Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3303, Task ID: 720

Task ID: 720 Risk Level: 10

Date Processed: 2016-05-18 10:30:52 (UTC)

Processing Time: 62.3 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\70b2225f430facf31ca65621c234f09e.exe"

Sample ID: Type: basic admin Owner:

70b2225f430facf31ca65621c234f09e Label:

Date Added: 2016-05-18 10:30:48 (UTC) PE32:win32:gui

File Type: File Size: 855552 bytes

MD5: 70b2225f430facf31ca65621c234f09e

375c6e3dfa967d9d6760d4e8ca0868c864fecde2735ce0d1f189b3b2aef512b7 SHA256:

Description: None

Pattern Matching Results

Modifies registry autorun entries

6 Writes to system32 folder

6 Tries to detect VM environment

10 Creates malicious events: Kelihos trojan 2 [Spam]

3 Connects to local host

5 Creates file in drivers folder

5 PE: Contains compressed section

5 Adds autostart object

Process/Thread Events

C:\WINDOWS\Temp\70b2225f430facf31ca65621c234f09e.exe

["c:\windows\temp\70b2225f430facf31ca65621c234f09e.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

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

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

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

File System Events

Creates C:\Documents and Settings\Admin\Local Settings\Temp\mmc004AA394.xml

Creates: C:\WINDOWS\Temp\tmp.exe Creates: C:\WINDOWS\system32\Packet.dll Creates: C:\WINDOWS\system32\wpcap.dll C:\WINDOWS\system32\drivers\npf.sys Creates:

C:\WINDOWS\Prefetch\70B2225F430FACF31CA65621C234F-383C54AD.pf Opens:

C:\Documents and Settings\Admin Opens: C:\WINDOWS\system32\ufat.dll Opens: Opens: C:\WINDOWS\system32\ulib.dll Opens: C:\WINDOWS\system32\ifsutil.dll Opens: C:\WINDOWS\system32\cfgmgr32.dll Opens: C:\WINDOWS\system32\setupapi.dll C:\WINDOWS\system32\mmcbase.dll Opens: Opens: C:\WINDOWS\system32\mfc42u.dll C:\WINDOWS\system32\msvcp60.dll Opens: Opens: C:\WINDOWS\system32\rpcns4.dll Opens: C:\WINDOWS\system32\sqlunirl.dll Opens: C:\WINDOWS\system32\winspool.drv C:\WINDOWS\system32\imm32.dll Opens: Opens: C:\WINDOWS\system32\comctl32.dll

C:\WINDOWS\system32\COMCTL32.dll.124.Manifest Opens: Opens: C:\WINDOWS\system32\COMCTL32.dll.124.Config

Opens: C:\WINDOWS\system32\shell32.dll

Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest

```
C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                         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
 Opens:
                         C:\WINDOWS\WindowsShell.Manifest
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\WINDOWS\system32\nddeapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\cmdial32.dll
                         C:\WINDOWS\system32\cmpbk32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\cmutil.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
                         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\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
 Opens:
                         C:\WINDOWS\Temp\70b2225f430facf31ca65621c234f09e.exe
 Opens:
                         C:\WINDOWS\Temp
 Opens:
                         C:\WINDOWS\Temp\tmp.exe
 Opens:
                         C:\WINDOWS\Temp\c1f32bed-894a-4ee4-8423-03eb3af42a6f
 Opens:
                         C:\dev\urandom
                         C:\WINDOWS\system32
 Opens:
 Opens:
                         C:\
 Opens:
                         C:\AUTOEXEC.BAT
 Opens:
                         C:\boot.ini
 Opens:
                         C:\WINDOWS\system32\drivers
                         C:\WINDOWS\system32\wpcap.dll
 Opens:
                         C:\CONFIG.SYS
 Opens:
 Opens:
                         C:\Documents and Settings
 Opens:
                         C:\Documents and Settings\Admin\Application Data
                         C:\Documents and Settings\Admin\Application Data\Adobe
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\AdobeCMapFnt09.lst
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\AdobeSysFnt09.1st
                         C:\WINDOWS\system32\wpcap.dll.2.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\wpcap.dll.2.Config
 Opens:
                         C:\WINDOWS\system32\Packet.dll
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0\Forms
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Acrobat\9.0\JavaScripts
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts\glob.js
 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:\WINDOWS\system32\packet.dll.2.Manifest
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\UserCache.bin
 Opens:
                         C:\WINDOWS\system32\packet.dll.2.Config
 Opens:
                         C:\WINDOWS\system32\npptools.dll
 Opens:
                         C:\WINDOWS\system32\drivers\npf.sys
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Flash Player
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Flash
Player\AssetCache
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Flash
Player\AssetCache\7PLTA3CP
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Adobe\Linguistics}
 Opens:
 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
 Opens:
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\all
                         C:\Documents and Settings\Admin\Application
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
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\LogTransport2
                         C:\Documents and Settings\Admin\Application
 Opens:
```

Data\Adobe\LogTransport2\Logs

```
C:\Documents and Settings\Admin\Application Data\desktop.ini
   Opens:
                                              C:\Documents and Settings\Admin\Application Data\Identities
   Opens:
                                              Opens:
1E8B-4ECF-8560-0E560368800D}
   Opens:
                                              {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia}
   Opens:
                                              {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash\ Player}
                                              C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
   Opens:
Player\#SharedObjects
   Opens:
                                              C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW
                                              C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
   Opens:
Player\macromedia.com
   Opens:
                                              C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support
   Opens:
                                              C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer
   Opens:
                                              C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys
   Opens:
                                              C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
   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
                                              {\tt C:\Documents\ and\ Settings\Admin\Application}
   Opens:
Data\Microsoft\CryptnetUrlCache
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\0797C381B2F87EB5A1D5573BD15BA4F4
                                              {\tt C:\Documents\ and\ Settings\Admin\Application}
   Opens:
Data\Microsoft\CryptnetUrlCache\Content\135BD6A358680A7BF1CCEC7C0172393D
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004
                                              C:\Documents and Settings\Admin\Application
   Opens:
Data\Microsoft\CryptnetUrlCache\Content\3130B1871A126520A8C47861EFE3ED4D
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\60E31627FDA0A46932B0E5948949F2A5
   Opens:
                                              C:\Documents and Settings\Admin\Application
C:\WINDOWS\system32\npp\ndisnpp.dll
   Opens:
                                              C:\WINDOWS\system32\rpcss.dll
   Opens:
   Opens:
                                              C:\WINDOWS\system32\MSCTF.dll
   Opens:
                                              C:\WINDOWS\system32\npp
   Opens:
                                              C:\Documents and Settings\Admin\Application
C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7396C420A8E1BC1DA97F1AF0D10BAD21
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE8E7EB5F575EC9
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\8DFDF057024880D7A081AFBF6D26B92F
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\A44F4E7CB3133FF765C39A53AD8FCFDD
                                              C:\Documents and Settings\Admin\Application
   Opens:
\label{lem:label} Data \\ \mbox{Microsoft} \\ \mbox{CryptnetUrlCache} \\ \mbox{Content} \\ \mbox{F482C95F83F1B59228F1B1E720F2EDF1} \\ \mbox{Reconstant of the content} \\ \mbox{Reconstant of the c
                                              C:\Documents and Settings\Admin\Application
   Opens:
Data\Microsoft\CryptnetUrlCache\MetaData
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\0797C381B2F87EB5A1D5573BD15BA4F4
                                              C:\Documents and Settings\Admin\Application
   Opens:
\label{lem:decomp} Data \\ \mbox{Microsoft} \\ \mbox{CryptnetUrlCache} \\ \mbox{MetaData} \\ \mbox{135BD6A358680A7BF1CCEC7C0172393D} \\ \mbox{Constant Microsoft} \\ \mbox{CryptnetUrlCache} \\ \mbox{MetaData} \\ \mbox
                                              C:\Documents and Settings\Admin\Application
   Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497DD56F57004
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\3130B1871A126520A8C47861EFE3ED4D
                                              C:\Documents and Settings\Admin\Application
   Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\60E31627FDA0A46932B0E5948949F2A5
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\62B5AF9BE9ADC1085C3C56EC07A82BF6
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7396C420A8E1BC1DA97F1AF0D10BAD21
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7B2238AACCEDC3F1FFE8E7EB5F575EC9
   Opens:
                                              C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\8DFDF057024880D7A081AFBF6D26B92F
                                              C:\Documents and Settings\Admin\Application
   Opens:
```

Data\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015

```
Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\A44F4E7CB3133FF765C39A53AD8FCFDD
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\F482C95F83F1B59228F1B1E720F2EDF1
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
 Opens:
1-5-21-1757981266-507921405-1957994488-1003
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
1-5-21-1757981266-507921405-1957994488-1003\6b29ae44e85efac3c72ff4d1865d73f1_fa860dc5-a965-4200-
a9d4-fb930ff1911b
 Opens:
                         \label{lem:condition} 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:\WINDOWS\win.ini
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\brndlog.bak
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
 Opens:
Explorer\brndlog.txt
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Desktop.htt
 Opens:
                         C:\Users\
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\desktop.ini
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Internet}
 Opens:
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\Show Desktop.scf
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Media\ Player}
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\MMC
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Office
 Opens:
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\Office\Excel12.pip
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Office\Recent}
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Office\Recent\Desktop.ini
                         {\tt 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-
 Opens:
5-21-1757981266-507921405-1957994488-1003
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
 Opens:
5-21-1757981266-507921405-1957994488-1003\3ea8a527-1704-4983-8596-ab49c663cca3
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\4f5d6884-c60c-4cd3-906b-3d677949fac1
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\fe1a937a-0ac9-4cf1-978d-5d0742ed2858
                         \label{lem:c:Documents} C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Protect\S-1-
 Opens:
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
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons
                         C:\Documents and Settings\Admin\Application
 Opens:
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
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\SystemCertificates\My\CRLs
                         {\tt C:\Documents\ and\ Settings\Admin\Application}
 Opens:
Data\Microsoft\SystemCertificates\My\CTLs
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Templates
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Windows
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Windows\Themes
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\Windows\Themes\Custom.theme
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Oracle
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Oracle\Java
                         C:\Documents and Settings\Admin\Application Data\Oracle\Java\Uninstall
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Sun
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Sun\Java
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Sun\Java\AU
                         C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment
 Opens:
```

C:\Documents and Settings\Admin\Application

Opens:

```
Data\Sun\Java\Deployment\cache
 Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0
 Opens:
                      C:\Documents and Settings\Admin\Application
Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\1
 Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\10
                      C:\Documents and Settings\Admin\Application
 Opens:
C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\12
                      C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171
                      C:\Documents and Settings\Admin\Application
 Opens:
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
                      C:\Documents and Settings\Admin\Application
 Opens:
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
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c
                      C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c.idx
 Opens:
                      C:\Documents and Settings\Admin\Application
C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\18
 Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19
 Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1
                      C:\Documents and Settings\Admin\Application
 Opens:
Opens:
                      C:\Documents and Settings\Admin\Application
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
Opens:
                      C:\Documents and Settings\Admin\Application
Opens:
                      C:\Documents and Settings\Admin\Application
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 and Settings\Admin\Application
Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\25
 Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\26
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\27
 Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\28
 Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\29
 Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\3
 Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\30
 Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\31
 Opens:
                      C:\Documents and Settings\Admin\Application
Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\33
                      C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\34
 Opens:
                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\35
                      C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\36
                      C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\37
```

```
Opens:
                        C:\Documents and Settings\Admin\Application
Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\39
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\4
                        C:\Documents and Settings\Admin\Application
 Opens:
C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\41
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\42
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\43
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d.idx
                        C:\Documents and Settings\Admin\Application
 Opens:
{\tt Data\Sun\Java\Deployment\cache\6.0\44}
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\45
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\46
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\47
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\48
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\49
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\5
 Opens:
                        C:\Documents and Settings\Admin\Application
Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\51
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\52
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\53
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\54
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\55
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\56
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\57
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\58
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\59
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\6
                        C:\Documents and Settings\Admin\Application
 Opens:
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
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\63
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\7
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\8
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\9
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\host
 Opens:
                        C:\Documents and Settings\Admin\Application
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
 Opens:
Data\Sun\Java\Deployment\deployment.properties
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\ext
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\log
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\security
                        C:\Documents and Settings\Admin\Application
 Opens:
```

```
C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\tmp
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\tmp\si
  Opens:
                                      C:\Documents and Settings\Admin\Application Data\Sun\Java\jre1.7.0_02
  Opens:
                                      C:\Documents and Settings\Admin\Cookies
  Opens:
                                      C:\Documents and Settings\Admin\Cookies\admin@c1.microsoft[2].txt
                                      C:\Documents\ and\ Settings\Admin\Cookies\admin@microsoft[1].txt
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Cookies\admin@rto.microsoft[1].txt
  Opens:
                                      C:\Documents and Settings\Admin\Cookies\admin@search.microsoft[1].txt
                                      {\tt C:\Documents\ and\ Settings\Admin\Cookies\admin@www.microsoft[2].txt}
  Opens:
  Opens:
                                      \label{lem:cokies-admin-ewww.microsoft} C: \verb|\Documents| and Settings-Admin-Cookies-admin-ewww.microsoft[3].txt | C: \verb|\Documents| and Settings-Admin-Ewww.microsoft[3].txt | C: \verb|\Document
  Opens:
                                      C:\Documents and Settings\Admin\Cookies\index.dat
                                      C:\Documents and Settings\Admin\Desktop
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Favorites
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Desktop.ini
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Links
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Links\desktop.ini
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url
                                      C:\Documents and Settings\Admin\Favorites\Links\Suggested Sites.url
  Opens:
  Opens:
                                      {\tt C:\Documents\ and\ Settings\Admin\Favorites\Links\Web\ Slice\ Gallery.url}
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Microsoft Websites
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE Add-on
site.url
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE site on
Microsoft.com.url
                                      C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
  Opens:
At Home.url
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Work.url
  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
  Opens:
                                      C:\Documents and Settings\Admin\IECompatCache\index.dat
                                      C:\Documents and Settings\Admin\IETldCache
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\IETldCache\index.dat
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application Data
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe
                                      C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Adobe\Acrobat
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache\AcroFnt09.1st
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache\Search
                                      C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Adobe\Acrobat\9.0\Updater
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Updater\updater.log
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Color
                                      {\tt 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
  Opens:
                                      {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\Updater6\aum.log
                                      {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
  Opens:
Data\Adobe\Updater6\aumLib.log
                                      C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Updater6\Install
  Opens:
                                      {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\GDIPFONTCACHEV1.DAT
                                      C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\IconCache.db
                                      C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Microsoft
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\CD Burning
                                      C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Microsoft\Credentials
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-1003
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds
                                      {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
  Opens:
Data\Microsoft\Feeds\FeedsStore.feedsdb-ms
```

Data\Sun\Java\Deployment\security\trusted.certs

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
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
                         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^
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Suggested Sites~.feed-ms
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\FBANKAIW
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\FBANKAIW\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\FBANKAIW\fwlink[1]
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Microsoft\Feeds Cache\G4DZ1I7H
                         {\tt 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:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY1QNV
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY1QNV\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY1QNV\fwlink[1]
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\TLMHA51J
                         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
 Opens:
Data\Microsoft\Internet Explorer
                         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
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Custom Settings\Custom0
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Custom Settings\CustomO\install.ins
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Microsoft\Internet Explorer\DOMStore
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\OWORJP5C
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK\www.microsoft[1].xml
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Internet Explorer\DOMStore\index.dat
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Microsoft\Internet Explorer\DOMStore\LQLIM8KB
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\frameiconcache.dat
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Recovery
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Recovery\Active
 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
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{80236AC0-AAD6-11E3-AE20-
08002733366F}.dat
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Recovery\Last Active\{69EE14A0-C276-11E3-AE24-08002733366F}.dat
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\rsoplog.bak
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\rsoplog.txt
                         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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Office
                         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
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Silverlight\mssl.lck
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Windows
                         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
 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\Microsoft\Windows Media\9.0\WMSDKNS.DTD
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML
                         C:\Documents and Settings\Admin\Local Settings\Application Data\Sun
 Opens:
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application\ Data\Sun\Java}
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
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\Local Settings\Application
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\1
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\10
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\13
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Sun\Java\Deployment\cache\6.0\15
 Opens:
                         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
Opens:
                         {\tt 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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
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
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\21
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\22
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\23
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
```

Data\Sun\Java\Deployment\cache\6.0\24

	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\25 Opens: C:\Documents	and	Settings\Admin\Local	Settings\Annlication
Data\Sun\Java\Deployment\cache\6.0\26	unu	Sectings (Maintin (Edear	Sectings (Application
		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\27 Opens: C:\Documents		Settings\Admin\Local	Settings\Annlication
Data\Sun\Java\Deployment\cache\6.0\28		Sectings (Admitteedat	Sectings (Application
·		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\29 Opens: C:\Documents		Settings\Admin\Local	Settings\Annlication
Data\Sun\Java\Deployment\cache\6.0\3	anu	Sectings (AdmitiveDear	Sectings (Application
		${\tt Settings \ Admin \ Local}$	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\30 Opens: C:\Documents		Settings\Admin\Local	Settings\Annlication
Data\Sun\Java\Deployment\cache\6.0\31	unu	Sectings (Mainti Leocal	Sectings (Application
·		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\32 Opens: C:\Documents		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\33		•	
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\34		Settings\Admin\Local	Settings\Application
' '		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\35			
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\36		Settings\Admin\Local	Settings\Application
Opens: C:\Documents	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\37		C-++:\ Adm:-\ L1	C-++i\
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\38		Settings\Admin\Local	Settings (Application
Opens: C:\Documents	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\39 Opens: C:\Documents		Settings\Admin\Local	Settings\Annlication
Data\Sun\Java\Deployment\cache\6.0\4	anu	Sectings (AdmitiveDear	Sectings (Application
·		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\40 Opens: C:\Documents		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\41		•	
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\42	and	Settings\Admin\Local	Settings\Application
' '	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\43		•	
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\44		Settings\Admin\Local	Settings\Application
' '		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\45		C-++:\	C-++:\
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45		Settings\Admin\Local 0542d-6963afcc	Settings\Application
Opens: C:\Documents	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\45` Opens: C:\Documents		0542d-6963afcc.idx Settings\Admin\Local	Sottings\Application
Data\Sun\Java\Deployment\cache\6.0\46		Sectings (Admitive)	Sectings Application
·		${\tt Settings \Admin \Local}$	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\47 Opens: C:\Documents		Settings\Admin\Local	Settings\Annlication
Data\Sun\Java\Deployment\cache\6.0\47		_	Sectings (Application
·		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\47' Opens: C:\Documents		/2e2f-21932044.idx Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\48		•	
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\49		Settings\Admin\Local	Settings\Application
		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\5			
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50		Settings\Admin\Local	Settings\Application
' '		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\51	and	Cottings\Admin\Logal	Cottings \ Annliestion
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\52		Settings\Admin\Local	Settings\Application
Opens: C:\Documents	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\53 Opens: C:\Documents		Settings\Admin\Local	Settings\Annlication
Data\Sun\Java\Deployment\cache\6.0\54		Section woman rocat	accessing what icacion
		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\55 Opens: C:\Documents		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\56		•	
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\57		Settings\Admin\Local	Settings\Application
' '		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\58		•	
Opens: C:\Documents	and	Settings\Admin\Local	Sectings (Application

