is an

egab\postshiftinfo

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\skins Opens key: HKCU\software\microsoft\mediaplayer\player\tasks Opens key: HKCU\software\microsoft\mediaplayer\player\tasks\nowplaying Opens key: HKCU\software\microsoft\mediaplayer\preferences HKCU\software\microsoft\mediaplayer\preferences\proxysettings Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http Opens key: Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms 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\messengerservice HKCU\software\microsoft\microsoft management console Opens key: Opens key: HKCU\software\microsoft\microsoft management console\recent file list Opens key: HKCU\software\microsoft\microsoft management console\settings Opens key: HKCU\software\microsoft\ms design tools Opens key: HKCU\software\microsoft\ms design tools\mdtdbd HKCU\software\microsoft\msdaipp Opens key: Opens key: HKCU\software\microsoft\msdaipp\providers Opens key: HKCU\software\microsoft\msdaipp\providers\{9fecd570-b9d4-11d1-9c78-0000f875ac61} HKCU\software\microsoft\msdaipp\providers\{9fecd571-b9d4-11d1-9c78-Opens key: 0000f875ac61} HKCU\software\microsoft\multimedia Opens key: Opens key: HKCU\software\microsoft\multimedia\audio HKCU\software\microsoft\multimedia\audio\waveformats Opens key: HKCU\software\microsoft\multimedia\audio compression manager Opens key: Opens key: HKCU\software\microsoft\multimedia\audio compression manager\msacm Opens key: HKCU\software\microsoft\multimedia\audio compression manager\priority v4.00 Opens key: HKCU\software\microsoft\narrator Opens key: HKCU\software\microsoft\netdde Opens key: HKCU\software\microsoft\netdde\dde trusted shares Opens key: HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a Opens key: HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a\chat\$ HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a\clpbk\$ Opens key: Opens key:  $HKCU \setminus software \setminus microsoft \setminus trusted shares \setminus d06176d5a \setminus d06176d5a \setminus trusted shares \setminus d06176d5a \setminus d06176d6a \setminus d06176$ Opens key: HKCU\software\microsoft\netshow Opens key: HKCU\software\microsoft\netshow\player Opens key: HKCU\software\microsoft\netshow\player\remote Opens key: HKCU\software\microsoft\notepad HKCU\software\microsoft\ntbackup Opens key: Opens key: HKCU\software\microsoft\office Opens key: HKCU\software\microsoft\office\11.0 HKCU\software\microsoft\office\11.0\common Opens key: Opens key: HKCU\software\microsoft\office\11.0\common\drawalerts Opens key: HKCU\software\microsoft\office\11.0\common\drawalerts\ftp sites  $HKCU \setminus software \setminus microsoft \setminus office \setminus 11.0 \setminus common \setminus dspadapter mru$ Opens key: Opens key: HKCU\software\microsoft\office\11.0\common\general Opens key: HKCU\software\microsoft\office\11.0\common\languageresources HKCU\software\microsoft\office\11.0\common\migration Opens key: Opens key:  $HKCU \ software \ microsoft \ office \ 11.0 \ common \ migration \ office$ Opens key: HKCU\software\microsoft\office\11.0\common\migration\word  $HKCU\software\microsoft\office\11.0\common\open$  find Opens key: Opens key: HKCU\software\microsoft\office\11.0\common\open find\microsoft office word HKCU\software\microsoft\office\11.0\common\open find\places Opens key: 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 HKCU\software\microsoft\office\11.0\word\wizards Opens key: Opens key: HKCU\software\microsoft\office\11.0\wordview Opens key: HKCU\software\microsoft\office\11.0\wordview\data HKCU\software\microsoft\office\12.0 Opens key: Opens key: HKCU\software\microsoft\office\12.0\common Opens key: HKCU\software\microsoft\office\12.0\common\drawalerts  $\label{lem:hkcu} HKCU \software \microsoft \softice \noindent \n$ Opens key: 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\languageresources\enabledlanguages

