Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 620, Task ID: 2426

Task ID: 2426 Risk Level: 10

Date Processed: 2016-02-22 05:28:39 (UTC)

Processing Time: 61.91 seconds
Virtual Environment: IntelliVM

Execution Arguments:

"c:\windows\temp\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe"

Sample ID: 620 Type: basic Owner: admin

Label: 188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5

Date Added: 2016-02-22 05:26:49 (UTC)

File Type: PE32:win32:gui File Size: 838656 bytes

MD5: 0feaaa4adc31728e54b006ab9a7e6afa

SHA256: 188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5

Description: None

Pattern Matching Results

3 Connects to local host

6 Modifies registry autorun entries

10 Creates malicious events: Kelihos trojan 2 [Spam]

6 Writes to system32 folder

5 Adds autostart object

5 Creates file in drivers folder

5 PE: Contains compressed section

Process/Thread Events

Creates process:

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

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

 $\label{lem:continuous} $$\operatorname{Creates semaphore:}$ $$\operatorname{Semaphore:}$ $$\operatorname{Sem$

File System Events

Creates:	<pre>C:\WINDOWS\Temp\tmp.exe</pre>
Creates:	<pre>C:\WINDOWS\system32\Packet.dll</pre>
Creates:	C:\WINDOWS\system32\wpcap.dll
Creates:	C:\WINDOWS\system32\drivers\npf.sy

Opens: C:\WINDOWS\Prefetch\188AB310143D0C0C9673D957FCFE7-0E6E254C.pf

Opens: C:\Documents and Settings\Admin C:\WINDOWS\system32\clusapi.dll Opens: Opens: C:\WINDOWS\system32\imm32.dll Opens: C:\WINDOWS\system32\cmutil.dll Opens: C:\WINDOWS\system32\dnsapi.dll Opens: C:\WINDOWS\system32\ws2_32.dll Opens: C:\WINDOWS\svstem32\ws2help.dll Opens: C:\WINDOWS\system32\iphlpapi.dll C:\WINDOWS\system32\mswsock.dll Opens: Opens: C:\WINDOWS\system32\psapi.dll Opens: C:\WINDOWS\system32\shell32.dll

Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83

Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll

Opens: C:\WINDOWS\WindowsShell.Manifest

```
C:\WINDOWS\WindowsShell.Config
 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\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Config
 Opens:
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
 Opens:
C:\WINDOWS\Temp\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe
 Opens:
                         C:\WINDOWS\Temp
                         C:\WINDOWS\Temp\tmp.exe
 Opens:
 Opens:
                         C:\WINDOWS\Temp\1145163a-23bc-4d54-bace-0f5599267294
 Opens:
                         C:\dev\urandom
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\
 Opens:
                         C:\AUTOEXEC.BAT
 Opens:
                         C:\boot.ini
 Opens:
                         C:\CONFIG.SYS
                         C:\Documents and Settings
 Opens:
                         C:\Documents and Settings\Admin\Application Data
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\AdobeCMapFnt09.1st
                         C:\WINDOWS\system32\drivers
 Opens:
 Opens:
                         C:\WINDOWS\system32\wpcap.dll
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\AdobeSysFnt09.1st
 Opens:
                         C:\WINDOWS\system32\wpcap.dll.2.Manifest
 Opens:
                         C:\WINDOWS\system32\wpcap.dll.2.Config
                         C:\WINDOWS\system32\Packet.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\packet.dll.2.Manifest
 Opens:
                         C:\WINDOWS\system32\packet.dll.2.Config
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0\Forms
 Opens:
                         C:\WINDOWS\system32\npptools.dll
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Acrobat\9.0\JavaScripts\glob.js
                         C:\WINDOWS\system32\mfc42u.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\drivers\npf.sys
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts\glob.settings.js
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\SharedDataEvents
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\UserCache.bin
                         C:\Documents and Settings\Admin\Application Data\Adobe\Flash Player
 Opens:
 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
                         C:\Documents and Settings\Admin\Application Data\Adobe\Linguistics
 Opens:
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Linguistics\Dictionaries
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\all
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\brt
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\can
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\eng
                         C:\Documents and Settings\Admin\Application Data\Adobe\LogTransport2
 Opens:
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\LogTransport2\Logs
                         C:\Documents and Settings\Admin\Application Data\desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Identities
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Identities\{5792731B-
1E8B-4ECF-8560-0E560368800D}
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Macromedia
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
```

```
Player\macromedia.com
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support
                                    C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys
                                    C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
  Opens:
Player\macromedia.com\support\flashplayer\sys\settings.sol
                                    C:\WINDOWS\system32\npp\ndisnpp.dll
  Opens:
  Opens:
                                    C:\WINDOWS\system32\rpcss.dll
  Opens:
                                    C:\WINDOWS\system32\MSCTF.dll
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\AddIns
  Opens:
  Opens:
                                    C:\WINDOWS\system32\npp
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Credentials
  Opens:
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-1003
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\0797C381B2F87EB5A1D5573BD15BA4F4
  Opens:
                                    C:\Documents and Settings\Admin\Application
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
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\62B5AF9BE9ADC1085C3C56EC07A82BF6
                                    C:\WINDOWS\win.ini
  Opens:
  Opens:
                                    C:\Users\
  Opens:
                                    C:\Documents and Settings\Admin\Application
\label{lem:lambda} Data\Microsoft\Cryptnet\UrlCache\Content\\ \land 696F3DE637E6DE85B458996D49D759AD
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7396C420A8E1BC1DA97F1AF0D10BAD21
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE8E7EB5F575EC9
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\8DFDF057024880D7A081AFBF6D26B92F
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\A44F4E7CB3133FF765C39A53AD8FCFDD
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\F482C95F83F1B59228F1B1E720F2EDF1
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\0797C381B2F87EB5A1D5573BD15BA4F4
  Opens:
                                    C:\Documents and Settings\Admin\Application
\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
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\3130B1871A126520A8C47861EFE3ED4D
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\60E31627FDA0A46932B0E5948949F2A5
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\62B5AF9BE9ADC1085C3C56EC07A82BF6
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7396C420A8E1BC1DA97F1AF0D10BAD21
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7B2238AACCEDC3F1FFE8E7EB5F575EC9
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\8DFDF057024880D7A081AFBF6D26B92F
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\A44F4E7CB3133FF765C39A53AD8FCFDD
  Opens:
                                    C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\F482C95F83F1B59228F1B1E720F2EDF1
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
1-5-21-1757981266-507921405-1957994488-1003
```