```
Data\Sun\Java\Deployment\cache\6.0\59
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\6
 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\61
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\62
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\63
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\7
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\7\2bbaaf87-5ca9d237
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
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\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\lastAccessed
                         {\tt 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:
{\tt Data\Sun\Java\Deployment\cache\6.0\tmp}
                         C:\Documents and Settings\Admin\Local Settings\desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History
                         C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\History\History.IE5}
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\desktop.ini
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014031220140313
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings \verb|\History\E5| MSH is to 12014031220140313 \verb|\Index.dat| \\
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings \verb|\History\History\IE5\MSHist012014033120140407\verb|\Lindex.dat| 
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings \verb|\History\History.IE5\MSHist012014041220140413|
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp
                         C:\Documents and Settings\Admin\Local Settings\Temp\296c0.msp
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\AdobeARM.log
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\AdobeARM_NotLocked.log
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ASPNETSetup_00000.log
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ASPNETSetup 00001.log
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\AUCHECK\_PARSER.txt}
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Compatibility Pack
 Opens:
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:
{\tt Settings\Temp\dd\_depcheck\_NETFX\_EXP\_35.txt}
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_dotnetfx35error.txt
                         C:\Documents and Settings\Admin\Local
 Opens:
{\tt Settings\Temp\dd\_dotnetfx35install.txt}
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework20_Setup164F.txt
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework30_Setup16AE.txt
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_NET_Framework35_MSI16E2.txt
 Opens:
                         C:\Documents and Settings\Admin\Local
{\tt Settings\Temp\dd\_NET\_Framework35\_MSI63E0.txt}
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_RGB9RAST_x86.msi601E.txt
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA2A49.txt
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA3565.txt
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA35A0.txt
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_XPS.txt
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\gen_py
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\gen_py\2.7
                         C:\Documents and Settings\Admin\Local Settings\Temp\gen_py\2.7\dicts.dat
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\gen_py\2.7\__init__.py
                         C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\JAUReg.log
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\java_install.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\java_install_reg.log
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\jusched.log
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft PowerPoint
Viewer (0).log
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_10.0.30319
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Opens:
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
                         {\tt 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 Settings\Temp\mmc004AA394.xml
 Opens:
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\pywin32_postinstall.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\setup.log
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\SilverlightO.log
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\SilverlightMSI.log}
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\uxeventlog.txt
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\AntiPhishing
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\AntiPhishing\2CEDBFBC-DBA8-43AA-B1FD-CC8E6316E3E2.dat
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\300lo[1].json
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\300lo[2].json
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\88666cc6-d578-45c8-baf0-89d3837f41c3_89[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\93e33485-fea3-4687-a642-2c5dd233522f_12[1].eot
                         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\Content.IE5\CXCXW1MR\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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\broker[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CA9ATUDW.css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CAMLW29Z.jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\CATM568T.jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CAVLZJ9D.jsx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\core114[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\core114[2].js
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\css[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\css[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\css[3].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\DataList[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
 Opens:
Files\Content.IE5\CXCXW1MR\event[2].js
                         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
 Opens:
Files\Content.IE5\CXCXW1MR\false[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
 Opens:
Files\Content.IE5\CXCXW1MR\georedirect[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
 Opens:
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
 Opens:
Files\Content.IE5\CXCXW1MR\oneMscomBlade[2].css
 Opens:
                         {\tt 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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Opens:
                         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
 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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
Files\Content.IE5\ONWV4FIP\CA39W67Q.jsx
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\ONWV4FIP\CAANG12B.css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\CAU35S9Y.jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\ChangePassword[1].css
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
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
                         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
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 \verb|\| Content.IE5 \verb|\| ONWV4FIP \verb|\| css[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\event[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\event[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\event[6].js
 Opens:
                         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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\js[2].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\is[31.ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[4].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\Login[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\modernizr.wol[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\nb-no[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\omniture_s_code[1].js
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\onemscomfooter[2].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\onemscomsearch[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\oneMscomSocial[2].css
 Opens:
                         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
 Opens:
Files\Content.IE5\ONWV4FIP\ScriptResource[1].axd
                         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
 Opens:
Files\Content.IE5\ONWV4FIP\SearchMSStoreClient[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\serverComponent[1].php
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files \verb|\Content.IE5| ONWV4FIP \verb|\Siteresource[1].ashx|
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\siteresource[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
 Opens:
Files\Content.IE5\ONWV4FIP\true[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
 Opens:
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
                         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
 Opens:
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
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
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\OXMNOBKF\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
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
 Opens:
                         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
 Opens:
Files\Content.IE5\QXMNQBKF\feedback[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\FormView[1].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\GlobalResources[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\Install[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\OXMNOBKF\is[11.ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\js[2].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\js[3].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\OXMNOBKF\is[41.ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\Menu[1].css
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\QXMNQBKF\omnibase[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\oneMscomBlade[2].css
                         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
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\QXMNQBKF\oneMscomSocial[2].css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Files\Content.IE5\QXMNQBKF\script[2].jsx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
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
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\QXMNQBKF\WebResource[1].axd
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\OXMNOBKF\welcome[1].htm
 Opens:
                         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
 Opens:
Files\Content.IE5\UH4D6D6X
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\300lo[1].json
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\auth016[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\broker-config_s1[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[2].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[3].js
                         {\tt C:\Documents\ and\ Settings\backslash Admin\backslash Local\ Settings\backslash Temporary\ Internet}
 Opens:
Files\Content.IE5\UH4D6D6X\broker-config_s1[4].js
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[5].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\broker[2].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA01EFSH.jsx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA7GG9I0.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\CA8VUH6F.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\CAI7MNGV.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\CallingControl[1].aspx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\confirmation[1].aspx
                         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
 Opens:
Files\Content.IE5\UH4D6D6X\Cookies[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
 Opens:
Files\Content.IE5\UH4D6D6X\CreateUserWizard[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\css[1].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\css[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\css[2].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\details-social[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\enable[2].htm
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\event[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\event[5].js
 Opens:
                         {\tt 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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ms[2].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\navcancl[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\oneMscomComponents[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\oneMscomListLayout[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\oneMscomListLayout[3].css
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\UH4D6D6X\oneMscomNav[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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
                                     C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\UH4D6D6X\script[2].jsx
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                                     C:\Documents and Settings\Admin\My Documents
  Opens:
  Opens:
                                     C:\Documents and Settings\Admin\My Documents\desktop.ini
  Opens:
                                     C:\Documents and Settings\Admin\My Documents\My Music
  Opens:
                                     C:\Documents and Settings\Admin\My Documents\My Music\Desktop.ini
  Opens:
                                     C:\Documents and Settings\Admin\My Documents\My Music\Sample Music.lnk
  Opens:
                                     C:\Documents and Settings\Admin\My Documents\My Pictures
  Opens:
                                     C:\Documents and Settings\Admin\My Documents\My Pictures\Desktop.ini
  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
                                     C:\Documents and Settings\Admin\ntuser.ini
  Opens:
  Opens:
                                     C:\Documents and Settings\Admin\PrintHood
  Opens:
                                     C:\Documents and Settings\Admin\PrivacIE
                                     {\tt C:\Documents\ and\ Settings\Admin\PrivacIE\index.dat}\\
  Opens:
  Opens:
                                     C:\Documents and Settings\Admin\Recent
                                     C:\Documents and Settings\Admin\Recent\Desktop.ini
  Opens:
                                     \label{localization} C: \verb|\Documents| and Settings\\| Admin\\| Recent\\| fp\_11.0.1.152\_| archive.lnk|| archive.lnk|
  Opens:
  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
                                     C:\Documents and Settings\Admin\SendTo\My Documents.mydocs
  Opens:
  Opens:
                                     C:\Documents and Settings\Admin\Start Menu
  Opens:
                                     C:\Documents and Settings\Admin\Start Menu\desktop.ini
                                     C:\Documents and Settings\Admin\Start Menu\Programs
  Opens:
  Opens:
                                     C:\Documents and Settings\Admin\Start Menu\Programs\Accessories
                                     C:\Documents and Settings\Admin\Start
  Opens:
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
  Opens:
                                     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
  Opens:
                                     C:\Documents and Settings\Admin\Start
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
 Opens:
                         C:\Documents and Settings\Admin\Templates\quattro.wb2
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Templates\wordpfct.wpd}
 Opens:
                         C:\Documents and Settings\Admin\Templates\wordpfct.wpg
 Opens:
                         C:\Documents and Settings\Administrator
 Opens:
                         C:\Documents and Settings\Administrator\Application Data
 Opens:
                         C:\Documents and Settings\Administrator\Application Data\desktop.ini
                         C:\Documents and Settings\Administrator\Application Data\Microsoft
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Application
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
                         C:\Documents and Settings\Administrator\Application
 Opens:
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
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
                         C:\Documents and Settings\Administrator\Desktop
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Favorites
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings
                         C:\Documents and Settings\Administrator\Local Settings\Application Data
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Credentials
                         {\tt C:\Documents\ and\ Settings\Administrator\Local\ Settings\Application}
 Opens:
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-500
                         C:\Documents and Settings\Administrator\Local Settings\Application
 Opens:
Data\Microsoft\Media Player
                         C:\Documents and Settings\Administrator\Local Settings\Application
 Opens:
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
                         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:
                         C:\Documents and Settings\Administrator\Local Settings\History
 Opens:
                         C:\Documents and Settings\Administrator\Local
Settings\History\desktop.ini
 Opens:
                         C:\Documents and Settings\Administrator\Local
```

```
Settings\History\History.IE5
                         C:\Documents and Settings\Administrator\Local
 Opens:
Settings\History\History.IE5\desktop.ini
 Opens:
                         C:\Documents and Settings\Administrator\Local
Settings\History\History.IE5\index.dat
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Temp
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Opens:
Internet Files\Content.IE5\CXCXW1MR
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
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
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\desktop.ini
                         C:\Documents and Settings\Administrator\My Documents
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\NetHood
                         C:\Documents and Settings\Administrator\NTUSER.DAT
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\NTUSER.DAT.LOG
 Opens:
                         C:\Documents and Settings\Administrator\ntuser.ini
 Opens:
                         C:\Documents and Settings\Administrator\PrintHood
 Opens:
                         C:\Documents and Settings\Administrator\Recent
 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:
                         C:\Documents and Settings\Administrator\SendTo\Mail Recipient.MAPIMail
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu\desktop.ini
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu\Programs
 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
 Opens:
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
 Opens:
                         C:\Documents and Settings\Administrator\Start
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
```

```
Opens:
                        C:\Documents and Settings\Administrator\Start Menu\Programs\Remote
Assistance.lnk
 Opens:
                        C:\Documents and Settings\Administrator\Start Menu\Programs\Startup
                        C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Startup\desktop.ini
 Opens:
                        C:\Documents and Settings\Administrator\Start Menu\Programs\Windows
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
                        C:\Documents and Settings\Administrator\Templates\presenta.shw
 Opens:
 Opens:
                        Opens:
                        C:\Documents and Settings\Administrator\Templates\wordpfct.wpd
                        C:\Documents and Settings\Administrator\Templates\wordpfct.wpg
 Opens:
 Opens:
                        C:\Documents and Settings\All Users
                        C:\Documents and Settings\All Users\Application Data
 Opens:
                        C:\Documents and Settings\All Users\Application Data\Adobe
 Opens:
 Opens:
                        C:\Documents and Settings\All Users\Application Data\Adobe\Acrobat
 Opens:
                        C:\Documents and Settings\All Users\Application Data\Adobe\Acrobat\9.0
                        C:\Documents and Settings\All Users\Application
 Opens:
Data\Adobe\Acrobat\9.0\Replicate
                        C:\Documents and Settings\All Users\Application
 Opens:
Data\Adobe\Acrobat\9.0\Replicate\Security
                        C:\Documents and Settings\All Users\Application
 Opens:
Data\Adobe\Acrobat\9.0\Replicate\Security\directories.acrodata
                        C:\Documents and Settings\All Users\Application Data\Adobe\Reader
 Opens:
 Opens:
                        Opens:
                        C:\Documents and Settings\All Users\Application Data\Adobe\Reader\9.4
                        C:\Documents and Settings\All Users\Application
 Opens:
Data\Adobe\Reader\9.4\ARM
 Opens:
                        C:\Documents and Settings\All Users\Application
Data\Adobe\Reader\9.4\ARM\AdbeRdrUpd951_all_incr.msp
                        C:\Documents and Settings\All Users\Application
Data\Adobe\Reader\9.4\ARM\AdbeRdrUpd952_all_incr.msp
                        C:\Documents and Settings\All Users\Application
 Opens:
Data\Adobe\Reader\9.4\ARM\AdbeRdrUpd953_all_incr.msp
 Writes to:
                        C:\WINDOWS\system32\Packet.dll
                        C:\WINDOWS\system32\wpcap.dll
 Writes to:
                        C:\WINDOWS\system32\drivers\npf.sys
 Writes to:
 Reads from:
                        C:\AUTOEXEC.BAT
                        C:\boot.ini
 Reads from:
                        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
Data\Adobe\Acrobat\9.0\AdobeSysFnt09.1st
                        C:\Documents and Settings\Admin\Application
 Reads from:
Data\Adobe\Acrobat\9.0\JavaScripts\glob.js
                        C:\Documents and Settings\Admin\Application
 Reads from:
Data\Adobe\Acrobat\9.0\JavaScripts\glob.settings.js
 Reads from:
                        C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\SharedDataEvents
 Reads from:
                        C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\UserCache.bin
 Reads from:
                        C:\Documents and Settings\Admin\Application Data\desktop.ini
 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
 Reads from:
Data\Microsoft\CryptnetUrlCache\Content\0797C381B2F87EB5A1D5573BD15BA4F4
                        C:\Documents and Settings\Admin\Application
 Reads from:
Data\Microsoft\CryptnetUrlCache\Content\135BD6A358680A7BF1CCEC7C0172393D
 Reads from:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004
                        C:\Documents and Settings\Admin\Application
 Reads from:
Data\Microsoft\CryptnetUrlCache\Content\3130B1871A126520A8C47861EFE3ED4D
                        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
                        C:\Documents and Settings\Admin\Application
 Reads from:
Data\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D49D759AD
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7396C420A8E1BC1DA97F1AF0D10BAD21
 Reads from:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE8E7EB5F575EC9
 Reads from:
                        C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\8DFDF057024880D7A081AFBF6D26B92F
                        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\MetaData\0797C381B2F87EB5A1D5573BD15BA4F4
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\135BD6A358680A7BF1CCEC7C0172393D
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497DD56F57004
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\3130B1871A126520A8C47861EFE3ED4D
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\60E31627FDA0A46932B0E5948949F2A5
 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-
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
 Reads from:
                         C:\WINDOWS\win.ini
 Reads from:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\brndlog.bak
 Reads from:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
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
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
 Reads from:
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
                         {\tt 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
                         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-
 Reads from:
5-21-1757981266-507921405-1957994488-1003\3ea8a527-1704-4983-8596-ab49c663cca3
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\4f5d6884-c60c-4cd3-906b-3d677949fac1
 Reads from:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
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
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons\SP_6A65DB879F95470886BD7EFE4977B10E.dat
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Windows\Themes\Custom.theme
                         C:\Documents and Settings\Admin\Application
 Reads from:
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171
                         C:\Documents and Settings\Admin\Application
 Reads from:
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171.idx
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c
                         C:\Documents and Settings\Admin\Application
 Reads from:
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c.idx
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-6.0.lap
 Reads from:
                         C:\Documents and Settings\Admin\Application
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
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-6.0.lap
 Reads from:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d
                         C:\Documents and Settings\Admin\Application
 Reads from:
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d.idx
```

C:\Documents and Settings\Admin\Application

Reads from:

```
Reads from:
                                     C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\lastAccessed
  Reads from:
                                     C:\Documents and Settings\Admin\Application
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
  Reads from:
                                     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:
                                     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-ewww.microsoft} C: \verb|\Documents| and Settings-Admin-Cookies-admin-ewww.microsoft[3].txt | C: \verb|\Documents| and Settings-Admin-Ewww.microsoft[3].txt | C: \verb|\Document
  Reads from:
                                     C:\Documents and Settings\Admin\Cookies\index.dat
                                     C:\Documents and Settings\Admin\Favorites\Desktop.ini
  Reads from:
  Reads from:
                                     C:\Documents and Settings\Admin\Favorites\Links\desktop.ini
  Reads from:
                                     C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url
                                     {\tt C:\Documents\ and\ Settings\Admin\Favorites\Links\Suggested\ Sites.url}
  Reads from:
  Reads from:
                                     C:\Documents and Settings\Admin\Favorites\Links\Web Slice Gallery.url
  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
                                     C:\Documents and Settings\Admin\Favorites\MSN.com.url
  Reads from:
  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
  Reads from:
                                     C:\Documents and Settings\Admin\Local Settings\Application
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
  Reads from:
                                     {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
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
  Reads from:
                                     {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Feeds\FeedsStore.feedsdb-ms
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Reads from:
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
  Reads from:
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-
  Reads from:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\desktop.ini
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\FBANKAIW\desktop.ini
  Reads from:
                                     {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Feeds Cache\FBANKAIW\fwlink[1]
  Reads from:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\G4DZ1I7H\desktop.ini
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Reads from:
Data\Microsoft\Feeds Cache\G4DZ1I7H\fwlink[1]
  Reads from:
                                     {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Feeds Cache\index.dat
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Reads from:
Data\Microsoft\Feeds Cache\J3XY1QNV\desktop.ini
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY10NV\fwlink[1]
  Reads from:
                                     C:\Documents and Settings\Admin\Local Settings\Application
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]
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\brndlog.bak
  Reads from:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\brndlog.txt
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Reads from:
```

Data\Microsoft\Internet Explorer\Custom Settings\Custom0\install.ins

```
Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK\www.microsoft[1].xml
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
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
 Reads from:
                        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
 Reads from:
Data\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{80236AC0-AAD6-11E3-AE20-
08002733366F}.dat
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
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
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
{\tt Data\Microsoft\Silverlight\mssl.lck}
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD
                        {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Reads from:
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc.idx
 Reads from:
                        C:\Documents and Settings\Admin\Local Settings\Application
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\7\2bbaaf87-5ca9d237
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Sun\Java\Deployment\cache\6.0\7\2bbaaf87-5ca9d237.idx
                        C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
C:\Documents and Settings\Admin\Local Settings\desktop.ini
 Reads from:
                        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
                        C:\Documents and Settings\Admin\Local
Settings \verb|\History\History\IE5\MSHist012014031220140313\lindex.dat
 Reads from:
                        C:\Documents and Settings\Admin\Local
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
                        C:\Documents and Settings\Admin\Local Settings\Temp\AdobeARM.log
 Reads from:
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\AdobeARM_NotLocked.log
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ASPNETSetup_00000.log
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ASPNETSetup_00001.log
 Reads from:
                        {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\AUCHECK\_PARSER.txt}
                        C:\Documents and Settings\Admin\Local Settings\Temp\Compatibility Pack
 Reads from:
for the 2007 Office system (0).log
                        C:\Documents and Settings\Admin\Local Settings\Temp\dd_clwireg.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\dd_depcheck_NETFX_EXP_35.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\dd_dotnetfx35error.txt
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\dd_dotnetfx35install.txt
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\dd_NET_Framework20_Setup164F.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework30_Setup16AE.txt
                        C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\dd_NET_Framework35_MSI16E2.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework35_MSI63E0.txt
 Reads from:
                        C:\Documents and Settings\Admin\Local
Settings\Temp\dd_RGB9RAST_x86.msi601E.txt
                        C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA2A49.txt
 Reads from:
 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:
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\gen_py\2.7\dicts.dat
 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
                          C:\Documents and Settings\Admin\Local Settings\Temp\java_install_reg.log
 Reads from:
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\jusched.log
 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
                          \hbox{$\tt C:\Documents$ and Settings\Admin\Local Settings\Temp\Microsoft\ Visual\ C++$}
 Reads from:
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:
                          C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_152314679.html
                          C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Reads from:
2010 x86 Redistributable Setup_20140312_152634747-MSI_vc_red.msi.txt
                          C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Reads from:
2010 x86 Redistributable Setup_20140312_152634747.html
                          C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Reads from:
2010 x86 Redistributable Setup_20140312_154212618-MSI_vc_red.msi.txt
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Microsoft\ Visual\ C++}\\
 Reads from:
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\Silverlight0.log
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\SilverlightMSI.log}
 Reads from:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\uxeventlog.txt}
 Reads from:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\AntiPhishing\2CEDBFBC-DBA8-43AA-B1FD-CC8E6316E3E2.dat
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\300lo[1].json
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files \verb|\CONTENT.IE5| CXCXW1MR \verb|\300lo[2].json| \\
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\88666cc6-d578-45c8-baf0-89d3837f41c3_89[1].css
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\93e33485-fea3-4687-a642-2c5dd233522f_12[1].eot
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[1].txt
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\| Content.IE5 \verb|\| CXCXW1MR \verb|\| ADSAdClient31[2].txt|
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[3].txt
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[4].txt
                          {\tt 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
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\auth016[1].js
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\CXCXW1MR\bimapping[2].js
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\broker[1].js
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CA9ATUDW.css
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\CAMLW29Z.jsx
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CATM568T.jsx
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CAVLZJ9D.jsx
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\core114[1].js
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\core114[2].js
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\css[1].css
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\DataList[1].css
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
                         {\tt 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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\js[2].ashx
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\omnibase[2].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomBlade[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\onemscomfooter[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\request[1].php
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\ScriptResource[1].axd
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\CXCXW1MR\ScriptResource[2].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\ScriptResource[3].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\ScriptResource[4].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\ScriptResource[5].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\script[2].jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\true[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\true[2].htm
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\views[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\CXCXW1MR\WebResource[1].axd| \\
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\wtid[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\736e3781-6a19-4119-b717-e61f0d8982c0_12[1].eot
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\ONWV4FIP\auth016[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\broker-config_s1[1].js
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\ONWV4FIP\broker-config_s1[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\broker-config_s1[3].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\CA39W67Q.jsx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         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\Content.IE5\ONWV4FIP\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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\css[2].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\details[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\details[2].htm
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\event[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
 Reads from:
                         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
 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[11.css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[3].ashx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[4].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\Login[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\modernizr.wol[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\nb-no[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\omniture_s_code[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\onemscomfooter[2].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\onemscomsearch[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\oneMscomSocial[2].css
                         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
                         {\tt 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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\SearchMSStoreClient[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\style[1].cssx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\Tracker[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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\QXMNQBKF\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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ADSAdClient31[1].txt
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ADSAdClient31[2].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\auth016[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\broker-config_s1[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\broker-config_s1[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\broker-config_s1[3].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\broker-config_s2[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\bullet[1]
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\CA9P88JQ.css
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\QXMNQBKF\core114[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\counter017[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\counter017[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\css[1].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\gl_site[1].svg
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\Import[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\omnibase[2].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         {\tt 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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\ScriptResource[1].axd
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\QXMNQBKF\script[1].jsx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\uninstall-arp-win[1].htm
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\WebResource[1].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\Content.IE5| QXMNQBKF| welcome[1].htm|
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\QXMNQBKF\windows8_site_ltr[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\300lo[1].json
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\Content.IE5\UH4D6D6X\300lo[2].json|
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ADSAdClient31[1].txt
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\adServer[1].htm
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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]
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[4].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[5].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA01EFSH.jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\CA7GG9I0.css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA8VUH6F.css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\counter017[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\CreateUserWizard[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\css[1].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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\Content.IE5\UH4D6D6X\enable[2].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\event[3].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\info 48[1]
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\internet-explorer-8-details[1].htm
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\js[1].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\Marquee[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ms[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\navcanc1[2]
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\oneMscomComponents[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\oneMscomListLayout[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\Content.IE5\UH4D6D6X\oneMscomListLayout[3].css|
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\oneMscomNav[2].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\pre_broker[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\Content.IE5\UH4D6D6X\ScriptResource[1].axd|
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ScriptResource[21.axd
 Reads from:
                         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
 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
 Reads from:
                         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
 Reads from:
Files\Content.IE5\UH4D6D6X\webtrends[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\UH4D6D6X\wt[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\My Documents\desktop.ini
                         C:\Documents and Settings\Admin\My Documents\My Music\Desktop.ini
 Reads from:
 Reads from:
                         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:
                         C:\Documents and Settings\Admin\My Documents\My Pictures\Sample
Pictures.lnk
                         C:\Documents and Settings\Admin\ntuser.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\PrivacIE\index.dat
                         C:\Documents and Settings\Admin\Recent\Desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Recent\fp_11.0.1.152_archive.lnk
 Reads from:
                         C:\Documents and Settings\Admin\SendTo\Compressed (zipped)
Folder.ZFSendToTarget
                         C:\Documents and Settings\Admin\SendTo\Desktop (create
 Reads from:
shortcut).DeskLink
                         C:\Documents and Settings\Admin\SendTo\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\SendTo\Mail Recipient.MAPIMail
 Reads from:
                         C:\Documents and Settings\Admin\SendTo\My Documents.mydocs
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\desktop.ini
                         C:\Documents and Settings\Admin\Start
 Reads from:
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
                        C:\Documents and Settings\Admin\Start
 Reads from:
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
 Reads from:
                        C:\Documents and Settings\Admin\Start
{\tt 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
 Reads from:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
                        C:\Documents and Settings\Admin\Start
 Reads from:
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
 Reads from:
                        C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Notepad.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Program
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
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Windows
 Reads from:
Explorer.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Internet
Explorer.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Outlook Express.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Remote
Assistance.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Startup\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Windows Media
Player.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Templates\amipro.sam
 Reads from:
                         C:\Documents and Settings\Admin\Templates\lotus.wk4
 Reads from:
                         C:\Documents and Settings\Admin\Templates\presenta.shw
 Reads from:
                         C:\Documents and Settings\Admin\Templates\quattro.wb2
 Reads from:
                         C:\Documents and Settings\Admin\Templates\wordpfct.wpd
 Reads from:
                         C:\Documents and Settings\Admin\Templates\wordpfct.wpg
 Reads from:
                         C:\Documents and Settings\Administrator\Application Data\desktop.ini
                         C:\Documents and Settings\Administrator\Application
 Reads from:
Data\Microsoft\Internet Explorer\brndlog.bak
                         C:\Documents and Settings\Administrator\Application
 Reads from:
Data\Microsoft\Internet Explorer\brndlog.txt
                         C:\Documents and Settings\Administrator\Cookies\index.dat
 Reads from:
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Administrator\Local\ Settings\Application}
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
 Reads from:
                         C:\Documents and Settings\Administrator\Local Settings\Application
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:
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\CXCXW1MR\desktop.ini
 Reads from:
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
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
 Reads from:
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\QXMNQBKF\desktop.ini
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Reads from:
Internet Files\Content.IE5\UH4D6D6X\desktop.ini
                         C:\Documents and Settings\Administrator\Local Settings\Temporary
 Reads from:
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
                         C:\Documents and Settings\Administrator\SendTo\Desktop (create
 Reads from:
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
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
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
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
Menu\Programs\Accessories\Entertainment\desktop.ini
 Reads from:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Notepad.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Program Compatibility Wizard.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
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
Menu\Programs\Accessories\Windows Explorer.lnk
                         C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini
 Reads from:
 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:
                         {\tt 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
                         C:\Documents and Settings\All Users\Application
Reads from:
                         C:\Documents and Settings\All Users\Application
Data\Adobe\Reader\9.4\ARM\AdbeRdrUpd951_all_incr.msp
 Reads from:
                         C:\Documents and Settings\All Users\Application
Data\Adobe\Reader\9.4\ARM\AdbeRdrUpd952_all_incr.msp
                         C:\Documents and Settings\All Users\Application
Data\Adobe\Reader\9.4\ARM\AdbeRdrUpd953_all_incr.msp
```

Network Events

C:\WINDOWS\Temp\tmp.exe

Connects to:	107 0 0 1 1000
	127.0.0.1:1039
Connects to:	46.126.72.20:80
Connects to:	127.0.0.1:1042
Connects to:	93.116.22.220:80
Connects to:	127.0.0.1:1045
Connects to:	123.110.243.219:80
	127.0.0.1:1048
Connects to:	
Connects to:	220.87.228.219:80
Connects to:	127.0.0.1:1051
Connects to:	78.84.133.219:80
Connects to:	127.0.0.1:1054
Connects to:	46.236.173.218:80
Connects to:	127.0.0.1:1057
Connects to:	178.233.254.221:80
Connects to:	127.0.0.1:1060
Connects to:	106.205.155.218:80
Connects to:	127.0.0.1:1063
Connects to:	88.192.173.13:80
Connects to:	127.0.0.1:1066
Connects to:	88.206.93.17:80
Connects to:	127.0.0.1:1069
Connects to:	
	89.114.116.17:80
Connects to:	127.0.0.1:1072
Connects to:	46.56.65.19:80
Connects to:	127.0.0.1:1075
Connects to:	120.205.133.20:80
Connects to:	127.0.0.1:1078
Connects to:	202.69.41.22:80
Connects to:	127.0.0.1:1081
Connects to:	27.4.103.23:80
Connects to:	127.0.0.1:1084
Connects to:	219.198.196.23:80
Connects to:	127.0.0.1:1087
Connects to:	111.125.235.23:80
Connects to:	127.0.0.1:1090
Connects to:	106.3.45.24:80
Connects to:	127.0.0.1:1093
Connects to:	78.139.246.24:80
Connects to:	127.0.0.1:1096
Connects to:	210.124.176.4:80
Connects to:	113.60.130.42:80
Sends data to:	127.0.0.1:1039
Sends data to:	46.126.72.20:80
Sends data to:	127.0.0.1:1042
Sends data to:	93.116.22.220:80
Sends data to:	127.0.0.1:1045
Sends data to:	123.110.243.219:80
Sends data to:	127.0.0.1:1048
Sends data to:	220.87.228.219:80
Sends data to:	127.0.0.1:1051
Sends data to:	78.84.133.219:80
	127.0.0.1:1054
Sends data to:	
Canda data tar	
Sends data to:	46.236.173.218:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057
Sends data to: Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80
Sends data to: Sends data to: Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060
Sends data to: Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80
Sends data to: Sends data to: Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060
Sends data to: Sends data to: Sends data to: Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081 27.4.103.23:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081 27.4.103.23:80 127.0.0.1:1084 219.198.196.23:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081 27.4.103.23:80 127.0.0.1:1084 219.198.196.23:80 127.0.0.1:1087
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081 27.4.103.23:80 127.0.0.1:1084 219.198.196.23:80 127.0.0.1:1087 111.125.235.23:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081 27.4.103.23:80 127.0.0.1:1084 219.198.196.23:80 127.0.0.1:1087 111.125.235.23:80 127.0.0.1:1087
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1084 219.198.196.23:80 127.0.0.1:1087 111.125.235.23:80 127.0.0.1:1087 111.125.235.23:80 127.0.0.1:1090 106.3.45.24:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081 27.4.103.23:80 127.0.0.1:1084 219.198.196.23:80 127.0.0.1:1087 111.125.235.23:80 127.0.0.1:1090 106.3.45.24:80 127.0.0.1:1093
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081 27.4.103.23:80 127.0.0.1:1084 219.198.196.23:80 127.0.0.1:1087 111.125.235.23:80 127.0.0.1:1089 106.3.45.24:80 127.0.0.1:1093 78.139.246.24:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081 27.4.103.23:80 127.0.0.1:1084 219.198.196.23:80 127.0.0.1:1087 111.125.235.23:80 127.0.0.1:1090 106.3.45.24:80 127.0.0.1:1093 78.139.246.24:80 127.0.0.1:1096
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081 27.4.103.23:80 127.0.0.1:1084 219.198.196.23:80 127.0.0.1:1087 111.125.235.23:80 127.0.0.1:1093 78.139.246.24:80 127.0.0.1:1093 78.139.246.24:80 127.0.0.1:1096 210.124.176.4:80
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081 27.4.103.23:80 127.0.0.1:1084 219.198.196.23:80 127.0.0.1:1087 111.125.235.23:80 127.0.0.1:1090 106.3.45.24:80 127.0.0.1:1093 78.139.246.24:80 127.0.0.1:1096
Sends data to:	46.236.173.218:80 127.0.0.1:1057 178.233.254.221:80 127.0.0.1:1060 106.205.155.218:80 127.0.0.1:1063 88.192.173.13:80 127.0.0.1:1066 88.206.93.17:80 127.0.0.1:1069 89.114.116.17:80 127.0.0.1:1072 46.56.65.19:80 127.0.0.1:1075 120.205.133.20:80 127.0.0.1:1078 202.69.41.22:80 127.0.0.1:1081 27.4.103.23:80 127.0.0.1:1084 219.198.196.23:80 127.0.0.1:1087 111.125.235.23:80 127.0.0.1:1093 78.139.246.24:80 127.0.0.1:1093 78.139.246.24:80 127.0.0.1:1096 210.124.176.4:80

Receives data from: 46.126.72.20:80 Receives data from: 127.0.0.1:1043 Receives data from: 127.0.0.1:1046 Receives data from: 123.110.243.219:80 Receives data from: 127.0.0.1:1049 Receives data from: 220.87.228.219:80 Receives data from: 127.0.0.1:1052 78.84.133.219:80 Receives data from: Receives data from: 127.0.0.1:1055 Receives data from: 46.236.173.218:80 Receives data from: 127.0.0.1:1058 Receives data from: 178.233.254.221:80 Receives data from: 127.0.0.1:1061 Receives data from: 106.205.155.218:80 Receives data from: 127.0.0.1:1064 Receives data from: 88.192.173.13:80 Receives data from: 127.0.0.1:1067 Receives data from: 88.206.93.17:80 Receives data from: 127.0.0.1:1070 Receives data from: 89.114.116.17:80 Receives data from: 127.0.0.1:1073 Receives data from: 46.56.65.19:80 Receives data from: 127.0.0.1:1076 Receives data from: 120.205.133.20:80 Receives data from: 127.0.0.1:1079 202.69.41.22:80 Receives data from: Receives data from: 127.0.0.1:1082 Receives data from: 127.0.0.1:1085 127.0.0.1:1088 Receives data from: Receives data from: 111.125.235.23:80 Receives data from: 127.0.0.1:1091 Receives data from: 106.3.45.24:80 Receives data from: 127.0.0.1:1094 Receives data from: 78.139.246.24:80 Receives data from: 127.0.0.1:1097 Receives data from: 210.124.176.4:80

Windows Registry Events

Creates key:

Creates key.	Tike in the system red in enticontributs et vices (tepip) par ameter s
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
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:	HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Creates key:	HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders	
Creates key:	HKLM\software\microsoft\windows\currentversion\explorer\shell folders
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>
options\70b2225f430facf3	1ca65621c234f09e.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:	<pre>HKCU\software\policies\microsoft\windows\safer\codeidentifiers</pre>
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>
options\msvcrt.dll	
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>
options\gdi32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll	
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ulib.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cfgmgr32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\setupapi.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ifsutil.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution

HKLM\system\currentcontrolset\services\tcpip\parameters

options\ufat.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\comdlg32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mfc42u.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcp60.dll $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows nt + current version + image file execution$ Opens key: options\ole32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\mmcbase.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcns4.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winspool.drv HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\sqlunirl.dll Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: HKLM\software\microsoft\windows nt\currentversion\windows Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon HKI M\ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics 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\ Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ control panel\+ desktop$ HKCU\control panel\desktop Opens key: Opens kev: HKLM\svstem\setup Opens key: HKLM\system\currentcontrolset\control\minint Opens key: HKLM\system\wpa\pnp Opens key: HKLM\software\microsoft\windows\currentversion\setup Opens key: ${\it HKLM \ } software \ \\ microsoft \ \\ windows \ \\ current version$ Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels Opens key: HKLM\svstem\currentcontrolset\control\computername\activecomputername Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: HKLM\software\policies\microsoft\system\dnsclient Opens key: HKLM\hardware\description\system Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced}} \\$ HKLM\software\microsoft\windows nt\currentversion\languagepack Opens key: Opens key: HKLM\software\microsoft\ole Opens key: HKCR\interface Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046} Opens key: HKLM\software\microsoft\oleaut Opens key: HKLM\software\microsoft\oleaut\userera Opens key: HKLM\system\currentcontrolset\control\wmi\security Opens key: HKCU\software\microsoft\microsoft sal server\80\tools\client Opens key: HKCU\software\microsoft\microsoft sql server\80\tools\sqlstr Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\nddeapi.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\cmutil.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cmpbk32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cmdial32.dll 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 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dnsapi.dll Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution 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 key:
                       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\normaliz.dll
 Opens kev:
                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
 Opens key:
                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
 Opens key:
                       HKCU\software\classes\
 Opens key:
                       HKCU\software\classes\protocols\name-space handler\
                       HKCR\protocols\name-space handler
 Opens kev:
 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
 Opens key:
                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
                       HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key:
                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
 Opens key:
                       \label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ internet explorer \+ main \+ feature control
 Opens key:
                       HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
 Opens key:
                       HKLM\software\microsoft\internet explorer\main\featurecontrol
 Opens key:
                       HKCU\software\microsoft\internet explorer\main\featurecontrol
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
                       HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
 Opens key:
                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
 Opens key:
                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                       \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\zonemap\ranges\
                       HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\ranges\
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key:
                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
                       HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens kev:
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
 Opens key:
```

Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
Opens key:
Opens key:
Opens key:
HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\hnetcfg.dll
  Opens key:
                                   HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:
                                   HKLM\software\microsoft\rpc
                                   \label{lem:hklmsoftware} \begin{tabular}{ll} \hline HKLM\software\mbox{\sc microsoft\windows} & nt\current\sc version\mbox{\sc microsoft\windows} \\ \hline \end{tabular}
  Opens key:
options\70b2225f430facf31ca65621c234f09e.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
                                   HKCU\software
  Opens key:
  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\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\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
                                   HKCU\software\adobe\acrobat reader\9.0\avconversiontopdf
  Opens key:
  Opens key:
                                   HKCU \ software \ a dobe \ a crobat \ reader \ \ 9.0 \ avconversion topd f \ \ csettings
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\avdisplay
                                   HKCU\software\adobe\acrobat reader\9.0\avgeneral
  Opens key:
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\avgeneral\cdockables
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars
                                   HKCU\software\adobe\acrobat
  Opens key:
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
                                   HKCU\software\adobe\acrobat reader\9.0\collab
  Opens key:
  Opens key:
                                   \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \adobe \acrobat reader \end{tabular} $0 \cap 1 $ \collab \cdocument center \end{tabular} $0 \cap 1 $ \cdocument \cdoc
                                   HKCU\software\adobe\acrobat reader\9.0\collab\cdocumentcenter\csettings
  Opens kev:
                                   HKCU\software\adobe\acrobat reader\9.0\collab\cemaildistribution
  Opens key:
                                   HKCU\software\adobe\acrobat
  Opens kev:
reader\9.0\collab\cemaildistribution\csettings
                                   HKCU\software\adobe\acrobat
  Opens key:
reader\9.0\collab\cinitiationwizardfirstlaunch
  Opens kev:
                                   HKCU\software\adobe\acrobat reader\9.0\collab\cserversettings
                                   \label{lem:hkcu} \mbox{HKCU\software\adobe\acrobat reader\9.0\formsprefs}
  Opens key:
  Opens key:
                                   HKCU \setminus software \setminus adobe \setminus acrobat \ reader \setminus 9.0 \setminus formsprefs \setminus crequired field hlcolor
                                   HKCU\software\adobe\acrobat reader\9.0\formsprefs\cruntimebgidlecolor
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\fullscreen
  Opens key:
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\handtool
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\installer
                                   HKCU\software\adobe\acrobat reader\9.0\installer\migrated
  Opens key:
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\installpath
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\jsprefs
                                   HKCU\software\adobe\acrobat reader\9.0\language
  Opens key:
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\language\current
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\language\next
  Opens key:
                                   \label{lem:hkcu} \verb+KCU \software \adobe \acrobat reader \9.0 \mbox{ multimedia}
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\multimedia\ccolorandborder
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\optionalcontent
                                   HKCU\software\adobe\acrobat reader\9.0\originals
  Opens key:
  Opens key:
                                   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
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\selection
  Opens key:
                                   HKCU\software\adobe\acrobat reader\9.0\usagemeasurement
                                   HKCU\software\adobe\adobe acrobat
  Opens key:
  Opens key:
                                   HKCU\software\adobe\adobe acrobat\9.0
  Opens key:
                                   HKCU\software\adobe\adobe acrobat\9.0\diskcabs
  Opens key:
                                   HKCU\software\adobe\adobe arm
  Opens key:
                                   HKCU\software\adobe\adobe arm\1.0
```

HKCU\software\adobe\adobe arm\1.0\arm

HKCU\software\adobe\adobe synchronizer

Opens key: Opens key:

```
Opens key:
                                                                                          HKCU\software\adobe\adobe synchronizer\9.0
      Opens key:
                                                                                          HKCU\software\adobe\adobe synchronizer\9.0\acrobat.com
      Opens key:
                                                                                          HKCU\software\adobe\commonfiles
      Opens key:
                                                                                          HKCU\software\adobe\commonfiles\usage
                                                                                          HKCU\software\adobe\commonfiles\usage\demographic
      Opens key:
      Opens key:
                                                                                          HKCU\software\adobe\commonfiles\usage\reader 9
      Opens key:
                                                                                          HKCU\software\intel
                                                                                          HKCU\software\intel\indeo
      Opens key:
      Opens key:
                                                                                          HKCU\software\intel\indeo\4.1
      Opens key:
                                                                                          HKCU\software\javasoft
                                                                                          HKCU\software\javasoft\java update
      Opens key:
      Opens key:
                                                                                          HKCU\software\javasoft\java update\policy
      Opens key:
                                                                                          HKCU\software\javasoft\prefs
      Opens key:
                                                                                          HKCU\software\macromedia
      Opens key:
                                                                                          HKCU\software\macromedia\flashplayer
      Opens key:
                                                                                          HKCU\software\macromedia\flashplayerupdate
      Opens kev:
                                                                                          HKCU\software\microsoft
      Opens key:
                                                                                          HKCU\software\microsoft\active setup
      Opens key:
                                                                                          HKCU\software\microsoft\active setup\installed components
                                                                                          Opens key:
0ee0-4f90-8827-78cefb8f4988}
                                                                                          HKCU\software\microsoft\active setup\installed components\>{26923b43-
      Opens key:
4d38-484f-9b9e-de460746276c}
      Opens key:
                                                                                          HKCU\software\microsoft\active setup\installed components\>{60b49e34-
c7cc-11d0-8953-00a0c90347ff}
                                                                                          HKCU\software\microsoft\active setup\installed components\>{60b49e34-
      Opens key:
c7cc-11d0-8953-00a0c90347ff}micros
                                                                                          HKCU\software\microsoft\active setup\installed components\>{881dd1c5-
      Opens key:
3dcf-431b-b061-f3f88e8be88a}
                                                                                          Opens key:
ebff-11cf-b6fd-00aa00b4e220}
                                                                                          HKCU\software\microsoft\active setup\installed components\{22d6f312-
      Opens key:
b0f6-11d0-94ab-0080c74c7e95}
                                                                                          \label{lem:hkcu} \mbox{ HKCU\software\mbox{\sc}} active \ setup\nstalled \ components\scaled \ component
      Opens key:
2b09-4501-b3f3-f3508c9228ed}
                                                                                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \active setup \slightly installed components \end{tabular} \begin{tabular}{ll} 44bba840-\microsoft \active setup \slightly installed components \end{tabular} \begin{tabular}{ll} 44bba840-\microsoft \active setup \slightly installed \active setup \slightly installed \active setup \slightly installed \active setup \active setup \slightly installed \
      Opens key:
cc51-11cf-aafa-00aa00b6015c}
                                                                                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{$microsoft$ active setup$ installed components $$\{44bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba842-1944bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba844bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba84bba
      Opens key:
cc51-11cf-aafa-00aa00b6015b}
                                                                                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \active setup \slightly installed components \end{tabular} \begin{tabular}{ll} 44bba848-\\ \end{tabular}
      Opens key:
cc51-11cf-aafa-00aa00b6015c}
                                                                                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{$microsoft$ active setup$ installed components $$\{4b218e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-18e3e-1
      Opens key:
bc98-4770-93d3-2731b9329278}
                                                                                          Opens key:
1e7d-11d1-bc44-00c04fd912be}
                                                                                          HKCU\software\microsoft\active setup\installed components\{6bf52a52-
     Opens key:
394a-11d3-b153-00c04f79faa6}
      Opens key:
                                                                                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \active setup \slightly installed components \end{tabular} \begin{tabular}{ll} 47790769c-\microsoft \active setup \slightly installed components \end{tabular} \begin{tabular}{ll} 47790769c-\microsoft \active setup \slightly installed \active \active setup \slightly installed \acti
0471-11d2-af11-00c04fa35d02}
      Opens key:
                                                                                          HKCU\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4340}
                                                                                          HKCU\software\microsoft\active setup\installed components\{89820200-
      Opens kev:
ecbd-11cf-8b85-00aa005b4383}
      Opens key:
                                                                                          HKCU\software\microsoft\active setup\installed components\{89b4c1cd-
b018-4511-b0a1-5476dbf70820}
      Opens key:
                                                                                          HKCU\software\microsoft\activemovie
      Opens key:
                                                                                          HKCU\software\microsoft\activemovie\devenum
      Opens key:
                                                                                          HKCU\software\microsoft\activemovie\devenum\{083863f1-70de-11d0-bd40-
00a0c911ce86}
                                                                                          Opens key:
00a0c911ce86}\{31345649-0000-0010-8000-00aa00389b71}
      Opens key:
                                                                                          HKCU\software\microsoft\activemovie\devenum\{083863f1-70de-11d0-bd40-
00a0c911ce86}\{a2551f60-705f-11cf-a424-00aa003735be}
                                                                                          HKCU\software\microsoft\advanced inf setup
      Opens kev:
                                                                                          \label{lem:hkcu} \mbox{HKCU\software\mbox{$\mbox{microsoft\advanced inf setup\ie userdata nt}} \\
      Opens key:
      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 kev:
                                                                                          HKCU\software\microsoft\advanced inf setup\ie.hkcuzoneinfo
      Opens key:
                                                                                          HKCU\software\microsoft\advanced inf setup\ie.hkcuzoneinfo\regbackup
                                                                                          \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\advanced inf setup\ie.hkcuzoneinfo\regbackup\0}} \mbox{\sc one} \mbo
      Opens key:
      Opens key:
                                                                                          HKCU\software\microsoft\advanced inf
setup\ie.hkcuzoneinfo\regbackup\0.map
      Opens key:
                                                                                          HKCU\software\microsoft\advanced inf setup\ie40.useragent
      Opens kev:
                                                                                          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
                                                                                      HKCU\software\microsoft\clock
     Opens key:
                                                                                      HKCU\software\microsoft\command processor
     Opens kev:
     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 microsoft \setminus ctf \setminus compartment \setminus \{544d6a63 - e2e8 - 4752 - bbd1 - e2e8 - e
000960bca083}
                                                                                      HKCU\software\microsoft\ctf\langbar
     Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\ctf\msutb
     Opens key:
                                                                                      HKCU\software\microsoft\ctf\sapilayr
     Opens key:
                                                                                      HKCU\software\microsoft\ctf\tip
     Opens key:
                                                                                      HKCU \setminus software \setminus microsoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-00c04fc324a1\}
                                                                                      HKCU \setminus software \setminus microsoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143
     Opens key:
00c04fc324a1}\languageprofile
                                                                                      HKCU \setminus software \setminus microsoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143
     Opens key:
00c04fc324a1}\languageprofile\0x00000409
     Opens key:
                                                                                      HKCU\software\microsoft\direct3d
     Opens key:
                                                                                      HKCU\software\microsoft\direct3d\mostrecentapplication
                                                                                      HKCU\software\microsoft\eventsystem
     Opens key:
                                                                                      HKCU\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
     Opens key:
00805fc79216}
     Opens key:
                                                                                      HKCU\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions
     Opens key:
                                                                                      HKCU\software\microsoft\feeds
                                                                                      HKCU\software\microsoft\file manager
     Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\file manager\settings
     Opens key:
                                                                                      HKCU\software\microsoft\ftp
                                                                                      HKCU\software\microsoft\gdiplus
     Opens kev:
     Opens key:
                                                                                      HKCU\software\microsoft\ieak
     Opens key:
                                                                                      HKCU\software\microsoft\ieak\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:
                                                                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ internet\ explorer\+ browseremulation
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\caretbrowsing
                                                                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ internet explorer\+ desktop
     Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\desktop\components
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\desktop\components\0
     Opens key:
                                                                                      \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\desktop\general}} \\
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\desktop\old workareas
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\desktop\safemode
                                                                                      \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$^{$\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet explorer \desktop \software} \end{tabular} \begin{tabular}{ll} Akcount \mbox{$^{\rm microsoft}$ internet \desktop \software} \end{tabular
     Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\desktop\scheme
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\document windows
                                                                                      HKCU\software\microsoft\internet explorer\domstorage
     Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\domstorage\total
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\download
                                                                                      HKCU\software\microsoft\internet explorer\extensions
     Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\extensions\cmdmapping
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\help menu urls
                                                                                      HKCU\software\microsoft\internet explorer\ietld
     Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\ietld\lowmic
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\informationbar
                                                                                      \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\label{lem:hkcu} international} \\
     Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\10
     Opens key:
                                                                                      HKCU \ software \ microsoft \ internet\ explorer \ international \ scripts \ \ 11
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\12
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\13
     Opens key:
                                                                                      HKCU \ software \ microsoft \ internet\ explorer \ international \ scripts \ 14
     Opens key:
                                                                                      HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus international \setminus scripts \setminus 15
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\16
     Opens key:
                                                                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU software \microsoft \m
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\18
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\19
                                                                                      Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\21
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\22
                                                                                      HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus international \setminus scripts \setminus 23
     Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\24
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\25
                                                                                      \label{thm:condition} \begin{tabular}{ll} HKCU \software \microsoft \internet explorer \normaliser in ternational \scripts \columnwidth \columnwid
     Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\27
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\28
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\29
     Opens key:
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\3
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\30
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\34
     Opens key:
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\35
                                                                                      HKCU\software\microsoft\internet explorer\international\scripts\37
     Opens kev:
```

HKCU\software\microsoft\internet explorer\international\scripts\38

Opens key:

```
HKCU\software\microsoft\internet explorer\international\scripts\39
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\internet explorer\international\scripts\4
                                               HKCU\software\microsoft\internet explorer\international\scripts\5
   Opens kev:
   Opens key:
                                               HKCU\software\microsoft\internet explorer\international\scripts\6
   Opens kev:
                                               HKCU\software\microsoft\internet explorer\international\scripts\7
   Opens key:
                                               HKCU\software\microsoft\internet explorer\international\scripts\8
                                               HKCU\software\microsoft\internet explorer\international\scripts\9
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\internet explorer\internetregistry
   Opens key:
                                               HKCU\software\microsoft\internet explorer\linksbar
   Opens key:
                                               HKCU\software\microsoft\internet explorer\linksbar\itemcache
   Opens key:
                                               HKCU\software\microsoft\internet explorer\linksbar\itemcache\0
   Opens key:
                                               HKCU\software\microsoft\internet explorer\linksbar\itemcache\1
   Opens key:
                                               HKCU\software\microsoft\internet explorer\lowregistry
                                               \label{lower} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\lowregistry\domstorage}} \mbox{\sc domstorage} \mbox{\sc do
   Opens key:
   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
   Opens key:
                                               HKCU\software\microsoft\internet explorer\main
   Opens key:
                                               \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\internet explorer\mbox{\tt main\default feeds}} \\
   Opens key:
                                               HKCU\software\microsoft\internet explorer\main\default feeds\{292f3d25-
c7e7-48ac-bfba-7b9c1f5b42a7}
                                               HKCU\software\microsoft\internet explorer\main\default feeds\{8dd206d8-
   Opens kev:
e6a9-4797-bfe9-b6a7783eb157}
   Opens key:
                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
   Opens key:
                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown\settings
   Opens kev:
                                               HKCU\software\microsoft\internet explorer\main\windowssearch
   Opens key:
                                               HKCU\software\microsoft\internet explorer\new windows
   Opens key:
                                               HKCU\software\microsoft\internet explorer\new windows\allow
                                               HKCU\software\microsoft\internet explorer\phishingfilter
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\internet explorer\privacy
   Opens key:
                                               HKCU\software\microsoft\internet explorer\recovery
   Opens key:
                                               HKCU\software\microsoft\internet explorer\recovery\active
   Opens key:
                                               HKCU\software\microsoft\internet explorer\searchscopes
   Opens key:
                                               HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}
   Opens key:
                                               HKCU\software\microsoft\internet explorer\searchurl
   Opens key:
                                               HKCU\software\microsoft\internet explorer\security
   Opens key:
                                               HKCU\software\microsoft\internet explorer\security\antiphishing
   Opens key:
                                               HKCU\software\microsoft\internet
explorer\security\antiphishing\2cedbfbc-dba8-43aa-b1fd-cc8e6316e3e2
                                               \label{lem:hkcu} \mbox{HKCU\software\mbox{$m$icrosoft\internet explorer\security\p3global} \\
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\internet explorer\security\p3sites
   Opens key:
                                               HKCU\software\microsoft\internet explorer\services
                                               HKCU\software\microsoft\internet explorer\settings
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\internet explorer\sqm
   Opens key:
                                               HKCU\software\microsoft\internet explorer\suggested sites
                                               \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\tabbedbrowsing}}
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\internet explorer\toolbar
   Opens key:
                                               HKCU\software\microsoft\internet explorer\toolbar\explorer
                                               \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\toolbar\shellbrowser}} \\
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\internet explorer\toolbar\webbrowser
   Opens kev:
                                               HKCU\software\microsoft\internet explorer\typedurls
   Opens key:
                                               HKCU\software\microsoft\internet explorer\urlsearchhooks
   Opens key:
                                               HKCU\software\microsoft\internet explorer\user preferences
   Opens key:
                                               HKCU\software\microsoft\internet explorer\zoom
                                               HKCU\software\microsoft\java vm
   Opens kev:
   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
                                               \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ mediaplayer\+ battery\+ presets
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\mediaplayer\battery\presets\brightsphere
   Opens key:
Opens key:
HKCU \ software \ \verb|microsoft| mediaplayer \ \verb|battery| presets \ bright sphere \ \verb|preshiftinfo| |
                                               \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \mediap layer \battery \presets \circled ance \end{tabular}
   Opens key:
   Opens key:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \mediaplayer \battery \presets \circled ance \current shift info
   Opens key:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \mediap layer \battery \presets \circled ance \postshift in formula and the layer \mediap layer \mediap layer \mediap layer \mediap layer \mediap \
   Opens kev:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \mediap layer \battery \presets \circled ance \preshift info
   Opens key:
                                               HKCU\software\microsoft\mediaplayer\battery\presets\cominatya
   Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\cominatya\currentshiftinfo
\label{thm:hammon} \begin{tabular}{ll} HKCU \software \microsoft \mediap layer \battery \presets \cominaty a \preshift in form \end{tabular}
   Opens key:
                                               \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ mediaplayer\+ battery\+ presets\+ cotton star
```

```
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\cottonstar\currentshiftinfo
 Opens kev:
HKCU\software\microsoft\mediaplayer\battery\presets\cottonstar\preshiftinfo
 Opens kev:
                         HKCU\software\microsoft\mediaplayer\batterv\presets\dandelionaid
```

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

Opens kev: $HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus dandelionaid \setminus postshift info$ Opens key:

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

Opens key:

Opens key:

HKCU\software\microsoft\mediaplayer\battery\presets\drowningflower\postshiftinfo Opens key:

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

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

Opens key:

Opens key:

 $HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ eletriar nation \ postshift infonce in the property of the property \ mediaplayer \ battery \ presets \ eletriar nation \ postshift \ infonce in the property \ presets \ eletriar \ eletriar \ eletriar \ eletriar \ eletriar \ eletriar \ e$ Opens key:

 $\label{lem:hkcu} \verb+KCU \software \microsoft \mediaplayer \mbox{\verb+battery \presets \eventhorizon}$ Opens key:

Opens key:

 $HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus eventhorizon \setminus currents hiftinfo$ Opens kev:

HKCU\software\microsoft\mediaplayer\battery\presets\eventhorizon\postshiftinfo Opens key:

 $\label{thm:local_hammon} \begin{tabular}{l} HKCU \software \microsoft \mediaplayer \mediaplayer$

Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick ascii Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick

ascii\currentshiftinfo

HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick Opens key:

ascii\postshiftinfo

HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick Opens key:

ascii\preshiftinfo

Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\gemstone matrix

Opens key: $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc mediaplayer\battery\presets\gemstone}} \\$

matrix\currentshiftinfo

Opens kev: HKCU\software\microsoft\mediaplayer\batterv\presets\gemstone

matrix\preshiftinfo

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

Opens key:

 $HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ grooves \ wirl \ currents \ hiftinfollowed \ battery \ batte$

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

Opens key:

 $HKCU \ software \ \verb|microsoft| mediaplayer \ \verb|battery| presets \ | grooves wirl \ | preshift in fooling the large state of t$ HKCU\software\microsoft\mediaplayer\battery\presets\illuminator Opens key:

Opens key:

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

Opens kev:

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

Opens kev:

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

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

Opens key:

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

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \mediap layer \battery \presets \see the truth \preshift in formula and the layer \mediap layer \end{tabular} \begin{tabular}{ll} HKCU \software \microsoft \mediap layer \see the truth \preshift in formula \see the layer \mediap layer \see the layer \mediap \see the layer \see the layer \mediap \see$ HKCU\software\microsoft\mediaplayer\battery\presets\kaleidoscope

Opens kev:

Opens key:

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

Opens key:

Opens key:

 $HKCU \ software \ \verb|microsoft| mediaplayer \ \verb|battery| presets \ \verb|kaleidoscope| preshiftinfo| \\$

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

Opens kev:

Opens key:

 $HKCU \ software \ microsoft \ mediap layer \ battery \ presets \ khemical nova \ postshift in formula \ microsoft \ mediap \ layer \ battery \ presets \ khemical nova \ postshift \ in formula \ postshift \ presets \ khemical \ postshift \ presets \ prese$ Opens kev:

 $HKCU \ software \ icrosoft \ mediaplayer \ battery \ presets \ khemical nova \ preshift in formula \ preshift \ in formula \ preshift \ presets \ khemical \ preshift \ presets \ preset$ HKCU\software\microsoft\mediaplayer\battery\presets\lotus Opens kev: Opens key:

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

Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\lotus\preshiftinfo Opens kev: Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\nerds are cool

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

cool\currentshiftinfo

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

cool\postshiftinfo

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

cool\preshiftinfo

 $Opens\ key: \\ HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ relatively calmage. \\$

Opens key:

 $\label{thm:local} HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ relatively calm \ currents \ hiftin fo$

Opens key:

Opens key:

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

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

Opens key:

 $\label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \mbox{\mathbb{N} info} \\ \end{tabular} \begin{tabu$

Opens key:

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

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

water\currentshiftinfo

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

water\preshiftinfo

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

Opens key:

Opens kev:

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

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

Opens key:

Opens key:

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

Opens key:

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \mediaplayer \battery \presets \strawberry aid \preshift in formula and the linear \microsoft \mediaplayer \arrow \microsoft \mediaplayer \arrow \microsoft \mediaplayer \arrow \microsoft \mediaplayer \microsoft \mediaplayer \microsoft \micro$

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

Opens key:

 $HKCU \ software \ \verb|microsoft| mediaplayer \ battery \ \verb|presets| tornado \ \verb|currents| if tinfo \ battery \ batte$

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

Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings
Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http
Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\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

Opens key: HKCU\software\microsoft\microsoft management console

Opens key: HKCU\software\microsoft\microsoft management console\recent file list
Opens key: HKCU\software\microsoft\microsoft management console\settings

Opens key: HKCU\software\microsoft\ms design tools
Opens key: HKCU\software\microsoft\ms design tools\mdtdbd

Opens key: HKCU\software\microsoft\msdaipp

Opens key: ${\tt HKCU \setminus software \setminus microsoft \setminus msdaipp \setminus providers}$

 $Opens \ key: \\ HKCU \ software \ microsoft \ msdaipp \ providers \ \{9fecd 570-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b9d4-11d1-9c78-b$

0000f875ac61}

Opens key: HKCU\software\microsoft\msdaipp\providers\{9fecd571-b9d4-11d1-9c78-

0000f875ac61}

Opens key: HKCU\software\microsoft\multimedia
Opens key: HKCU\software\microsoft\multimedia\audio

Opens key: HKCU\software\microsoft\multimedia\audio\waveformats
Opens key: HKCU\software\microsoft\multimedia\audio compression manager
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

```
HKCU\software\microsoft\netdde\dde trusted shares
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a
  Opens key:
                                    HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a\chat$
  Opens key:
                                    HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a\clpbk$
  Opens kev:
                                    HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a\hearts$
  Opens key:
                                    HKCU\software\microsoft\netshow
                                    HKCU\software\microsoft\netshow\player
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\netshow\player\remote
  Opens key:
                                    HKCU\software\microsoft\notepad
  Opens key:
                                    HKCU\software\microsoft\ntbackup
  Opens key:
                                    HKCU\software\microsoft\office
  Opens key:
                                    HKCU\software\microsoft\office\11.0
  Opens key:
                                    HKCU\software\microsoft\office\11.0\common
                                    HKCU\software\microsoft\office\11.0\common\drawalerts
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\office\11.0\common\drawalerts\ftp sites
                                    HKCU\software\microsoft\office\11.0\common\dspadaptermru
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\office\11.0\common\general
  Opens key:
                                    HKCU\software\microsoft\office\11.0\common\languageresources
  Opens key:
                                    HKCU\software\microsoft\office\11.0\common\migration
  Opens key:
                                    HKCU\software\microsoft\office\11.0\common\migration\office
  Opens key:
                                    HKCU\software\microsoft\office\11.0\common\migration\word
                                    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
  Opens key:
                                    HKCU\software\microsoft\office\11.0\common\open find\places
                                    HKCU\software\microsoft\office\11.0\common\research
  Opens key:
  Opens key:
                                    \label{thm:local_hammon} HKCU \software \microsoft \softice \slation \slation
  Opens key:
                                    HKCU\software\microsoft\office\11.0\common\toolbars
                                    HKCU\software\microsoft\office\11.0\common\toolbars\settings
  Opens kev:
  Opens key:
                                    HKCU\software\microsoft\office\11.0\common\userinfo
  Opens key:
                                    HKCU\software\microsoft\office\11.0\word
                                    HKCU\software\microsoft\office\11.0\word\options
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\office\11.0\word\userinfo
  Opens key:
                                    HKCU\software\microsoft\office\11.0\word\wizards
                                    HKCU\software\microsoft\office\11.0\wordview
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\office\11.0\wordview\data
  Opens key:
                                    HKCU\software\microsoft\office\12.0
  Opens key:
                                    HKCU\software\microsoft\office\12.0\common
  Opens key:
                                    HKCU\software\microsoft\office\12.0\common\drawalerts
  Opens key:
                                    HKCU\software\microsoft\office\12.0\common\drawalerts\ftp sites
  Opens key:
                                    HKCU\software\microsoft\office\12.0\common\general
  Opens key:
                                    HKCU\software\microsoft\office\12.0\common\languageresources
  Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \office \12.0 \common \label{lem:hkcu} \end{tabular} aggers aggers \label{lem:hkcu}
  Opens key:
                                    HKCU\software\microsoft\office\12.0\common\migration
  Opens key:
                                    HKCU\software\microsoft\office\12.0\common\migration\excel
  Opens key:
                                    \label{local-common-migration} HKCU \software \mbox{$\mbox{$\mbox{microsoft} office}$} 12.0 \common \mbox{$\mbox{$\mbox{$\mbox{$microsoft}$} office}$
  Opens key:
                                    HKCU\software\microsoft\office\12.0\common\open find
  Opens key:
                                    HKCU\software\microsoft\office\12.0\common\open find\microsoft office
excel viewer
  Opens key:
                                    HKCU\software\microsoft\office\12.0\common\open find\places
  Opens key:
                                    HKCU\software\microsoft\office\12.0\common\research
                                    \label{lem:hkcu} $$HKCU\software\microsoft\office\12.0\common\research\translation
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\office\12.0\excel
  Opens kev:
                                    HKCU\software\microsoft\office\12.0\excel\options
  Opens key:
                                    HKCU\software\microsoft\office\12.0\excel viewer
  Opens key:
                                    HKCU\software\microsoft\office\12.0\excel viewer\viewer options
  Opens key:
                                    HKCU\software\microsoft\office\12.0\user settings
                                    \label{local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-loc
  Opens kev:
  Opens key:
                                    HKCU\software\microsoft\office\12.0\user settings\mso_intl
  Opens key:
                                    HKCU\software\microsoft\office\12.0\user settings\powerpoint_intl
  Opens key:
                                    HKCU\software\microsoft\office\14.0
  Opens key:
                                    HKCU\software\microsoft\office\14.0\common
  Opens key:
                                    HKCU\software\microsoft\office\14.0\common\drawalerts
                                    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
                                    \label{local-common} HKCU \ software \ icrosoft \ office \ 14.0 \ common \ open \ find \ microsoft
  Opens key:
powerpoint viewer
  Opens key:
                                    HKCU\software\microsoft\office\14.0\common\open find\places
                                    HKCU \ software \ microsoft \ office \ 14.0 \ common \ research
  Opens key:
  Opens key:
                                    \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \office \14.0 \common \research \translation \end{tabular}
  Opens key:
                                    HKCU\software\microsoft\office\14.0\powerpoint
  Opens key:
                                    HKCU\software\microsoft\office\14.0\powerpoint viewer
  Opens key:
                                    HKCU\software\microsoft\office\14.0\powerpoint viewer\options
  Opens key:
                                    HKCU\software\microsoft\office\common
  Opens key:
                                    HKCU\software\microsoft\office\common\smart tag
  Opens key:
                                    HKCU\software\microsoft\office\common\smart tag\actions
  Opens key:
```

455d-a40b-c95f1f91ff8a}