Opens key: HKCU\software\microsoft\office\12.0\common\migration

Opens key: HKCU\software\microsoft\office\12.0\common\migration\office

Opens key: HKCU\software\microsoft\office\12.0\common\migration\office

Opens key: HKCU\software\microsoft\office\12.0\common\open find

 $Opens~key: \\ HKCU \ Software \ microsoft \ office \ 12.0 \ common \ open~find \ microsoft~office \ not the limit of the$ 

```
excel viewer
                                                                           HKCU\software\microsoft\office\12.0\common\open find\places
    Opens key:
                                                                           HKCU\software\microsoft\office\12.0\common\research
    Opens key:
                                                                           HKCU\software\microsoft\office\12.0\common\research\translation
    Opens key:
    Opens key:
                                                                           HKCU\software\microsoft\office\12.0\excel
    Opens key:
                                                                           HKCU \ software \ `microsoft \ office \ '12.0 \ excel \ 'options' \\
                                                                           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:
    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
                                                                           HKCU\software\microsoft\office\14.0\common
    Opens key:
                                                                           HKCU \setminus software \setminus microsoft \setminus office \setminus 14.0 \setminus common \setminus drawalerts
    Opens key:
                                                                           HKCU\software\microsoft\office\14.0\common\drawalerts\ftp sites
    Opens key:
    Opens key:
                                                                           HKCU\software\microsoft\office\14.0\common\general
    Opens key:
                                                                           HKCU\software\microsoft\office\14.0\common\languageresources
    Opens key:
HKCU\software\microsoft\office\14.0\common\languageresources\enabledlanguages
    Opens key:
                                                                           HKCU\software\microsoft\office\14.0\common\open find
                                                                           HKCU\software\microsoft\office\14.0\common\open find\microsoft
    Opens key:
powerpoint viewer
    Opens key:
                                                                           HKCU\software\microsoft\office\14.0\common\open find\places
    Opens key:
                                                                           HKCU\software\microsoft\office\14.0\common\research
                                                                           HKCU\software\microsoft\office\14.0\common\research\translation
    Opens key:
    Opens key:
                                                                           HKCU\software\microsoft\office\14.0\powerpoint
                                                                           HKCU\software\microsoft\office\14.0\powerpoint viewer
    Opens key:
    Opens key:
                                                                           Opens key:
                                                                           HKCU\software\microsoft\office\common
    Opens key:
                                                                           HKCU\software\microsoft\office\common\smart tag
    Opens key:
                                                                           HKCU\software\microsoft\office\common\smart tag\actions
    Opens key:
                                                                           455d-a40b-c95f1f91ff8a}
                                                                           HKCU\software\microsoft\office\common\smart tag\actions\{49df3409-46b3-
    Opens key:
4b0c-b7bf-fec0f9401edd}
    Opens key:
                                                                           HKCU\software\microsoft\office\common\smart tag\actions\{64ab6c69-b40e-
40af-9b7f-f5687b48e2b6}
                                                                           HKCU \setminus software \setminus microsoft \setminus office \setminus common \setminus smart tag \setminus actions \setminus \{c3754d1a - 04d3 - 04
    Opens key:
4085-8cfb-97705b57a98f}
                                                                           HKCU \setminus software \setminus microsoft \setminus office \setminus common \setminus smart \ tag \setminus actions \setminus \{f114ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-
    Opens key:
4238-92c9-bbe330af25fd}
                                                                           HKCU\software\microsoft\office\common\smart tag\recognizers
    Opens kev:
                                                                           HKCU \setminus software \setminus microsoft \setminus office \setminus common \setminus smart \ tag \setminus recognizers \setminus \{64ab6c69-tag \setminus recognizers \setminus \{64ab6c60\} \setminus \{64ab6c60\} \setminus \{64ab6c60\} \setminus \{64ab6c60\} \setminus \{64ab6c60\} \setminus \{64ab60\} \setminus \{64ab60\} \setminus \{64ab60\} \setminus \{64ab60\} \setminus
    Opens key:
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
                                                                           HKCU\software\microsoft\outlook express
    Opens kev:
                                                                           \label{local-hammons} \mbox{HKCU\software\mbox{\sc microsoft\outlook} express\sc .0}
    Opens key:
    Opens key:
                                                                           HKCU\software\microsoft\outlook express\5.0\shared settings
    Opens key:
                                                                           HKCU\software\microsoft\outlook express\5.0\shared settings\setup
    Opens key:
                                                                           HKCU\software\microsoft\plus!
    Opens key:
                                                                           HKCU\software\microsoft\plus!\themes
    Opens kev:
                                                                           HKCU\software\microsoft\plus!\themes\apply
                                                                           HKCU\software\microsoft\plus!\themes\current
    Opens key:
    Opens key:
                                                                           HKCU\software\microsoft\protected storage system provider
    Opens key:
                                                                           HKCU\software\microsoft\protected storage system provider\s-1-5-21-
1757981266-507921405-1957994488-1003
    Opens key:
                                                                           HKCU\software\microsoft\ras phonebook
    Opens key:
                                                                           HKCU\software\microsoft\regedt32
    Opens key:
                                                                           HKCU\software\microsoft\regedt32\settings
    Opens key:
                                                                           HKCU\software\microsoft\sapi layer
    Opens key:
                                                                           HKCU\software\microsoft\schedule+
                                                                           HKCU\software\microsoft\schedule+\microsoft schedule+
    Opens key:
    Opens key:
                                                                           HKCU\software\microsoft\search assistant
    Opens key:
                                                                           HKCU\software\microsoft\security center
                                                                           HKCU\software\microsoft\shared
    Opens key:
    Opens key:
                                                                           HKCU\software\microsoft\shared tools
    Opens key:
                                                                           HKCU\software\microsoft\shared tools\font mapping
                                                                           HKCU\software\microsoft\shared tools\proofing tools
    Opens key:
    Opens key:
                                                                           HKCU\software\microsoft\shared tools\proofing tools\custom dictionaries
    Opens key:
                                                                           HKCU\software\microsoft\speech
                                                                           {\tt HKCU \ } software \verb|\ microsoft \> speech \> applexicons
    Opens key:
    Opens key:
                                                                           HKCU\software\microsoft\speech\audiooutput
    Opens key:
                                                                           HKCU\software\microsoft\speech\currentuserlexicon
                                                                           \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ speech\+ current user lexicon\+ applexicons
    Opens key:
    Opens key:
                                                                           85d6-72e5eeb6995a}
                                                                           HKCU \setminus software \setminus microsoft \setminus speech \setminus current user \\ lexicon \setminus \{c9e37c15 - df92 - 4727 - df92 - d
    Opens key:
85d6-72e5eeb6995a}\files
    Opens key:
                                                                           HKCU\software\microsoft\speech\phoneconverters
    Opens key:
                                                                           HKCU\software\microsoft\speech\voices
```

```
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:
                                                               \label{lem:hkcu} \verb+KKCU \software \microsoft \systemcertificates \ca\ctls
    Opens key:
                                                               HKCU\software\microsoft\systemcertificates\disallowed
                                                               \label{thm:condition} \begin{tabular}{ll} HKCU \software \mbox{$^{\circ}$} is allowed \certificates \end{tabular}
    Opens key:
    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:
                                                               {\it HKCU} \ software \ `microsoft \ 'system certificates \ '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\trust
    Opens key:
                                                               HKCU\software\microsoft\systemcertificates\trust\certificates
    Opens key:
                                                               HKCU\software\microsoft\systemcertificates\trust\crls
    Opens key:
                                                               \label{lem:hkcu} \verb+KKCU \software \microsoft \system certificates \trust \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\visualstudio
                                                               HKCU\software\microsoft\visualstudio\9.0
    Opens key:
    Opens key:
                                                               HKCU\software\microsoft\visualstudio\9.0\downloadmanager
    Opens key:
                                                               HKCU\software\microsoft\wbem
                                                               HKCU\software\microsoft\wbem\wmic
    Opens kev:
    Opens key:
                                                               HKCU\software\microsoft\windows
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion
                                                               HKCU\software\microsoft\windows\currentversion\app management
    Opens key:
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\applets
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\applets\regedit
                                                               \label{thm:local_hammon} \parbox{$HKCU\software\microsoft\windows\currentversion\applets\systray} \\
    Opens key:
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\applets\tour
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\controls folder
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\explorer
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\bitbucket
    Opens key:
                                                               \label{lem:hkcu} \verb+KKCU\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\clsid
    Opens key:
                                                               HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus 
ad25-11d0-98a8-0800361b1103}
    Opens key:
                                                               HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (645ff 040-1) + (645ff 
5081-101b-9f08-00aa002f954e}
                                                               \label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\clsid| \{871c5380-microsoft| windows \verb|\currentversion| explorer \verb|\clsid| (871c5380-microsoft| windows \verb|\currentversion| explorer windows window
    Opens key:
42a0-1069-a2ea-08002b30309d}
                                                               HKCU\software\microsoft\windows\currentversion\explorer\comdlg32
    Opens key:
    Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\lastvisitedmru
   Opens kev:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \comdlg 32 \open savemru \end{tabular}
                                                               HKCU\software\microsoft\windows\currentversion\explorer\desktop
    Opens kev:
    Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\cleanupwiz
    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\.aif
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.aifc
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.aiff
    Opens key:
Opens key:
                                                               \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\..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\.css
    Opens key:
                                                               \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.dib}
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.doc
                                                               \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \explorer \fileexts \cdots. docm
    Opens key:
    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-ms
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.egg-
info
```

HKCU\software\microsoft\sqmclient

Opens key:

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.emf

```
Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm
    Opens kev:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ico
    Opens key:
    Opens kev:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ivf
    Opens key:
                                                              \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\fiff+ in the property of the property of
    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\.m1v
    Opens key:
                                                              HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus file exts \setminus .m3u
    Opens key:
                                                              \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\..mid+ \\
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.midi
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp2
    Opens key:
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp2v
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp3
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpa
    Opens kev:
    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
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.msi
    Opens kev:
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.png
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.pot
    Opens key:
                                                              \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \explorer \fileexts \cdots. potmulation \cdots \
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.potx
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ppsm
    Opens kev:
                                                              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\.rmi
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.rtf
    Opens key:
                                                              \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.snd}
    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\.txt
    Opens key:
                                                              \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc urrentversion\explorer\fileexts\sc .wav} \\
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wax
    Opens key:
                                                              \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\..wdp+
    Opens key:
                                                              \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \file exts \colongraph. \end{tabular} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \file exts \colongraph. \end{tabular} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \file \colongraph. \end{tabular} \begin{tabular}{ll} HKCU \software \microsoft \windows \current \colongraph. \end{tabular} \begin{tabular}{ll} HKCU \software \microsoft \windows \current \colongraph. \end{tabular} \begin{tabular}{ll} HKCU \software \microsoft \windows \current \colongraph. \end{tabular} \begin{tabular}{ll} HKCU \software \microsoft \colongraph. \end{tabular} \begin{tabular}{ll} HKCU \software \microsoft \colongraph. \end{tabular} \begin{tabular}{ll} HKCU \software \colongraph. \end{tabular} \begin{tabular}{ll} HKCU \software \microsoft \microsoft \microsoft \microsoft \microsoft \micro
    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:
                                                              \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\.wpl+ \\
    Opens key:
                                                              \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\..wri+ \\
    Opens kev:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wvx
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xaml
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xbap
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlam
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xls
    Opens key:
                                                              \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.xlsb}
    Opens kev:
                                                              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
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xltx
    Opens key:
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xps
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.zip
    Opens key:
                                                              \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\mbox{\tt \mbox{\tt menuorder}}} \\
    Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites
                                                              HKCU\software\microsoft\windows\currentversion\explorer\menuorder\start
    Opens key:
menu
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2
    Opens key:
                                                              \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\mbox{\tt mountpoints2\cd}} \\ \mbox{\tt currentversion\explorer\mbox{\tt mountpoints2\cd}} \\ \mbox{\tt currentversion\explorer\mbox{\tt mountpoints2\cd}} \\ \mbox{\tt currentversion\explorer\mbox{\tt mountpoints2\cd}} \\ \mbox{\tt currentversion\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\e
    Opens key:
                                                              HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus d
    Opens key:
\label{lem:hcu} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \f 90255c0-6bc4-11e3-9fc7-10c0 \mbox{\current} \end{\current} .
806d6172696f}
    Opens key:
806d6172696f}
    Opens kev:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\mycomputer
    Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mycomputer\namespace
    Opens key:
```

HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.gif

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\recentdocs\.zip

```
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\streammru
         Opens key:
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\explorer\streams
         Opens key:
                                                                                                                                     \label{lem:hkcu} $$HKCU\software\microsoft\windows\currentversion\explorer\streams\0$
         Opens key:
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\explorer\streams\1
         Opens key:
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\explorer\streams\desktop
         Opens key:
                                                                                                                                     HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus stuck rects 2
         Opens key:
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\explorer\tips
         Opens key:
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\explorer\travnotifv
         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\{5e6ab780-7743-11cf-a12b-
00aa004ae837}
         Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (75048700 - ef1f-11d0-9888 - ef1f-11d
006097deacf9}
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\explorer\visualeffects
         Opens key:
         Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ visual effects \ an imatemin max \ max \ max \ max \ microsoft \ max \ ma
         Opens key:
Opens key:
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\fontsmoothing
         Opens key:
HKCU \ software \ microsoft \ windows \ current version \ (explorer \ visual effects) \ list box smooth scrolling \ microsoft \ windows \ (explorer) \ described \ for the substitution \ des
         Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ visual effects \ list viewal phase lect
         Opens key:
Opens key:
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\menuanimation
         Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\selectionfade
         Opens key:
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\themes
         Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\tooltipanimation
         Opens kev:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\webview
         Opens key:
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\explorer\webview
         Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\webview\barricadedfolders
         Opens key:
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo
         Opens key:
HKCU\software\microsoft\windows\currentversion\ext
         Opens key:
         Opens key:
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\ext\settings
         Opens key:
                                                                                                                                     HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus set in version \setminus ext \setminus set in version \setminus ext 
 e8ad-4283-a596-fa578c2ebdc3}
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\ext\settings\{4eb89ff4-
         Opens kev:
 7f78-4a0f-8b8d-2bf02e94e4b2}
                                                                                                                                     \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \ext\settings \cdot \cd
         Opens key:
d24c-4e72-af07-b576699ac0de}
         Opens key:
                                                                                                                                     HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus set in version \setminus ext \setminus set in version \setminus ext 
 0439-4c05-91e3-cf5cb290c3d0}
         Opens key:
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\ext\settings\{754ff233-
 5d4e-11d2-875b-00a0c93c09b3}
                                                                                                                                     Opens key:
 2274-4efb-b00b-d6aaba6d3850}
         Opens key:
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\ext\settings\{761497bb-
 d6f0-462c-b6eb-d4daf1d92d43}
         Opens key:
                                                                                                                                    HKCU\software\microsoft\windows\currentversion\ext\settings\{9059f30f-
4eb1-4bd2-9fdc-36f43a218f4a}
         Opens key:
                                                                                                                                     HKCU\software\microsoft\windows\currentversion\ext\settings\{b1549e58-
3894-11d2-bb7f-00a0c999c4c1}
         Opens key:
                                                                                                                                    HKCU\software\microsoft\windows\currentversion\ext\settings\{bdd307c3-
 7bc0-4542-9f8f-a9611fe6c1bf}
         Opens key:
                                                                                                                                    HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533adf1-microsoft\} \setminus \{c53adf1-microsoft\} \setminus
```

HKCU\software\microsoft\windows\currentversion\explorer\runmru

Opens key:

0c80-11d1-8c54-00a02468f316}

```
Opens key:
                                     HKCU\software\microsoft\windows\currentversion\ext\settings\{d27cdb6e-
ae6d-11cf-96b8-444553540000}
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-
a445-435b-bc74-9c25c1c588a9}
                                     HKCU\software\microsoft\windows\currentversion\ext\settings\{e7e6f031-
  Opens kev:
17ce-4c07-bc86-eabfe594f69c}
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\ext\stats
                                     HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-
  Opens key:
11cf-aaa5-00401c608501}
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
4283-a596-fa578c2ebdc3}
  Opens key:
                                     11cf-8fd0-00aa00686f13}
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\ext\stats\{761497bb-d6f0-
462c-b6eb-d4daf1d92d43}
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\ext\stats\{8856f961-340a-
11d0-a96b-00c04fd705a2}
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\ext\stats\{cfbfae00-17a6-
11d0-99cb-00c04fd64497}
                                     HKCU\software\microsoft\windows\currentversion\ext\stats\{d27cdb6e-ae6d-
  Opens key:
11cf-96b8-444553540000}
                                     HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
  Opens key:
435b-bc74-9c25c1c588a9}
                                     HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus stats \setminus \{dfeaf541 - f3e1 - 
  Opens key:
4c24-acac-99c30715084a}
                                     HKCU\software\microsoft\windows\currentversion\ext\stats\{e2e2dd38-d088-
  Opens key:
4134-82b7-f2ba38496583}
                                     HKCU\software\microsoft\windows\currentversion\ext\stats\{e7e6f031-17ce-
  Opens key:
4c07-bc86-eabfe594f69c}
                                     HKCU\software\microsoft\windows\currentversion\ext\stats\{fb5f1910-f110-
  Opens key:
11d2-bb9e-00c04f795683}
                                     HKCU\software\microsoft\windows\currentversion\group policy
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\group policy\appmgmt
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\group
policy\groupmembership
                                     HKCU\software\microsoft\windows\currentversion\group policy\history
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\group
policy\history\{a2e30f80-d7de-11d2-bbde-00c04f86ae3b}
                                     HKCU\software\microsoft\windows\currentversion\group policy objects
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\group policy
  Opens key:
objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}machine
                                     HKCU\software\microsoft\windows\currentversion\group policy
  Opens key:
objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}machine\software
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\group policy
objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}user
                                    HKCU\software\microsoft\windows\currentversion\grpconv
  Opens key:
  Opens key:
                                     \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\grpconv\mbox{\tt mapgroups}} \\
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
                                     HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\5.0
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\activities
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\activities\blog
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\activities\email
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\activities\map
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\activities\translate
                                     HKCU\software\microsoft\windows\currentversion\internet settings\cache
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\cache\content
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\cache\cookies
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\cache\history
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\connections
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
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
                                    HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
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
                                       HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\p3p\history
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\passport
                                       HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\passport\damap
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\protocols
  Opens key:
                                       \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\protocols\mailto
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\internet settings\url
history
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\internet settings\zonemap
                                       HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
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
                                       HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\ranges
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\internet settings\zones
  Opens key:
                                       \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\zones\endown} \mbox{\tt 20} \mbox{\tt 10} \mbox{\tt 10} \mbox{\tt 20} \mbox{\tt 10} \mbox{\tt 20} 
  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\policies
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\run
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\runonce
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\settings
  Opens key:
                                       \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{$m$icrosoft \windows \current version \settings \coremap. } \end{tabular} \label{lem:hkcu}
  Opens key:
HKCU \ software \ microsoft \ windows \ current version \ settings \ zone map \ protocolde faults
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\shell extensions
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\shell extensions\approved
                                       HKCU\software\microsoft\windows\currentversion\shell
  Opens key:
extensions\approved\{bdeadf00-c265-11d0-bced-00a0c90ab50f}
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
                                       HKCU\software\microsoft\windows\currentversion\shell extensions\cached
  Opens key:
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\syncmgr
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\syncmgr\handlers
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\telephony
  Opens key:
HKCU\software\microsoft\windows\currentversion\telephony\handoffpriorities
  Opens key:
HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key:
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\themes
  Opens key:
HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstvleoff
  Opens key:
HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleon
                                       HKCU\software\microsoft\windows\currentversion\themes\lasttheme
  Opens key:
  Opens kev:
                                       HKCU\software\microsoft\windows\currentversion\webcheck
  Opens key:
                                       HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus webcheck \setminus store. 1
  Opens key:
HKCU\software\microsoft\windows\currentversion\webcheck\store.1\{462932d0-0018-01cf-0000-
00002cc2cb62}
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\windowsupdate
  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\shell
  Opens key:
                                       HKCU\software\microsoft\windows\shell\bagmru
                                       HKCU\software\microsoft\windows\shell\bags
  Opens key:
  Opens key:
                                       HKCU\software\microsoft\windows\shell\bags\1
                                       HKCU\software\microsoft\windows\shell\bags\1\desktop
  Opens key:
                                       HKCU\software\microsoft\windows\shell\localizedresourcename
  Opens key:
  Opens key:
                                       HKCU\software\microsoft\windows\shellnoroam
                                       HKCU\software\microsoft\windows\shellnoroam\bagmru
  Opens kev:
                                       HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus bagmru \setminus 0
  Opens key:
  Opens key:
                                       HKCU\software\microsoft\windows\shellnoroam\bagmru\0\0
  Opens key:
                                       HKCU\software\microsoft\windows\shellnoroam\bagmru\0\1
  Opens key:
                                       HKCU\software\microsoft\windows\shellnoroam\bagmru\1
```

HKCU\software\microsoft\windows\shellnoroam\bagmru\2
HKCU\software\microsoft\windows\shellnoroam\bagmru\2\0

HKCU\software\microsoft\windows\shellnoroam\bagmru\3

Opens key:

Opens key: Opens key:

```
HKCU\software\microsoft\windows\shellnoroam\bags\1
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\1\shell
    Opens kev:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\10
    Opens key:
    Opens kev:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\10\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\11
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\11\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\12
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\12\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\13
    Opens key:
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\13\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\14
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\14\shell
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\15
    Opens key:
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\15\shell
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\16
    Opens key:
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\16\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\17
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\17\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\18
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\18\shell
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\19
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\19\shell
    Opens kev:
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\2
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\2\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\20
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\20\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\21
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\21\shell
    Opens kev:
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\22
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\22\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\23
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\23\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\24
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\24\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\25
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\25\shell
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\26
    Opens key:
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\26\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\27
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\27\shell
    Opens key:
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\28
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\28\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\29
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\29\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\3
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\3\shell
    Opens key:
    Opens key:
                                                                  HKCU \ software \ microsoft \ windows \ shell no roam \ bags \ 30
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\30\shell
    Opens kev:
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\31
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\31\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\32
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\32\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\4
    Opens kev:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\4\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\5
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\5\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\6
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\6\shell
    Opens key:
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\7
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\7\shell
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\8
    Opens key:
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\8\shell
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\9
                                                                  HKCU\software\microsoft\windows\shellnoroam\bags\9\shell
    Opens key:
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\duibags
    Opens key:
                                                                  HKCU\software\microsoft\windows\shellnoroam\duibags\shellfolders
    Opens key:
HKCU \ software \ microsoft \ windows \ shell no roam \ duibags \ shell folders \ \{20d04fe0-3aea-1069-a2d8-4046e1\} \ duibags \ shell folders \ \{20d04fe0-3aea-1069-a2d8-4046e1\} \ duibags \ shell folders \ folders \ duibags \ shell folders \ folders \ duibags \ folders \ fold
08002b30309d}
    Opens key:
HKCU \ software \ microsoft \ windows \ shell no roam \ duibags \ shell folders \ \{21ec2020-3aea-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2
08002b30309d}
    Opens key:
\label{thm:local-ham} HKCU \software \microsoft \windows \shell no roam \duibags \shell folders \cite{Grander-hammer} 47007 acc7-3202-11d1-aad2-barren \cite{Grander-hammer} 4
00805fc1270e}
    Opens key:
00aa0060fa31}
    Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus duibags \setminus shell folders \setminus \{f3364ba0 - 65b9 - 11ce - a9ba - 4bab - 4bab
00aa004ae837}
```

HKCU\software\microsoft\windows\shellnoroam\muicache

HKCU\software\microsoft\windows\shellnoroam\bags

Opens key:

Opens key:

```
Opens key:
                          HKCU\software\microsoft\windows help
 Opens key:
                          HKCU\software\microsoft\windows media
 Opens key:
                          HKCU\software\microsoft\windows media\wmsdk
 Opens key:
                          HKCU\software\microsoft\windows media\wmsdk\audiodecode
 Opens key:
                          HKCU\software\microsoft\windows media\wmsdk\general
 Opens key:
                          HKCU \setminus software \setminus microsoft \setminus windows \ media \setminus wmsdk \setminus local
                          HKCU\software\microsoft\windows media\wmsdk\namespace
 Opens key:
 Opens key:
                          HKCU\software\microsoft\windows media\wmsdk\remote
                          HKCU\software\microsoft\windows media\wmsdk\videodecode
 Opens key:
 Opens key:
                          HKCU\software\microsoft\windows nt
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion
 Opens key:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows nt\+ current version\+ devices
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\extensions
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\network
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\network\event viewer
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\network\persistent
connections
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\network\server manager
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\network\user manager
                          HKCU\software\microsoft\windows nt\currentversion\network\user manager
 Opens key:
for domains
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\printerports
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\program manager
                          HKCU\software\microsoft\windows nt\currentversion\program
 Opens key:
manager\restrictions
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\program
manager\settings
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\program
manager\unicode groups
                          HKCU\software\microsoft\windows nt\currentversion\taskmanager
 Opens key:
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\time zones
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\truetype
                          HKCU\software\microsoft\windows nt\currentversion\windows
 Opens key:
 Opens key:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows nt\- current version\+ winlogon
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\winlogon\gpextensions
 Opens key:
                          HKCU\software\microsoft\windows
nt\currentversion\winlogon\gpextensions\{a2e30f80-d7de-11d2-bbde-00c04f86ae3b}
 Opens key:
                          HKCU\software\microsoft\windows script
 Opens key:
                          HKCU\software\microsoft\windows script\settings
 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
                          HKCU\software\policies\microsoft\systemcertificates
 Opens key:
 Opens key:
                          HKCU\software\policies\microsoft\systemcertificates\ca
 Opens key:
                          HKCU\software\policies\microsoft\systemcertificates\ca\certificates
                          HKCU\software\policies\microsoft\systemcertificates\ca\crls
 Opens key:
 Opens key:
                          HKCU\software\policies\microsoft\systemcertificates\ca\ctls
 Opens key:
                          HKCU\software\policies\microsoft\systemcertificates\disallowed
 Opens key:
HKCU\software\policies\microsoft\systemcertificates\disallowed\certificates
                          HKCU\software\policies\microsoft\systemcertificates\disallowed\crls
 Opens key:
                          HKCU\software\policies\microsoft\systemcertificates\disallowed\ctls
 Opens kev:
 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\trustedpublisher
 Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus trusted publisher \setminus certificates
 Opens key:
\label{lem:hkcu} \verb+KCU \software \policies \microsoft \system certificates \trusted publisher \crls
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\ctls
                          HKCU\software\classes
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid
 Opens key:
                          HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}
                          HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-
 Opens key:
00805f499d93}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0013-0000-0003-abcdeffedcba}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0013-0000-0003-
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0013-0000-0004-abcdeffedcba}
                          HKCU\software\classes\clsid\{cafeefac-0013-0000-0004-
 Opens key:
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0013-0000-0005-abcdeffedcba}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0013-0000-0005-
```

```
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0000-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0000-
abcdeffedcba}\inprocserver32
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0003-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0003-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0003-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0003-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0004-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0004-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0004-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0004-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0005-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0005-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0005-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0005-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0007-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0007-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0007-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0007-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0008-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0008-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0008-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0008-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0009-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0009-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0009-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0010-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0010-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0010-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0010-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0011-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0011-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0011-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0011-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0012-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0012-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0012-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0012-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0013-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0013-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0013-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0013-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0014-abcdeffedcba}
```

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

abcdeffedcbb}\inprocserver32

```
Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0001-abcdeffedcba}
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0001-
 Opens key:
abcdeffedcba}\inprocserver32
                          \label{local-condition} HKCU \setminus software \setminus classes \setminus clsid \setminus \{cafee fac-0014-0001-0001-abcdeffed cbb\}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0001-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0002-abcdeffedcba}
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0002-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0002-abcdeffedcbb}
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0002-
 Opens key:
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0003-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0003-
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0003-abcdeffedcbb}
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0003-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0004-abcdeffedcba}
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0004-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0004-abcdeffedcbb}
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0004-
 Opens key:
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-
 Opens key:
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-
 Opens key:
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0006-abcdeffedcba}
 Opens kev:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0006-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0006-abcdeffedcbb}
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0006-
 Opens key:
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0007-abcdeffedcba}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0007-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0007-abcdeffedcbb}
 Opens key:
 Opens key
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0007-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0000-abcdeffedcba}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0000-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0000-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0000-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0001-abcdeffedcba}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0001-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0001-abcdeffedcbb}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0001-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0002-abcdeffedcba}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0002-
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0002-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0002-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0003-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0003-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0003-abcdeffedcbb}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0003-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0004-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0004-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0004-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0004-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0005-abcdeffedcba}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0005-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0005-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0005-
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0006-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0006-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0006-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0002-0006-
```

```
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0007-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0007-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0007-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0007-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0008-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0008-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0008-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0008-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0009-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0009-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0009-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0009-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0010-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0010-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0010-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0010-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0011-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0011-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0011-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0011-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0012-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0012-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0012-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0012-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0014-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0014-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0014-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0014-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0015-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0015-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0015-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0015-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0016-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0016-
 Opens kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0016-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0016-
abcdeffedcbb}\inprocserver32
 Opens key:
                         \label{localization} \begin{tabular}{ll} HKCU \software \classes \clsid \cafeefac-0014-0002-0017-abcdeffedcba \end{tabular}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0017-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0017-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0017-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0018-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0018-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0018-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0018-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0019-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0019-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0019-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0019-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-abcdeffedcbb}
```

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0021-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0021-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0021-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0021-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0022-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0022-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0022-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0022-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0023-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0023-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0023-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0023-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0024-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0024-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0024-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0024-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0025-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0025-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0025-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0025-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0026-abcdeffedcba}
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0026-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0026-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0026-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0027-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0027-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0027-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0027-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0028-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0028-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0028-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0028-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0029-abcdeffedcba}
                         Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0029-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0029-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0030-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0030-
 Opens key
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0030-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0030-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0031-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0031-
 Opens kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0031-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0031-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0032-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0032-
 Opens kev
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0032-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0032-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0033-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0033-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0033-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0033-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0034-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0034-
 Opens key:
```

abcdeffedcba}\inprocserver32

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0034-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0034-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-ffff-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-ffff-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-
 Opens kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-abcdeffedcbc}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-abcdeffedcba}
                         Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-abcdeffedcbc}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-
```

```
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-
abcdeffedcbc}\inprocserver32
 Opens kev:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-abcdeffedcbc}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-abcdeffedcbb}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-abcdeffedcba}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-
 Opens key:
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-
 Opens kev:
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0014-abcdeffedcba}
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0014-
 Opens kev:
abcdeffedcba}\inprocserver32
                          \label{local-equation} \begin{tabular}{ll} HKCU \software \classes \clsid \cafeefac-0015-0000-0014-abcdeffedcbb} \end{tabular}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0014-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0014-abcdeffedcbc}
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0014-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-abcdeffedcbb}
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-
 Opens key:
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-abcdeffedcbc}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-
 Opens kev:
abcdeffedcbc}\inprocserver32
                          \label{local-condition} HKCU \setminus software \setminus classes \setminus clsid \setminus \{cafee fac-0015-0000-0016-abcdeffedcba\}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-abcdeffedcbb}
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-abcdeffedcbc}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-abcdeffedcba}
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-abcdeffedcbc}
```

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-
 Opens kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-abcdeffedcbb}
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-
 Opens kev:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-abcdeffedcbc}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-
 Opens key
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-abcdeffedcbc}
                         Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-
 Opens key
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-
 Opens kev
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-
 Opens kev
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-abcdeffedcbc}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-abcdeffedcbc}
                         Opens key:
```

abcdeffedcbc}\inprocserver32

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-abcdeffedcbc}
                         Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-abcdeffedcbb}
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-abcdeffedcbc}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-abcdeffedcbc}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-ffff-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-ffff-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-abcdeffedcbc}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-abcdeffedcbc}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-
```

```
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-
abcdeffedcba}\inprocserver32
 Opens kev:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-abcdeffedcbc}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-abcdeffedcbb}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-
 Opens key:
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-abcdeffedcbc}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-
 Opens kev:
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-
abcdeffedcba}\inprocserver32
                          \label{local-condition} \mbox{HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-abcdeffedcbb}}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-
 Opens kev:
abcdeffedcbb}\inprocserver32
                          \label{local-condition} HKCU \setminus software \setminus classes \setminus clsid \setminus \{cafee fac-0016-0000-0008-abcdeffedcbc\}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-abcdeffedcba}
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-
 Opens key:
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-abcdeffedcbc}
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-
 Opens key:
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-
 Opens kev:
abcdeffedcba}\inprocserver32
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \cafeefac-0016-0000-0010-abcdeffedcbb \end{tabular}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-abcdeffedcbc}
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-abcdeffedcbb}
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-abcdeffedcbc}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-abcdeffedcba}
```