```
Opens key:
                                      HKCU\software\microsoft\office\common\smart tag\actions\{49df3409-46b3-
4b0c-b7bf-fec0f9401edd}
  Opens key:
                                      HKCU\software\microsoft\office\common\smart tag\actions\{64ab6c69-b40e-
40af-9b7f-f5687b48e2b6}
  Opens key:
                                      HKCU \setminus software \setminus microsoft \setminus office \setminus common \setminus smart tag \setminus actions \setminus \{c3754d1a - 04d3 - 04
4085-8cfb-97705b57a98f}
  Opens key:
                                      HKCU\software\microsoft\office\common\smart tag\actions\{f114ae61-1331-
4238-92c9-bbe330af25fd}
  Opens key:
                                      HKCU\software\microsoft\office\common\smart tag\recognizers
                                      HKCU\software\microsoft\office\common\smart tag\recognizers\{64ab6c69-
  Opens key:
b40e-40af-9b7f-f5687b48e2b6}
  Opens key:
                                      HKCU\software\microsoft\office\common\smart tag\recognizers\{87ef1cfe-
51ca-4e6b-8c76-e576aa926888}
                                     HKCU\software\microsoft\office\common\userinfo
  Opens key:
                                      HKCU\software\microsoft\outlook express
  Opens key:
                                      HKCU\software\microsoft\outlook express\5.0
  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 key:
                                      HKCU\software\microsoft\plus!\themes\apply
  Opens key:
                                      HKCU\software\microsoft\plus!\themes\current
                                      HKCU\software\microsoft\protected storage system provider
  Opens kev:
  Opens key:
                                      HKCU\software\microsoft\protected storage system provider\s-1-5-21-
1757981266-507921405-1957994488-1003
                                     HKCU\software\microsoft\ras phonebook
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\regedt32
                                      HKCU\software\microsoft\regedt32\settings
  Opens key:
                                      HKCU\software\microsoft\sapi layer
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\schedule+
  Opens key:
                                      HKCU\software\microsoft\schedule+\microsoft schedule+
                                      HKCU\software\microsoft\search assistant
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\security center
  Opens key:
                                      HKCU\software\microsoft\shared
                                      HKCU\software\microsoft\shared tools
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\shared tools\font mapping
  Opens key:
                                      HKCU\software\microsoft\shared tools\proofing tools
                                      HKCU\software\microsoft\shared tools\proofing tools\custom dictionaries
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\speech
  Opens key:
                                      HKCU\software\microsoft\speech\applexicons
                                      HKCU\software\microsoft\speech\audiooutput
  Opens key:
  Opens key:
                                      {\tt HKCU \backslash software \backslash microsoft \backslash speech \backslash current user lexicon}
  Opens key:
                                      HKCU\software\microsoft\speech\currentuserlexicon\applexicons
                                      Opens key:
85d6-72e5eeb6995a}
  Opens key:
                                      HKCU\software\microsoft\speech\currentuserlexicon\{c9e37c15-df92-4727-
85d6-72e5eeb6995a}\files
  Opens key:
                                      HKCU\software\microsoft\speech\phoneconverters
                                      HKCU\software\microsoft\speech\voices
  Opens kev:
                                      HKCU\software\microsoft\sqmclient
  Opens key:
  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 kev:
                                      HKCU\software\microsoft\systemcertificates\ca\ctls
                                      \label{lower} \verb+ HKCU \+ software \+ microsoft \+ system certificates \+ disallowed
  Opens key:
  Opens key:
                                      HKCU \setminus software \setminus microsoft \setminus system certificates \setminus disallowed \setminus certificates
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\disallowed\crls
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\disallowed\ctls
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\my
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\root
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\root\certificates
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\root\crls
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\root\ctls
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ system certificates\+ root\+ protected roots
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\trust
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\trust\certificates
  Opens key:
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ system certificates \verb+ trust \verb+ crls+ \\
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\trust\ctls
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\trustedpublisher
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ systemcertificates \verb+ \trusted publisher \verb+ certificates \verb+ \\
  Opens key:
  Opens key:
                                      HKCU \setminus software \setminus microsoft \setminus system certificates \setminus trusted publisher \setminus crls
  Opens key:
                                      HKCU\software\microsoft\systemcertificates\trustedpublisher\ctls
  Opens key:
                                      HKCU\software\microsoft\visualstudio
  Opens key:
                                      HKCU\software\microsoft\visualstudio\9.0
  Opens key:
                                      HKCU\software\microsoft\visualstudio\9.0\downloadmanager
                                      HKCU\software\microsoft\wbem
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\wbem\wmic
  Opens key:
                                      HKCU\software\microsoft\windows
                                      HKCU\software\microsoft\windows\currentversion
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\app management
  Opens kev:
                                      HKCU\software\microsoft\windows\currentversion\applets
  Opens key:
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ applets\+ regedit
```

```
Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\applets\systray
                                                        HKCU\software\microsoft\windows\currentversion\applets\tour
   Opens key:
                                                        \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ controls folder
   Opens kev:
                                                        HKCU\software\microsoft\windows\currentversion\explorer
   Opens key:
   Opens kev:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
   Opens key:
                                                        \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \bitbucket \end{tabular}
                                                        \label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\cabinetstate
   Opens key:
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\cd burning
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\cd
burning\drives
   Opens kev:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\clsid
   Opens key:
                                                        ad25-11d0-98a8-0800361b1103}
                                                        HKCU\software\microsoft\windows\currentversion\explorer\clsid\{645ff040-
   Opens key:
5081-101b-9f08-00aa002f954e}
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
42a0-1069-a2ea-08002b30309d}
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\comdlg32
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\lastvisitedmru
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\opensavemru
   Opens kev:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\desktop
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\cleanupwiz
                                                        \label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\discardable}}
   Opens key:
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\discardable\postsetup
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts
   Opens kev:
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.aif
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.aifc
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.aiff
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.application
                                                        \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \file exts \color=0.5 \color=0.
   Opens key:
   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
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dib
   Opens key:
   Opens key:
                                                        \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\.. doc
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.docm
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.docx
   Opens key:
   Opens key:
                                                        HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus file exts \setminus .dot
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dvr-ms
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.egg-
info
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.emf
                                                        \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\
   Opens key:
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ico
   Opens key:
                                                        \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.ivf}
   Opens kev:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.jfif
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.jpe
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.jpeg
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.jpg
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m1v
   Opens key:
   Opens key:
                                                        HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus file exts \setminus .m3u
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mid
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.midi
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp2
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp2v
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp3
   Opens key:
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpa
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpe
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpeg
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpg
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpv2
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.msc
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.msi
   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} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.potm}
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.potx
                                                        \label{lem:hccu} \mbox{HKCU\software\mbox{\sc urrentversion\explorer\fileexts\sc .ppsm}} \mbox{\sc urrentversion\explorer\sc .ppsm} \mbox{\sc urrentversion\explorer\sc urrentversion\explorer\sc .ppsm} \mbox{\sc urrentversion\explorer\sc urr
   Opens key:
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ppsx
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ppt
```

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

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \explorer \fileexts \cdots. pptx$

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

 $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+..rtf+ \\$

Opens key:

Opens key:

Opens kev:

Opens key:

```
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:
                                                                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\.tiff}
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.txt
     Opens key:
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.way
     Opens key:
                                                                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+ file exts \verb+..wax+ \\
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wdp
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wm
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wma
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wmf
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wmv
     Opens key:
     Opens key:
                                                                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.wmx} \\
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wpl
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wri
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wvx
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xaml
     Opens kev:
                                                                          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:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlsb
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlsm
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlsx
     Opens kev:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlt
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xltm
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xltx
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xps
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.zip
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\menuorder
     Opens kev:
HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites
    Opens key:
                                                                         HKCU\software\microsoft\windows\currentversion\explorer\menuorder\start
menu
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\c
     Opens key:
                                                                         HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\d
     Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c0-6bc4-11e3-9fc7-
806d6172696f}
     Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints \\ 2 \setminus \{f90255c2-6bc4-11e3-9fc7-12e3-12e4\} \setminus \{f90255c2-6bc4-11e3-9fc7-12e4\} \setminus \{f90255c2-6bc4-12e4\} \setminus \{f90255c2-6bc4-12e4\} \setminus \{f9025c2-6bc4-12e4\} \setminus \{f9025c2-6bc4-12e4\} \setminus \{f9025c2-6bc4-12e4\} \setminus \{f9025c2-6bc4-12e4\} \setminus \{f9025c2-6bc4-12e4\} \setminus \{f9025c2-6bc4-
806d6172696f}
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\mycomputer
     Opens kev:
     Opens key:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \microsoft \windows \current \curre
     Opens key:
\label{thm:local_explorer} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \newshort cuthandlers} \end{tabular}
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\recentdocs
     Opens kev:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\recentdocs\.zip
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\runmru
     Opens key:
                                                                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \shell folders} \end{tabular}
     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 kev:
                                                                          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\software\microsoft\windows\currentversion\explorer\stuckrects2
     Opens key:
                                                                         HKCU\software\microsoft\windows\currentversion\explorer\tips
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\traynotify
     Opens key:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders
     Opens key:
                                                                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\userassist}}
     Opens kev:
HKCU \ software \ microsoft \ windows \ current version \ (see ab 780 - 7743 - 11cf - a 12b - 
00aa004ae837}
     Opens key:
HKCU \setminus software \\ \mbox{microsoft} \\ \mbox{windows} \\ \mbox{current} \\ \mbox{version} \\ \mbox{explorer} \\ \mbox{userassist} \\ \mbox{75048700-ef1f-11d0-9888-1000} \\ \mbox{ef1} \\ \mbox{ef2} \\ \mbox{ef
006097deacf9}
     Opens kev:
                                                                          HKCU\software\microsoft\windows\currentversion\explorer\visualeffects
     Opens key:
```

HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\cursorshadow

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dragfullwindows\currentversion\explorer\visualeffects\dragfullwindows\currentversion\explorer\visualeffects\dragfullwindows\currentversion\explorer\visualeffects\dragfullwindows\currentversion\explorer\visualeffects\dragfullwindows\currentversion\explorer\visualeffects\dragfullwindows\currentversion\explorer\visualeffects\dragfullwindows\currentversion\explorer\visualeffects\dragfullwindows\currentversion\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfullwindows\explorer\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfull\dragfull\visualeffects\dragfull\visualeffects\dragfull\visualeffects\dragfu

 $\label{lem:hkcu} HKCU \software \microsoft \windows \current version \explorer \visual effects \dragfull windows \end{substitute} Opens \ key:$

HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\animateminmax

HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\comboboxanimation

Opens key:

Opens key:

 $\label{lem:hkcu} HKCU \software \microsoft \windows \current version \explorer \visual effects \drops \hadow Opens \key:$

 $\label{lem:hkcu} HKCU\software\microsoft\windows\currentversion\explorer\visual effects\fontsmoothing Opens key:$

```
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listboxsmoothscrolling
      Opens kev:
HKCU \ software \ microsoft \ windows \ \ current version \ \ explorer \ \ visual effects \ \ list viewal phase lect
      Opens key:
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewwatermark
      Opens key:
HKCU \ software \ \ microsoft \ \ windows \ \ current version \ \ \ \ visual effects \ \ \ menuanimation
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\selectionfade
      Opens key:
HKCU \ software \ microsoft \ windows \ current version \ lex plorer \ visual effects \ task baranimations
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\themes
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\tooltipanimation
      Opens key:
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
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo
      Opens kev:
      Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in fow 0000000000000331
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\ext
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\settings
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-
      Opens key:
 e8ad-4283-a596-fa578c2ebdc3}
                                                                                              HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{4eb89ff4-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{4eb89ff4-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{4eb89ff4-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{4eb89ff4-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{4eb89ff4-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{4eb89ff4-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{4eb89ff4-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{4eb89ff4-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{4eb89ff4-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{4eb89ff4-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{4eb89ff4-microsoft \setminus ext \setminus
      Opens key:
 7f78-4a0f-8b8d-2bf02e94e4b2}
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\settings\{4edcb26c-
      Opens key:
d24c-4e72-af07-b576699ac0de}
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\settings\{7390f3d8-
0439-4c05-91e3-cf5cb290c3d0}
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\settings\{754ff233-
      Opens key:
 5d4e-11d2-875b-00a0c93c09b3}
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\settings\{7584c670-
 2274-4efb-b00b-d6aaba6d3850}
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\settings\{761497bb-
      Opens key:
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}
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\settings\{bdd307c3-
      Opens key:
7bc0-4542-9f8f-a9611fe6c1bf}
      Opens key:
                                                                                              HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{c533 adf1-microsoft \setminus windows \setminus ext \setminus 
0c80-11d1-8c54-00a02468f316}
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\settings\{d27cdb6e-
 ae6d-11cf-96b8-444553540000}
      Opens kev:
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-
a445-435b-bc74-9c25c1c588a9}
      Opens key:
                                                                                              HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{e7e6f031-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{e7e6f031-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{e7e6f031-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{e7e6f031-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{e7e6f031-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{e7e6f031-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{e7e6f031-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{e7e6f031-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{e7e6f031-microsoft \setminus windows \setminus ext \setminus settings \setminus ext \setminus settings \setminus \{e7e6f031-microsoft \setminus windows \setminus ext \setminus settings \setminus ext \setminus settings \setminus ext \setminus settings \setminus ext \setminus ext \setminus settings \setminus ext \setminus settings \setminus ext \setminus ex
 17ce-4c07-bc86-eabfe594f69c}
      Opens key:
                                                                                              \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\ext\stats}} \\
      Opens key:
                                                                                              11cf-aaa5-00401c608501}
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
 4283-a596-fa578c2ebdc3}
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\stats\{25336920-03f9-
 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}
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\stats\{cfbfae00-17a6-
      Opens key:
 11d0-99cb-00c04fd64497}
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\stats\{d27cdb6e-ae6d-
 11cf-96b8-444553540000}
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
 435b-bc74-9c25c1c588a9}
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\stats\{dfeaf541-f3e1-
4c24-acac-99c30715084a}
      Opens key:
                                                                                              4134-82b7-f2ba38496583}
      Opens key:
                                                                                              4c07-bc86-eabfe594f69c}
                                                                                              HKCU\software\microsoft\windows\currentversion\ext\stats\{fb5f1910-f110-
      Opens key:
 11d2-bb9e-00c04f795683}
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\group policy
                                                                                              HKCU\software\microsoft\windows\currentversion\group policy\appmgmt
      Opens key:
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\group
```

```
policy\groupmembership
                                     HKCU\software\microsoft\windows\currentversion\group policv\history
  Opens kev:
                                     HKCU\software\microsoft\windows\currentversion\group
  Opens key:
policy\history\{a2e30f80-d7de-11d2-bbde-00c04f86ae3b}
  Opens kev:
                                     HKCU\software\microsoft\windows\currentversion\group policy objects
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\group policy
objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}machine
                                     HKCU\software\microsoft\windows\currentversion\group policy
  Opens kev:
objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}machine\software
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\group policy
objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}user
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\grpconv
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\grpconv\mapgroups
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings
                                     HKCU\software\microsoft\windows\currentversion\internet settings\5.0
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\cache
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\activities
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
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 kev:
settings\activities\translate
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\cache
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
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
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\0
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\1
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\2
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                     HKCU\software\microsoft\windows\currentversion\internet settings\p3p
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\passport
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\passport\damap
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\protocols
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\protocols\mailto
                                     HKCU\software\microsoft\windows\currentversion\internet settings\url
  Opens key:
history
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zonemap
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\escdomains
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\protocoldefaults
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens kev:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
                                     \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \sides for the local partial partial
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\policies
                                     HKCU\software\microsoft\windows\currentversion\policies\explorer
```

Opens key: HKCU\software\microsoft\windows\currentversion\policie
Opens key: HKCU\software\microsoft\windows\currentversion\run
Opens key: HKCU\software\microsoft\windows\currentversion\run

```
Opens key:
                                                                                                                                 HKCU\software\microsoft\windows\currentversion\settings
        Opens key:
                                                                                                                                 HKCU\software\microsoft\windows\currentversion\settings\zonemap
        Opens key:
HKCU\software\microsoft\windows\currentversion\settings\zonemap\protocoldefaults
        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}
                                                                                                                                 \label{thm:locked} \mbox{HKCU\software\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbo
        Opens key:
        Opens key:
                                                                                                                                 HKCU\software\microsoft\windows\currentversion\shell extensions\cached
        Opens key:
                                                                                                                                 HKCU\software\microsoft\windows\currentversion\syncmgr
                                                                                                                                 \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc urrentversion\sc yncmgr\handlers}} \mbox{\sc urrentversion\sc urrentversion\s
        Opens key:
        Opens key:
                                                                                                                                 HKCU\software\microsoft\windows\currentversion\telephony
        Opens key:
HKCU\software\microsoft\windows\currentversion\telephony\handoffpriorities
```

Opens key:

HKCU\software\microsoft\windows\currentversion\telephony\handoffpriorities\mediamodes Opens key: HKCU\software\microsoft\windows\currentversion\thememanager HKCU\software\microsoft\windows\currentversion\themes Opens key:

Opens key:

HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleoff

Opens key:

HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleon

Opens key: HKCU\software\microsoft\windows\currentversion\themes\lasttheme Opens key: HKCU\software\microsoft\windows\currentversion\webcheck

Opens key: HKCU\software\microsoft\windows\currentversion\webcheck\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

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ wintrust\+ trust\+ providers$ Opens key:

Opens key: $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc urrentversion\wintrust\trust}} \\$

providers\software publishing

HKCU\software\microsoft\windows\shell Opens kev: Opens key: HKCU\software\microsoft\windows\shell\bagmru Opens key: HKCU\software\microsoft\windows\shell\bags Opens key: HKCU\software\microsoft\windows\shell\bags\1

Opens key: HKCU\software\microsoft\windows\shell\bags\1\desktop Opens key: HKCU\software\microsoft\windows\shell\localizedresourcename

Opens key: HKCU\software\microsoft\windows\shellnoroam

Opens key: HKCU\software\microsoft\windows\shellnoroam\bagmru Opens key: HKCU\software\microsoft\windows\shellnoroam\bagmru\0 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 Opens key: Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus bagmru \setminus 2 \setminus 0$ Opens key: HKCU\software\microsoft\windows\shellnoroam\bagmru\3 HKCU\software\microsoft\windows\shellnoroam\bags Opens key: Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\1 Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\1\shell $HKCU \ software \ microsoft \ windows \ shell no roam \ bags \ 10$ Opens key: Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\10\shell

Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\11 $HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus bags \setminus 11 \setminus shell$ Opens key: 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: 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 Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\15 Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\15\shell Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\16

Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\16\shell Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\17 HKCU\software\microsoft\windows\shellnoroam\bags\17\shell Opens key: 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: Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\19\shell 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 $HKCU \ software \ `microsoft \ windows \ shell no roam \ bags \ \ 21$ Opens key: Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\21\shell 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 HKCU\software\microsoft\windows\shellnoroam\bags\23\shell Opens kev:

Opens key: HKCU\software\microsoft\windows\shellnoroam\bags\24

```
Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\25
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\25\shell
    Opens kev:
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\26
    Opens kev:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\26\shell
    Opens key:
                                                         HKCU \ software \ microsoft \ windows \ shell no roam \ bags \ 27
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\27\shell
    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:
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\29\shell
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\3
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\3\shell
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\30
    Opens key:
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\30\shell
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\31
    Opens key:
    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 key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\4\shell
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\5
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\5\shell
    Opens kev:
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\6
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\6\shell
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\7
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\7\shell
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\8
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\8\shell
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\9
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\bags\9\shell
                                                         HKCU\software\microsoft\windows\shellnoroam\duibags
    Opens key:
    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 \ duibags \ folders \ fold
08002b30309d}
   Opens key:
\label{twindows} HKCU \software \microsoft \windows \shell no roam \duibags \shell folders \cite{Colored} a ea-1069-a 2dd-1069-a 2
08002b30309d}
    Opens key:
HKCU \ software \ microsoft \ windows \ shell no roam \ duibags \ shell folders \ \{7007acc7-3202-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aad2-11d1-aa
00805fc1270e}
   Opens kev:
00aa0060fa31}
    Opens key:
00aa004ae837}
    Opens key:
                                                         HKCU\software\microsoft\windows\shellnoroam\muicache
                                                         HKCU\software\microsoft\windows help
    Opens key:
    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 kev:
                                                         HKCU\software\microsoft\windows media\wmsdk\local
    Opens key:
                                                         HKCU\software\microsoft\windows media\wmsdk\namespace
    Opens key:
                                                         HKCU\software\microsoft\windows media\wmsdk\remote
    Opens key:
                                                         HKCU\software\microsoft\windows media\wmsdk\videodecode
                                                         HKCU\software\microsoft\windows nt
    Opens kev:
    Opens key:
                                                         HKCU\software\microsoft\windows nt\currentversion
    Opens key:
                                                         HKCU\software\microsoft\windows nt\currentversion\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
                                                         \label{lem:hkcu} \mbox{HKCU\software\mbox{$\mbox{$m$icrosoft\windows}$ nt\currentversion\network\location} \\
    Opens key:
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
    Opens key:
                                                         HKCU\software\microsoft\windows nt\currentversion\network\user manager
for domains
    Opens key:
                                                         HKCU\software\microsoft\windows nt\currentversion\printerports
    Opens key:
                                                         HKCU\software\microsoft\windows nt\currentversion\program manager
    Opens key:
                                                         HKCU\software\microsoft\windows nt\currentversion\program
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
    Opens key:
                                                         HKCU\software\microsoft\windows nt\currentversion\taskmanager
    Opens kev:
                                                         HKCU\software\microsoft\windows nt\currentversion\time zones
    Opens key:
                                                         HKCU\software\microsoft\windows nt\currentversion\truetype
```

HKCU\software\microsoft\windows\shellnoroam\bags\24\shell

Opens key:

```
Opens key:
                            HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:
                            HKCU\software\microsoft\windows nt\currentversion\winlogon
  Opens kev:
                            HKCU\software\microsoft\windows nt\currentversion\winlogon\gpextensions
                            HKCU\software\microsoft\windows
  Opens key:
nt\currentversion\winlogon\gpextensions\{a2e30f80-d7de-11d2-bbde-00c04f86ae3b}
  Opens key:
                            HKCU\software\microsoft\windows script
  Opens key:
                            HKCU\software\microsoft\windows script\settings
                            HKCU\software\netscape
  Opens key:
  Opens key:
                            HKCU\software\netscape\netscape navigator
  Opens key:
                            HKCU\software\netscape\netscape navigator\suffixes
  Opens kev:
                            HKCU\software\netscape\netscape navigator\user trusted external
applications
  Opens key:
                            HKCU\software\netscape\netscape navigator\viewers
  Opens key:
                            HKCU\software\policies
  Opens key:
                            HKCU\software\policies\microsoft
  Opens key:
                            HKCU\software\policies\microsoft\systemcertificates
  Opens kev:
                            HKCU\software\policies\microsoft\systemcertificates\ca
  Opens key:
                            HKCU\software\policies\microsoft\systemcertificates\ca\certificates
  Opens key:
                            HKCU\software\policies\microsoft\systemcertificates\ca\crls
  Opens key:
                            HKCU\software\policies\microsoft\systemcertificates\ca\ctls
  Opens key:
                            HKCU\software\policies\microsoft\systemcertificates\disallowed
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus disallowed \setminus certificates
  Opens key:
                            HKCU\software\policies\microsoft\systemcertificates\disallowed\crls
  Opens key:
                            HKCU\software\policies\microsoft\systemcertificates\disallowed\ctls
                            HKCU\software\policies\microsoft\systemcertificates\trust
  Opens key:
  Opens key:
                            HKCU \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus trust \setminus certificates
  Opens key:
                            HKCU\software\policies\microsoft\systemcertificates\trust\crls
                            HKCU\software\policies\microsoft\systemcertificates\trust\ctls
  Opens key:
  Opens key:
                            \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \system certificates \trusted publisher \end{tabular}
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus trusted publisher \setminus certificates
  Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\crls
  Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\ctls
                            HKCU\software\classes
  Opens kev:
  Opens key:
                            HKCU\software\classes\clsid
  Opens key:
                            HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}
  Opens key:
                            HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-
00805f499d93}\inprocserver32
                            HKCU\software\classes\clsid\{cafeefac-0013-0000-0003-abcdeffedcba}
  Opens key:
                            HKCU\software\classes\clsid\{cafeefac-0013-0000-0003-
  Opens kev:
```

abcdeffedcba}\inprocserver32

HKCU\software\classes\clsid\{cafeefac-0013-0000-0004-abcdeffedcba} Opens kev:

HKCU\software\classes\clsid\{cafeefac-0013-0000-0004-Opens key:

abcdeffedcba}\inprocserver32

Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0000-0005-abcdeffedcba}

HKCU\software\classes\clsid\{cafeefac-0013-0000-0005-Opens key:

abcdeffedcba}\inprocserver32

 $\label{local-condition} HKCU \setminus software \setminus classes \setminus clsid \setminus \{cafeefac-0013-0001-0000-abcdeffedcba\}$ Opens key:

HKCU\software\classes\clsid\{cafeefac-0013-0001-0000-Opens key:

abcdeffedcba}\inprocserver32

HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-abcdeffedcba} Opens key:

HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-Opens key:

abcdeffedcba}\inprocserver32

HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-abcdeffedcbb} Opens key:

HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-Opens key:

abcdeffedcbb}\inprocserver32

HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-abcdeffedcba} Opens key:

Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-

abcdeffedcba}\inprocserver32

HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-abcdeffedcbb} Opens key:

HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-Opens kev:

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

Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0003-abcdeffedcbb}

HKCU\software\classes\clsid\{cafeefac-0013-0001-0003-Opens kev:

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

Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0004-abcdeffedcbb}

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

Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0005-abcdeffedcbb}

Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0005-

abcdeffedcbb}\inprocserver32

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0007-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0007-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0007-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0007-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0008-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0008-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0008-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0008-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0009-abcdeffedcba}
                         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 kev:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0010-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0010-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0010-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0010-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0011-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0011-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0011-abcdeffedcbb}
                         Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0012-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0012-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0012-abcdeffedcbb}
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0012-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0013-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0013-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0013-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0013-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0014-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0014-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0014-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0014-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0015-abcdeffedcba}
 Opens kev:
 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
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0016-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0016-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0016-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0016-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0017-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0017-
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 kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0018-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0018-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0018-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0019-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0019-
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:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0013-0001-0020-
abcdeffedcba}\inprocserver32
 Opens kev:
                          HKCU\software\classes\clsid\{cafeefac-0013-0001-0020-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0013-0001-0020-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0013-0001-0021-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0013-0001-0021-
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0013-0001-0021-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0013-0001-0021-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0000-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0000-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0000-abcdeffedcbb}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0000-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0001-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0001-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0001-abcdeffedcbb}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0001-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0002-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0002-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0002-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0002-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0003-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0003-
 Opens key:
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0003-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0003-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0004-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0004-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0004-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0000-0004-
 Opens key:
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0000-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0000-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0000-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0000-
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0001-abcdeffedcba}
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0001-
 Opens kev:
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 key:
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}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0002-
abcdeffedcbb}\inprocserver32
 Opens key:
                          \label{local-condition} HKCU \setminus software \setminus classes \setminus clsid \setminus \{cafee fac-0014-0001-0003-abcdeffedcba\}
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0003-
 Opens key:
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0003-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0003-
 Opens kev:
abcdeffedcbb}\inprocserver32
                          \label{local_equation} \begin{tabular}{ll} HKCU \software \classes \clsid \cafeefac-0014-0001-0004-abcdeffedcba} \end{tabular}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0004-
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0004-abcdeffedcbb}
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0004-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-abcdeffedcbb}
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0006-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0006-
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0014-0001-0006-abcdeffedcbb}
```

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

abcdeffedcba}\inprocserver32

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0012-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0012-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0014-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0014-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0014-abcdeffedcbb}
 Opens key:
 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 key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0016-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0016-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0017-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0017-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0017-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0017-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0018-abcdeffedcba}
                         Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0018-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0018-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0019-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0019-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0019-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0019-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0021-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0021-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0021-abcdeffedcbb}
 Opens kev:
 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
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0022-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0022-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0023-abcdeffedcba}
 Opens kev:
 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 kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0024-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0025-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0025-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0025-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0025-
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:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0026-
abcdeffedcbb}\inprocserver32
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0027-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0027-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0027-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0027-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0028-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0028-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0028-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0028-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0029-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0029-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0029-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0029-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0030-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0030-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0030-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0030-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0031-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0031-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0031-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0031-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0032-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0032-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0032-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0032-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0033-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0033-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0033-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0033-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0034-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0034-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0034-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0034-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         Opens key:
                         Opens key:
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
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-
 Opens kev:
abcdeffedcba}\inprocserver32
                         \label{local-condition} \begin{tabular}{l} HKCU \software \classes \clsid \cafeefac-0015-0000-0001-abcdeffedcbb \end{tabular}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-abcdeffedcba}
```

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-
 Opens kev:
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:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-
 Opens kev:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-abcdeffedcba}
                         Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-
 Opens key
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-
 Opens kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-
 Opens kev
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-abcdeffedcba}
                         Opens key:
```

abcdeffedcba}\inprocserver32

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-
 Opens key:
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
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0014-abcdeffedcbb}
                         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
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-abcdeffedcbc}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-abcdeffedcba}
                         Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-abcdeffedcbc}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-abcdeffedcba}
 Opens kev:
 Opens key
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-abcdeffedcbc}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-
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 kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-
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
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-
 Opens key:
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}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-
 Opens kev:
abcdeffedcbc}\inprocserver32
                         \label{local-condition} \begin{tabular}{l} HKCU \software \classes \clsid \cafeefac-0015-0000-0029-abcdeffedcba \end{tabular}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-
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
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-abcdeffedcbc}
```

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-ffff-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-ffff-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-
 Opens kev:
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:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-
 Opens kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-abcdeffedcbb}
                         Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-
 Opens key
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-
 Opens kev
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-abcdeffedcbc}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-
 Opens kev
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-abcdeffedcbb}
                         Opens key:
```

abcdeffedcbb}\inprocserver32

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-
 Opens key:
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
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-abcdeffedcbc}
                         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 kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-abcdeffedcbb}
                         Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-abcdeffedcbc}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-abcdeffedcbc}
 Opens kev:
 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
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0013-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0013-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0013-abcdeffedcbc}
 Opens kev:
 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 kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0014-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0015-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0015-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0015-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0015-
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:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0016-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0016-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0016-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0016-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0016-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-abcdeffedcbc}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0017-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0018-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0018-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0018-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0018-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0018-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0018-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0019-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0020-
 Opens kev:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-
 Opens key:
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
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-
 Opens kev:
abcdeffedcba}\inprocserver32
                         \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \cafeefac-0016-0000-0023-abcdeffedcbb \end{tabular}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcdeffedcba}
```

Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0025abcdeffedcba}\inprocserver32 Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcdeffedcbb} HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-Opens key: abcdeffedcbb}\inprocserver32 Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcdeffedcbc} HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-Opens key: abcdeffedcbc}\inprocserver32 Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-abcdeffedcba} Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0026abcdeffedcba}\inprocserver32 Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-abcdeffedcbb} HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-Opens key: abcdeffedcbb}\inprocserver32 Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-abcdeffedcbc} Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0026abcdeffedcbc}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-abcdeffedcba} Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-Opens key: abcdeffedcba}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-abcdeffedcbb} Opens key: Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0027abcdeffedcbb}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-abcdeffedcbc} Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-Opens key: abcdeffedcbc}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-abcdeffedcba} Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-Opens key: abcdeffedcba}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-abcdeffedcbb} Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-Opens kev: abcdeffedcbb}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-abcdeffedcbc} Opens key: Opens key HKCU\software\classes\clsid\{cafeefac-0016-0000-0028abcdeffedcbc}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-abcdeffedcba} Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-Opens kev: abcdeffedcba}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-abcdeffedcbb} Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-Opens key: abcdeffedcbb}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-abcdeffedcbc} Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-Opens key: abcdeffedcbc}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0016-0000-ffff-abcdeffedcba} Opens kev: HKCU\software\classes\clsid\{cafeefac-0016-0000-ffff-Opens key abcdeffedcba}\inprocserver32 Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-abcdeffedcba} HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-Opens key: abcdeffedcba}\inprocserver32 $\label{local-equation} \begin{tabular}{ll} HKCU \software \classes \clsid \cafeefac-0017-0000-0000-abcdeffedcbb \end{tabular}$ Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-Opens key abcdeffedcbb}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-abcdeffedcbc} Opens key: Opens key: abcdeffedcbc}\inprocserver32 $\label{local-equation} \begin{tabular}{ll} HKCU \software \classes \clsid \cafeefac-0017-0000-0001-abcdeffedcba} \end{tabular}$ Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-Opens key abcdeffedcba}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-abcdeffedcbb} Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-Opens key: abcdeffedcbb}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-abcdeffedcbc} Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-Opens kev: abcdeffedcbc}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcba} Opens kev: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-Opens key: abcdeffedcba}\inprocserver32 Opens key: $\label{local-continuity} \mbox{HKCU\software\classes\clsid\{} cafeefac-0017-0000-0002-abcdeffedcbb\}}$ HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-Opens kev abcdeffedcbb}\inprocserver32 HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc} Opens kev: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-Opens key: abcdeffedcbc}\inprocserver32 Opens key: $\label{local-equation} HKCU \setminus software \setminus classes \setminus clsid \setminus \{cafeefac-0017-0000-ffff-abcdeffedcba\}$ HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-Opens key: abcdeffedcba}\inprocserver32 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{e19f9331-3110-11d4-991c-005004d3b3db\}$ Opens key: HKCU\software\classes\clsid\{e19f9331-3110-11d4-991c-Opens kev: 005004d3b3db}\inprocserver32

Opens key: HKCU\software\classes\javaplugin.1020
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
 Opens key:
                       HKCU\software\classes\software\microsoft\mediaplayer\preferences
 Opens key:
                       HKLM\software\microsoft\windows\currentversion\run
 Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
                       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
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
08002be10318}
 Opens key:
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000
 Opens key:
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage
                       HKLM\system\currentcontrolset\services\npf
 Opens key:
 Opens key:
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001
 Opens kev:
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\linkage
                       HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\ms
 Opens key:
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 key:
08002be10318}\0003
 Opens key:
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\linkage
                       Opens key:
08002be10318}\0004
 Opens key:
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004\linkage
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
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
 Opens key:
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\linkage
 Opens key:
                       08002be10318}\0007
 Opens key:
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\linkage
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
08002be10318}\0008
 Opens key:
                       08002be10318}\0008\linkage
 Opens key:
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009
                       Opens key:
08002be10318}\0009\linkage
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
08002be10318}\0010
 Opens key:
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010\linkage
                       HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens kev:
08002be10318}\0011
                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
08002be10318}\0011\linkage
 Opens key:
                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ndisnpp.dll
 Opens key:
                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
 Opens kev:
HKLM\software\microsoft\ctf\compatibility\70b2225f430facf31ca65621c234f09e.exe
 Opens key:
                       HKLM\software\microsoft\ctf\systemshared\
 Opens key:
                       HKCU\keyboard layout\toggle
 Opens key:
                       HKLM\software\microsoft\ctf\
 Opens key:
                       HKCU\software\far\plugins\ftp\hosts
                       HKCU \ software \ far 2 \ plugins \ ftp \ hosts
 Opens key:
 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 key: HKLM\system\currentcontrolset\control\productoptions