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0013-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0013-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0013-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0013-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0013-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0013-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0014-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0014-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0014-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0014-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0014-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0014-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0015-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0015-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0015-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0015-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0015-abcdeffedcbc}
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0015-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0016-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0016-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0016-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0016-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0016-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0016-
 Opens kev:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0018-abcdeffedcba}
                         Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0018-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0018-
 Opens key
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0018-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0018-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-
 Opens kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-
 Opens kev
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-abcdeffedcba}
                         Opens key:
```

abcdeffedcba}\inprocserver32

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-
 Opens kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcdeffedcbc}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-abcdeffedcbc}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-abcdeffedcbc}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-ffff-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-ffff-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-
```

```
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-abcdeffedcbb}
 Opens key:
 Opens key:
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-
abcdeffedcbb}\inprocserver32
 Opens key:
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-abcdeffedcbc}
 Opens key:
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-abcdeffedcba}
 Opens key:
 Opens key:
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-abcdeffedcbb}
 Opens key:
 Opens key:
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-abcdeffedcbc}
 Opens key:
 Opens key:
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}
 Opens kev:
 Opens key:
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}
 Opens key:
 Opens key:
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprocserver32
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}
 Opens kev:
 Opens key:
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbc}\inprocserver32
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-abcdeffedcba}
 Opens key:
 Opens key:
                        HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-
abcdeffedcba}\inprocserver32
                        HKCU\software\classes\clsid\{e19f9331-3110-11d4-991c-005004d3b3db}
 Opens key:
 Opens key:
                        HKCU\software\classes\clsid\{e19f9331-3110-11d4-991c-
005004d3b3db}\inprocserver32
                        HKCU\software\classes\javaplugin.1020
 Opens key:
 Opens key:
                        HKCU \ software \ classes \ javaplugin. 1020 \ clsid
 Opens key:
                        HKCU\software\classes\software
 Opens key:
                        HKCU\software\classes\software\microsoft
 Opens key:
                        HKCU\software\classes\software\microsoft\mediaplayer
                        HKCU\software\classes\software\microsoft\mediaplayer\preferences
 Opens kev:
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\run
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
 Opens key:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
 Opens key:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mfc42u.dll
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\npptools.dll
 Opens key:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\packet.dll
 Opens key:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wpcap.dll
 Opens key:
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}
 Opens key:
                        08002be10318}\0000
 Opens key:
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage
 Opens key:
                        HKLM\system\currentcontrolset\services\npf
 Opens key:
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001
 Opens key:
                        08002be10318}\0001\linkage
 Opens key:
                        HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\ms
tcp loopback interface
 Opens key:
                        HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens key:
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002
 Opens key:
                        08002be10318}\0002\linkage
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens kev:
08002be10318}\0003
 Opens key:
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\linkage
 Opens key:
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
08002be10318}\0004\linkage
 Opens key:
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005
 Opens key:
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005\linkage
 Opens key:
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006
```

```
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
08002be10318}\0006\linkage
 Opens key:
                      HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007
 Opens kev:
                      08002be10318}\0007\linkage
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\linkage
                      Opens kev:
08002be10318}\0009
 Opens key:
                      08002be10318}\0009\linkage
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010
                      Opens key:
08002be10318}\0010\linkage
 Opens key:
                      08002be10318}\0011
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\linkage
                      \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
 Opens kev:
options\ndisnpp.dll
 Opens key:
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
 Opens key:
HKLM\software\microsoft\ctf\compatibility\752d6fe81122349daf998a56f48e0b38.exe
 Opens kev:
                      HKLM\software\microsoft\ctf\systemshared\
 Opens key:
                      HKCU\keyboard layout\toggle
 Opens key:
                      HKLM\software\microsoft\ctf\
                      HKCU\software\flashfxp
 Opens key:
 Opens key:
                      HKCU\software\flashfxp\3
 Opens key:
                      HKCU\software\flashfxp\4
                      HKLM\software\flashfxp
 Opens key:
 Opens key:
                      HKLM\software\flashfxp\3
 Opens key:
                      HKLM\software\flashfxp\4
                      HKLM\software\microsoft\windows\currentversion\uninstall
 Opens key:
 Opens key:
                      HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus address book
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash
player activex
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\branding
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\connection
manager
 Opens key:
                      HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus direct an imation
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\directdrawex
                      HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus dxm\_runtime
 Opens key:
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\fontcore
                      HKLM\software\microsoft\windows\currentversion\uninstall\icw
 Opens kev:
 Opens key:
HKLM\software\microsoft\windows\currentversion\uninstall\idnmitigationapis
                      HKLM\software\microsoft\windows\currentversion\uninstall\ie40
 Opens key:
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\ie4data
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\ie5bakex
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\ie7
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\ie8
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\iedata
                      HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-v5
 Opens key:
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\microsoft .net
framework 3.5 sp1
 Opens key:
HKLM\software\microsoft\windows\currentversion\uninstall\mobileoptionpack
                      HKLM\software\microsoft\windows\currentversion\uninstall\mplayer2
 Opens key:
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\netmeeting
 Opens key:
HKLM\software\microsoft\windows\currentversion\uninstall\nlsdownlevelmapping
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\outlookexpress
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\pchealth
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\schedulingagent
                      HKLM\software\microsoft\windows\currentversion\uninstall\wic
 Opens kev:
                      Opens key:
3d01-b289-befc77a11a1e}
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-
4ca4-87b4-2f83217002ff}
 Opens key:
                      4ee8-baa9-00bcb3d54227}
 Opens key:
                      4037-7777-5f2748764d10}
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-
0409-0000-0000000ff1ce}
 Opens key:
                      11d3-8cfe-0150048383c9}
 Opens key:
```

0409-0000-0000000ff1ce} HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-Opens key: 0409-0000-0000000ff1ce} Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-3813-a88d-b8dccde8f8c7} Opens key:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus \{ac76ba86-7ad7-ba86-7ad7$ 1033-7b44-a93000000001} Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-3f2d-899a-6a1d67f2073f} Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-4027-b136-2b3e1f5ab6e2} Opens key: 36ca-84d3-9f4dcf5c5bd9} HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-Opens key: 36ca-84d3-9f4dcf5c5bd9}.kb953595 Opens key: HKCU\software\bpftp\bullet proof ftp\main HKCU\software\bulletproof software\bulletproof ftp client\main Opens kev: 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 HKCU\software\turboftp Opens key: HKCU\software\cryer\websitepublisher Opens key: Opens key: HKLM\system\currentcontrolset\control\computername Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername 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\microsoft\windows\currentversion Opens key: HKCU\software\globalscape\cuteftp 6 home\qctoolbar Opens key: HKCU\software\globalscape\cuteftp 6 professional\qctoolbar Opens key:  ${\tt HKCU \setminus software \setminus global scape \setminus cuteftp~7~home \setminus qctoolbar}$ Opens key: HKCU\software\globalscape\cuteftp 7 professional\qctoolbar HKCU\software\globalscape\cuteftp 8 home\qctoolbar Opens key: Opens key: HKCU\software\globalscape\cuteftp 8 professional\qctoolbar Opens key: HKCU\software\sota\ffftp\options HKCU\software\south river technologies\webdrive\connections Opens key: Opens key: HKCU\software\nch software\classicftp\ftpaccounts Opens key: HKLM\software\nch software\fling\accounts HKCU\software\filezilla Opens key: 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\microsoft\windows\currentversion\uninstall\ultrafxp Opens key: HKCU\software\martin prikryl Opens key: HKLM\software\martin prikryl Opens key: HKCU\software\ftpware\coreftp\sites HKCU\software\far\plugins\ftp\hosts Opens kev: 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\microsoft\windows nt\currentversion\image file execution options\userenv.dll Opens kev: HKLM\svstem\currentcontrolset\control\productoptions Opens key: HKLM\software\policies\microsoft\windows\system HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Opens key: 1757981266-507921405-1957994488-1003 Opens key: HKCU\software\ghisler\windows commander Opens key: HKCU\software\ghisler\total commander Opens key: HKLM\software\ghisler\windows commander Opens key: HKLM\software\ghisler\total commander Opens key: HKCU\software\acebit Opens key: HKLM\software\acebit HKCR\typelib\{cb1f2c0f-8094-4aac-bcf5-41a64e27f777} Opens key: Opens key: HKCR\typelib\{9ea55529-e122-4757-bc79-e4825f80732c} Opens key: HKLM\software  $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key: options\atl.dll Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\pstorec.dll Opens key: HKCU\software\mozilla Opens key: HKLM\software\mozilla HKLM\software\mozilla\firefox Opens key: Opens key: HKLM\software\mozilla\firefox\extensions HKCU\software\chromeplus Opens kev: HKCU\software\leechftp Opens key: Opens key: HKLM\software\classes Opens key: HKCU\software\flashpeak\blazeftp\settings Opens key: Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value:

 $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers[transparentenabled]|$ 

Oueries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled] Oueries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack] Oueries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Queries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles] Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[752d6fe81122349daf998a56f48e0b38] HKLM\software\microsoft\windows nt\currentversion\ime Oueries value: compatibility[752d6fe81122349daf998a56f48e0b38] Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit\_dlls] HKLM\system\currentcontrolset\control\session Oueries value: manager[criticalsectiontimeout] Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout] Oueries value: HKCR\interface[interfacehelperdisableall] Queries value: HKCR\interface[interfacehelperdisableallforole32] Queries value: HKCR\interface[interfacehelperdisabletypelib] HKCR\interface\{00020400-0000-0000-c000-Oueries value: 00000000046}[interfacehelperdisableall] Queries value: . HKCR\interface\{00020400-0000-0000-c000-00000000046}[interfacehelperdisableallforole32] HKCU\control panel\desktop[multiuilanguageid] Queries value: Queries value: HKCU\control panel\desktop[smoothscroll] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings[disableimprovedzonecheck] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_protocol\_lockdown[752d6fe81122349daf998a56f48e0b38.exe] HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature\_protocol\_lockdown[\*] HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-Oueries value: ab78-1084642581fb1 Queries value: 0000-0000000000000] Oueries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]

Queries value:

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

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]

Oueries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]

Queries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]

Oueries value:

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value:

Oueries value:

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

 $\label{local-observation} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ and $$ is a simple of the control set \end{tabular} $$ and $$ is a simple of \end{tabular} $$ and $$ is a simple of \end{tabular} $$ and \end{ta$ Oueries value:

Queries value:

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

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]

Queries value:

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

Queries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]

Queries value:

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

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]

Oueries value:

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

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable wandynamic update]$ 

Queries value:

```
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Oueries value:
 Queries value:
                      HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Queries value:
                      HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
 Oueries value:
                      HKLM\system\setup[systemsetupinprogress]
 Queries value:
HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters[dnsquery time outs]|
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsmulticast query time outs]
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog 9 [next\_catalog\_entry\_id]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Oueries 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]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem]
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Oueries value:
Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001 \ [address family]
```

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[displaystring]
Oueries 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]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[supportednamespace]
Oueries 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]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[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]
Oueries 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]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[enabled] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[version]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32numhandlebuckets]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32spincount]

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

 Queries value:
 HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]

 Queries value:
 HKLM\system\currentcontrolset\services\winsock\parameters[transports]

 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
 Oueries value:

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

Queries value: HKLM\system\currentcontrolset\control\nls\language groups[5]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[2]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[4]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000419]
Queries value: HKCU\software\microsoft\internet explorer\main[]

Queries value: HKCU\software\microsoft\internet explorer\main[shownotifysize]
Queries value: HKCU\software\microsoft\internet explorer\main[recordsavedactive]
Queries value: HKCU\software\microsoft\internet explorer\main[widthlocalizeduse]
Queries value: HKCU\software\microsoft\internet explorer\main[pagecompressedinvalid]
Queries value: HKCU\software\microsoft\internet explorer\main[textcompletedmin]
Queries value: HKCU\software\microsoft\internet explorer\main[textcompletedmin]
Queries value: HKLM\software\microsoft\windows\currentversion\run[sonyagent]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [enabledhcp]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{16325b0b-4636-4303-abe3-c7d49d7cecdc\}[lease \ obtained time]$ 

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[leaseterminatestime]

Queries value:

 $\label{lem:hkkm} HKLM \system \current controls et \services \troip \parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [dhcpserver]$ 

Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0000[componentid]

```
Queries value:
                                                                   HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage[export]
    Oueries value:
                                                                   HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001[componentid]
    Oueries value:
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\linkage[export]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[domain]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpdomain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationenabled]
    Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[registeradaptername]
    Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr
c7d49d7cecdc}[nameserver]
    Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[dhcpnameserver]
    Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr
c7d49d7cecdc}[usezerobroadcast]
    Queries value:
c7d49d7cecdc}[dhcpipaddress]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpsubnetmask]
    Queries value:
                                                                   HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002[componentid]
                                                                   Queries value:
08002be10318}\0002\linkage[export]
    Queries value:
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003[componentid]
    Queries value:
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\linkage[export]
                                                                  Queries value:
08002be10318}\0004[componentid]
    Queries value:
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004\linkage[export]
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Queries value:
08002be10318}\0005[componentid]
                                                                  Queries value:
08002be10318}\0005\linkage[export]
    Queries value:
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[componentid]
    Oueries value:
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\linkage[export]
    Queries value:
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[componentid]
    Queries value:
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\linkage[export]
    Oueries value:
                                                                   HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008[componentid]
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Queries value:
08002be10318}\0008\linkage[export]
    Queries value:
                                                                  08002be10318}\0009[componentid]
    Oueries value:
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009\linkage[export]
                                                                   Oueries value:
08002be10318}\0010[componentid]
    Queries value:
                                                                  08002be10318}\0010\linkage[export]
                                                                   Oueries value:
08002be10318}\0011[componentid]
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Oueries value:
08002be10318}\0011\linkage[export]
    Queries value:
                                                                   HKLM\software\microsoft\ctf\systemshared[cuas]
    Queries value:
                                                                   HKCU\keyboard layout\toggle[language hotkey]
                                                                   HKCU\keyboard layout\toggle[hotkey]
    Oueries value:
    Queries value:
                                                                   HKCU\keyboard layout\toggle[layout hotkey]
    Queries value:
                                                                   HKLM\software\microsoft\ctf[enableanchorcontext]
                                                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
    Oueries value:
folders[appdata]
    Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\addressbook[uninstallstring]
    Queries value:
```

```
player activex[uninstallstring]
                                                HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash
   Oueries value:
player activex[displayname]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\branding[uninstallstring]
                                                \label{thm:local_hammon} $HKLM \setminus microsoft \wedge current version \cap connection $$ (All the first of the first of
   Queries value:
manager[uninstallstring]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\uninstall\directanimation[uninstallstring]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\uninstall\directdrawex[uninstallstring]
   Queries value:
Oueries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus fontcore[uninstalls tring]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\uninstall\icw[uninstallstring]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\idnmitigationapis[uninstallstring]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie40[uninstallstring]
   Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\uninstall\ie4data[uninstallstring]|
HKLM \ software \ microsoft \ windows \ current version \ uninstall \ ie5 bakex \ [uninstallstring]
   Queries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus ie7[uninstall string]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie8[uninstallstring]
HKLM\software\microsoft\windows\currentversion\uninstall\ie8[displayname]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\iedata[uninstallstring]
                                               HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-
   Queries value:
v5[uninstallstring]
   Queries value:
                                                HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-
v5[displayname]
   Queries value:
                                                HKLM\software\microsoft\windows\currentversion\uninstall\microsoft .net
framework 3.5 sp1[uninstallstring]
                                                HKLM\software\microsoft\windows\currentversion\uninstall\microsoft .net
   Queries value:
framework 3.5 sp1[displayname]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\mobileoptionpack[uninstallstring]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\mplayer2[uninstallstring]
   Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\uninstall\netmeeting[uninstallstring]|
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\nlsdownlevelmapping[uninstallstring]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\outlookexpress[uninstallstring]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\uninstall\pchealth[uninstallstring]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\pchealth[displayname]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\schedulingagent[uninstallstring]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\uninstall\wic[uninstallstring]
   Queries value:
                                                HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-
3d01-b289-befc77a11a1e}[uninstallstring]
   Queries value:
                                                HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-
3d01-b289-befc77a11a1e}[displayname]
                                                HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-
   Oueries value:
4ca4-87b4-2f83217002ff}[uninstallstring]
   Oueries value:
                                                HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-
4ca4-87b4-2f83217002ff}[displayname]
   Queries value:
                                                HKLM \ software \ `microsoft\ `windows \ `current version \ `uninstall\ \{350c97b0-3d7c-microsoft\ `windows\ `current version\ `uninstall\ `table (350c97b0-3d7c-microsoft\ `windows\ `current version\ `windows\ `current version\ `windows\ `current version\ `windows\ `current version\ `windows\ `windows\
4ee8-baa9-00bcb3d54227}[uninstallstring]
   Oueries value:
                                                HKLM\software\microsoft\windows\currentversion\uninstall\{4a03706f-666a-
4037-7777-5f2748764d10}[uninstallstring]
   Oueries value:
                                                0409-0000-0000000ff1ce}[uninstallstring]
   Queries value:
                                                HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-
0409-0000-0000000ff1ce}[displayname]
                                                HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-
   Oueries value:
11d3-8cfe-0150048383c9}[uninstallstring]
   Oueries value:
                                                11d3-8cfe-0150048383c9}[displayname]
   Queries value:
                                                HKLM\software\microsoft\windows\currentversion\uninstall\{95120000-003f-
0409-0000-0000000ff1ce}[uninstallstring]
                                                HKLM\software\microsoft\windows\currentversion\uninstall\{95120000-003f-
   Oueries value:
0409-0000-0000000ff1ce}[displayname]
```

Oueries value: 0409-0000-0000000ff1ce}[uninstallstring] Oueries value: 0409-0000-0000000ff1ce}[displayname] HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-Oueries value: 3813-a88d-b8dccde8f8c7}[uninstallstring] Queries value:  $HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{a3051cd0-2f64-464-464\} \ and \ and$ 3813-a88d-b8dccde8f8c7}[displayname] Queries value:  $HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{ac76ba86-7ad7-14b$ 1033-7b44-a93000000001}[uninstallstring] HKLM\software\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-Oueries value: 1033-7b44-a93000000001}[displayname] Queries value: 3f2d-899a-6a1d67f2073f}[uninstallstring] HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-Queries value: 3f2d-899a-6a1d67f2073f}[displayname] HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-Oueries value: 4027-b136-2b3e1f5ab6e2}[uninstallstring]  $HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{c3cc4df5-39a5-40f5-39a5$ Queries value: 4027-b136-2b3e1f5ab6e2}[displayname] Queries value: 36ca-84d3-9f4dcf5c5bd9}[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-36ca-84d3-9f4dcf5c5bd9}[displayname] Queries value: 36ca-84d3-9f4dcf5c5bd9}.kb953595[uninstallstring] Queries value: 36ca-84d3-9f4dcf5c5bd9}.kb953595[displayname] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common appdata] Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername] Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir] HKLM\software\microsoft\windows\currentversion[commonfilesdir] Queries value: HKLM\software\microsoft\windows Oueries value: nt\currentversion\winlogon[userenvdebuglevel] HKLM\software\microsoft\windows Queries value: nt\currentversion\winlogon[chkaccdebuglevel] Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[personal] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local settings] HKLM\software\microsoft\windows Queries value: nt\currentversion\winlogon[rsopdebuglevel] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Oueries value: 1757981266-507921405-1957994488-1003[profileimagepath] Oueries value: HKLM\software[debuglogpath] HKLM\software[debugloglevel] Oueries value: Queries value: HKLM\software[enabledebuglog] Queries value: HKLM\software\mozilla\firefox[pathtoexe] Oueries value: HKLM\software\mozilla\firefox\extensions[pathtoexe] Queries value: HKLM\software\mozilla[pathtoexe] Oueries value:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus address book [address book]$ Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\branding[branding] HKLM\software\microsoft\windows\currentversion\uninstall\connection Queries value: manager[connection manager] Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\directanimation[directanimation] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\directdrawex[directdrawex] Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\dxm\_runtime[dxm\_runtime] Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\fontcore[fontcore] Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\icw[icw] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\idnmitigationapis[idnmitigationapis] Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\ie40[ie40] Queries value:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus ie4 data[ie4 data]$ Queries value:

HKLM\software\microsoft\windows\currentversion\uninstall\ie5bakex[ie5bakex] HKLM\software\microsoft\windows\currentversion\uninstall\ie7[ie7] Oueries value: Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\iedata[iedata] Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\mobileoptionpack[mobileoptionpack] Queries value:

HKLM\software\microsoft\windows\currentversion\uninstall\mplayer2[mplayer2]

Queries value:

HKLM\software\microsoft\windows\currentversion\uninstall\netmeeting[netmeeting]

Queries value:

HKLM\software\microsoft\windows\currentversion\uninstall\nlsdownlevelmapping[nlsdownlevelmapping]
 Oueries value:

Queries value.

HKLM\software\microsoft\windows\currentversion\uninstall\outlookexpress[outlookexpress]

Queries value:

4ee8-baa9-00bcb3d54227}[{350c97b0-3d7c-4ee8-baa9-00bcb3d54227}]

Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{4a03706f-666a-

4037-7777-5f2748764d10}[{4a03706f-666a-4037-7777-5f2748764d10}]

Queries value: HKCU\software\classes\[clsid\{11c1d741-a95b-11d2-8a80-

0080adb32ff4}\inprocserver32]

Queries value: HKLM\software\classes[clsid\{11c1d741-a95b-11d2-8a80-

0080adb32ff4}\inprocserver32]

Sets/Creates value: HKCU\software\microsoft\internet explorer\main[shownotifysize]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[recordsavedactive]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[widthlocalizeduse]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[pagecompressedinvalid]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[textcompletedmin]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\run[sonyagent]

Value changes: HKLM\software\microsoft\cryptography\rng[seed]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[appdata]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[local appdata]

Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell

folders[common appdata]

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