```
Opens key:
                         HKLM\software\policies\microsoft\windows\system
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003
                         HKCU\software\ghisler\windows commander
 Opens key:
 Opens key:
                         HKCU\software\ghisler\total commander
 Opens key:
                         HKLM\software\ghisler\windows commander
                         HKLM\software\ghisler\total commander
 Opens key:
                         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
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall
 Opens key:
                         HKLM \verb|\software\m| icrosoft \verb|\windows\currentversion\uninstall\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:
                         \label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \noindent all \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
                         HKI M\software\microsoft\windows\currentversion\uninstall\dxm runtime
 Opens kev:
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall\fontcore
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall\icw
 Opens key:
HKLM\software\microsoft\windows\currentversion\uninstall\idnmitigationapis
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall\ie40
 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
                         HKLM\software\microsoft\windows\currentversion\uninstall\ie8
 Opens key:
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall\iedata
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-v5
                         HKLM\software\microsoft\windows\currentversion\uninstall\microsoft .net
 Opens key:
framework 3.5 sp1
 Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus mobile option pack
 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
                         HKLM\software\microsoft\windows\currentversion\uninstall\pchealth
 Opens key:
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall\schedulingagent
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall\wic
                         Opens key:
3d01-b289-befc77a11a1e}
                         HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-
 Opens key:
4ca4-87b4-2f83217002ff}
                         HKLM\software\microsoft\windows\currentversion\uninstall\{350c97b0-3d7c-
 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:
                         HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-
11d3-8cfe-0150048383c9}
Opens key: 0409-0000-0000000ff1ce}
                         HKLM\software\microsoft\windows\currentversion\uninstall\{95120000-003f-
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-
0409-0000-0000000ff1ce}
                         HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-
 Opens key:
3813-a88d-b8dccde8f8c7}
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-
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:
                         HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-
36ca-84d3-9f4dcf5c5bd9}
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-
36ca-84d3-9f4dcf5c5bd9}.kb953595
 Opens key:
                         {\it 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
 Opens key:
                         HKCU\software\turboftp
                         HKCU\software\cryer\websitepublisher
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\control\computername
```

```
HKU\
 Opens key:
 Opens key:
                         HKCU\software\ftpclient\sites
 Opens key:
                         HKCU\software\softx.org\ftpclient\sites
 Opens key:
                         HKCU\software\martin prikryl\winscp 2\sessions
                         HKCU\software\vandyke\securefx
 Opens key:
 Opens key:
                         HKCU\software\globalscape\cuteftp 6 home\qctoolbar
                         HKCU\software\globalscape\cuteftp 6 professional\qctoolbar
 Opens key:
                         HKCU\software\globalscape\cuteftp 7 home\qctoolbar
 Opens key:
 Opens key:
                         HKCU\software\globalscape\cuteftp 7 professional\qctoolbar
 Opens key:
                         HKCU\software\globalscape\cuteftp 8 home\qctoolbar
 Opens key:
                         HKCU\software\globalscape\cuteftp 8 professional\qctoolbar
 Opens key:
                         HKCU\software\sota\ffftp\options
 Opens key:
                         HKCU\software\ftpware\coreftp\sites
 Opens key:
                         HKCU\software\south river technologies\webdrive\connections
 Opens key:
                         HKCU\software\nch software\classicftp\ftpaccounts
 Opens key:
                         HKLM\software\nch software\fling\accounts
 Opens kev:
                         HKCU\software\filezilla
 Opens key:
                         HKCU\software\filezilla\recent servers
 Opens key:
                         HKCU\software\filezilla\site manager
 Opens key:
                         HKCU\software\ftp explorer\profiles
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\uninstall\ultrafxp
 Opens key:
                         HKLM\software
                         HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Oueries value:
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                         \label{thm:local_equation} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \control session manager [safedll search mode] \end{tabular}
 Queries value:
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\gre_initialize[disablemetafiles]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\compatibility32[70b2225f430facf31ca65621c234f09e]
                         HKLM\software\microsoft\windows nt\currentversion\ime
 Oueries value:
compatibility[70b2225f430facf31ca65621c234f09e]
                         HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\locale[00000409]
                         HKLM\system\currentcontrolset\control\nls\language groups[1]
 Oueries value:
 Oueries value:
                         HKCU\control panel\desktop[multiuilanguageid]
                         HKLM\system\setup[systemsetupinprogress]
 Queries value:
 Queries value:
                         HKLM\system\wpa\pnp[seed]
 Oueries value:
                         HKLM\system\setup[osloaderpath]
 Queries value:
                         HKLM\system\setup[systempartition]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus setup [service pack cachepath] \\
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion[devicepath]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\setup[loglevel]
                         HKLM\software\microsoft\windows\currentversion\setup[logpath]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value:
                         HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
                         HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Oueries value:
 Queries value:
                         HKLM\hardware\description\system[identifier]
 Oueries value:
                         HKCU\control panel\desktop[smoothscroll]
 Oueries value:
HKLM\system\currentcontrolset\control\session
 Queries value:
manager[criticalsectiontimeout]
 Queries value:
                         HKLM\software\microsoft\ole[rwlockresourcetimeout]
                         HKCR\interface[interfacehelperdisableall]
 Queries value:
                         HKCR\interface[interfacehelperdisableallforole32]
 Oueries value:
 Queries value:
                         HKCR\interface[interfacehelperdisabletypelib]
                         HKCR\interface\{00020400-0000-0000-c000-
 Oueries value:
00000000046}[interfacehelperdisableall]
                         HKCR\interface\{00020400-0000-0000-c000-
 Queries value:
00000000046}[interfacehelperdisableallforole32]
                         Oueries value:
ab78-1084642581fb]
                         Oueries value:
0000-00000000000001
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Queries value:
```

 $\label{lem:hklm} \verb+KLM\+ system \verb+ current control set \verb+ services \verb+ tcpip \verb+ parameters [usedomain name devolution]$

Oueries value:

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

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: 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] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] $\label{lem:hklmsystem} \verb|HKLM| system| current control set | services| dnscache| parameters [use hosts file]| \\$ Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: $\label{lem:hklm} \verb+KLM\+ system \verb+ current control set \verb+ services \verb+ dns cache \verb+ parameters [register reverse lookup]+ of the lemma of the lemma$ HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register wan adapters]$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update top level domain zones]$ Oueries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[dnstest] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] 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] HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Oueries value: HKLM\svstem\currentcontrolset\services\tcpip\parameters[dnsmulticastquervtimeouts] Oueries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck] HKLM\software\microsoft\internet Oueries value:

 $explorer \verb|\main| featurecontrol \\ feature_protocol_lockdown[70b2225f430facf31ca65621c234f09e.exe]|$

Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]

Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[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]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]

Queries value:

 $HKLM \system \current control set \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \noon0000000010 \[packed catalog item] \\ Queries value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]

Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000001 [library path] \ Queries \ value:$

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000001 \ [displaystring] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[supportednamespace] Queries 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\00000000001[storesserviceclassinfo] Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\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\0000000000002[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]
 Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000000002 \ [version] \ Oueries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Oueries 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\00000000003[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog5 \catalog_entries \namespace_catalog5 \catalog5 \cat$

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog\_entries \ (00000000003[storesserviceclass info]) \ (catalog\_entries) \ 
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
    Queries value:
                                                            HKLM\software\microsoft\rpc[maxrpcsize]
    Oueries value:
                                                             HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
    Oueries value:
                                                             HKLM\system\currentcontrolset\services\winsock\parameters[transports]
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
    Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
    Queries value:
HKLM\svstem\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[2]
                                                             HKLM\system\currentcontrolset\control\nls\language groups[4]
    Oueries value:
    Queries value:
                                                             HKLM\system\currentcontrolset\control\nls\locale[00000419]
    Queries value:
                                                             HKCU\software\microsoft\internet explorer\main[]
    Oueries value:
                                                             HKCU\software\microsoft\internet explorer\main[usecompressedline]
    Queries value:
                                                             HKCU\software\microsoft\internet explorer\main[themeenablednext]
    Queries value:
                                                             HKCU\software\microsoft\internet explorer\main[dbcompresseduse]
    Oueries value:
                                                             HKCU\software\microsoft\internet explorer\main[flagschangedpersistent]
    Queries value:
                                                             HKCU\software\microsoft\internet explorer\main[stateplayedprev]
    Queries value:
                                                             HKLM\software\microsoft\windows\currentversion\run[sonyagent]
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
c7d49d7cecdc}[leaseobtainedtime]
c7d49d7cecdc}[leaseterminatestime]
    Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-abe3-4304-a
c7d49d7cecdc}[dhcpserver]
                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Queries value:
08002be10318}\0000[componentid]
    Queries value:
                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage[export]
    Queries value:
                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001[componentid]
                                                            Queries value:
08002be10318}\0001\linkage[export]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[domain]
    Queries 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:
c7d49d7cecdc}[registeradaptername]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
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:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpipaddress]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
```

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

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

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

c7d49d7cecdc}[dhcpsubnetmask]

08002be10318}\0002[componentid]

08002be10318}\0003[componentid]

08002be10318}\0002\linkage[export]

Queries value:

Oueries value:

Queries value:

Queries value:

```
08002be10318}\0003\linkage[export]
 Oueries value:
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[componentid]
 Queries value:
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004\linkage[export]
 Queries value:
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[componentid]
 Oueries value:
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005\linkage[export]
 Queries value:
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[componentid]
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value:
08002be10318}\0006\linkage[export]
                         Oueries value:
08002be10318}\0007[componentid]
 Queries value:
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\linkage[export]
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value:
08002be10318}\0008[componentid]
 Queries value:
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\linkage[export]
 Queries value:
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009[componentid]
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value:
08002be10318}\0009\linkage[export]
 Queries value:
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[componentid]
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value:
08002be10318}\0010\linkage[export]
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value:
08002be10318}\0011[componentid]
 Queries value:
                         HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\linkage[export]
 Queries value:
                         HKLM\software\microsoft\ctf\systemshared[cuas]
 Oueries value:
                         HKCU\keyboard layout\toggle[language hotkey]
                         HKCU\keyboard layout\toggle[hotkey]
 Queries value:
 Oueries value:
                         HKCU\kevboard lavout\toggle[lavout hotkev]
 Oueries value:
                         HKLM\software\microsoft\ctf[enableanchorcontext]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[userenvdebuglevel]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
                         HKLM\system\currentcontrolset\control\productoptions[producttype]
 Oueries value:
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
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]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\uninstall\addressbook[uninstallstring]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash
player activex[uninstallstring]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash
player activex[displayname]
 Queries value:
HKLM \ software \ microsoft \ windows \ current version \ uninstall \ branding [uninstall string]
 Queries value:
                         manager[uninstallstring]
 Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\directanimation[uninstallstring]
 Queries value:
HKLM \ software \ microsoft \ windows \ current version \ uninstall \ direct drawex \ [uninstall string]
 Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\dxm runtime[uninstallstring]
 Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\fontcore[uninstallstring]
 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]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie4data[uninstallstring]
 Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie5bakex[uninstallstring]
 Queries value:
```

```
HKLM\software\microsoft\windows\currentversion\uninstall\ie7[uninstallstring]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie8[uninstallstring]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie8[displayname]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\iedata[uninstallstring]
   Oueries value:
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-
v5[uninstallstring]
   Queries value:
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-
v5[displayname]
   Queries value:
                                                     framework 3.5 sp1[uninstallstring]
   Queries value:
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\microsoft .net
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\software\microsoft\windows\currentversion\uninstall\netmeeting[uninstallstring]
   Queries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus nlsdownlevel mapping [uninstall string]
Queries value:
HKLM \ software \ microsoft \ windows \ current version \ uninstall \ pchealth [uninstall string]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\pchealth[displayname]
HKLM\software\microsoft\windows\currentversion\uninstall\schedulingagent[uninstallstring]
   Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\wic[uninstallstring]
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-
   Queries value:
3d01-b289-befc77a11a1e}[uninstallstring]
                                                     Queries value:
3d01-b289-befc77a11a1e}[displayname]
   Oueries value:
                                                     HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{26a24ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-14ae4-039d-1
4ca4-87b4-2f83217002ff}[uninstallstring]
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-
   Queries value:
4ca4-87b4-2f83217002ff}[displayname]
   Queries value:
                                                     4ee8-baa9-00bcb3d54227}[uninstallstring]
   Queries value:
                                                     4037-7777-5f2748764d10}[uninstallstring]
   Queries value:
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-
0409-0000-0000000ff1ce}[uninstallstring]
   Queries value:
                                                     0409-0000-0000000ff1ce}[displayname]
   Queries value:
                                                     11d3-8cfe-0150048383c9}[uninstallstring]
   Oueries value:
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-
11d3-8cfe-0150048383c9}[displayname]
   Queries value:
                                                     0409-0000-0000000ff1ce}[uninstallstring]
   Queries value:
                                                     0409-0000-0000000ff1ce}[displayname]
   Oueries value:
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-
0409-0000-0000000ff1ce}[uninstallstring]
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-
   Queries value:
0409-0000-0000000ff1ce}[displayname]
   Queries value:
                                                     3813-a88d-b8dccde8f8c7}[uninstallstring]
   Oueries value:
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-
3813-a88d-b8dccde8f8c7}[displayname]
   Oueries value:
                                                     HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76ba86-7ad7-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac76-4ac
1033-7b44-a93000000001}[uninstallstring]
   Queries value:
                                                     HKLM \ software \ `microsoft\ `windows \ `current version \ `uninstall\ \{ac76ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86-7ad7-140ba86
1033-7b44-a9300000001}[displayname]
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-
   Oueries value:
3f2d-899a-6a1d67f2073f}[uninstallstring]
   Oueries value:
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-
3f2d-899a-6a1d67f2073f}[displayname]
   Queries value:
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-
4027-b136-2b3e1f5ab6e2}[uninstallstring]
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-
   Oueries value:
4027-b136-2b3e1f5ab6e2}[displayname]
   Oueries value:
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-
36ca-84d3-9f4dcf5c5bd9}[uninstallstring]
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-
   Queries value:
36ca-84d3-9f4dcf5c5bd9}[displayname]
                                                     HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-
   Oueries value:
36ca-84d3-9f4dcf5c5bd9}.kb953595[uninstallstring]
```

Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-

36ca-84d3-9f4dcf5c5bd9}.kb953595[displayname]

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

folders[local appdata]

Queries value:

lue: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders[common appdata]

Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir] Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]

 Queries value:
 HKLM\software[debuglogpath]

 Queries value:
 HKLM\software[debugloglevel]

 Queries value:
 HKLM\software[enabledebuglog]

Sets/Creates value: HKCU\software\microsoft\internet explorer\main[usecompressedline]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[themeenablednext]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[dbcompresseduse]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[flagschangedpersistent]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[stateplayedprev]

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[stateplayedprev]