 ${\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Crypto\RSA\S-relation\ Data\Microsoft\Crypto\RSA\S-relation\ Data\Microsoft\Crypto\RSA\S-relation\ Data\Microsoft\Crypto\RSA\S-relation\ Data\Microsoft\Crypto\RSA\S-relation\ Data\Microsoft\Crypto\RSA\S-relation\ Data\Microsoft\Crypto\RSA\S-relation\ Data\Microsoft\Crypto\RSA\S-relation\ Data\Microsoft\RSA\S-relation\ Data\Microsoft\No. And Application\ Data\Microsoft\No. And Application\Microsoft\No. And Application\Micr$

Opens:

```
1-5-21-1757981266-507921405-1957994488-1003\6b29ae44e85efac3c72ff4d1865d73f1_fa860dc5-a965-4200-
a9d4-fb930ff1911b
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
1-5-21-1757981266-507921405-1957994488-1003\83aa4cc77f591dfc2374580bbd95f6ba_fa860dc5-a965-4200-
a9d4-fb930ff1911b
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
   Opens:
Explorer\brndlog.bak
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\brndlog.txt
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Desktop.htt
                                               {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Internet}
   Opens:
Explorer\Quick Launch
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Ouick Launch\desktop.ini
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
   Opens:
Explorer\Quick Launch\Show Desktop.scf
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Media Player
                                               {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\MMC}
   Opens:
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Office
   Opens:
                                               C:\Documents and Settings\Admin\Application
Data\Microsoft\Office\Excel12.pip
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Office\Recent
   Opens:
                                               C:\Documents and Settings\Admin\Application
   Opens:
Data\Microsoft\Office\Recent\Desktop.ini
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Protect
   Opens:
                                               C:\Documents and Settings\Admin\Application
   Opens:
Data\Microsoft\Protect\CREDHIST
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
   Opens:
5-21-1757981266-507921405-1957994488-1003
                                               \label{lem:condition} C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Prote
   Opens:
5-21-1757981266-507921405-1957994488-1003\3ea8a527-1704-4983-8596-ab49c663cca3
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
   Opens:
5-21-1757981266-507921405-1957994488-1003\4f5d6884-c60c-4cd3-906b-3d677949fac1
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
   Opens:
5-21-1757981266-507921405-1957994488-1003\fe1a937a-0ac9-4cf1-978d-5d0742ed2858
                                               \label{lem:condition} C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Protect\No.\Prote
5-21-1757981266-507921405-1957994488-1003\Preferred
                                               C:\Documents and Settings\Admin\Application Data\Microsoft\Speech
   Opens:
                                               {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Speech\Files}
   Opens:
                                               C:\Documents and Settings\Admin\Application
   Opens:
Data\Microsoft\Speech\Files\UserLexicons
   Opens:
                                               C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons\SP_6A65DB879F95470886BD7EFE4977B10E.dat
                                               C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\SystemCertificates
   Opens:
                                               C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My
   Opens:
                                               C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\Certificates
                                               C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\SystemCertificates\My\CRLs
   Opens:
                                               C:\Documents and Settings\Admin\Application
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
Data\Microsoft\Windows\Themes\Custom.theme
                                               C:\Documents and Settings\Admin\Application Data\Oracle
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Oracle\Java
   Opens:
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Oracle\Java\Uninstall
   Opens:
                                               {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Sun}
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Sun\Java
                                               C:\Documents and Settings\Admin\Application Data\Sun\Java\AU
   Opens:
   Opens:
                                               C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment
                                               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
Data\Sun\Java\Deployment\cache\6.0\0
   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:
Data\Sun\Java\Deployment\cache\6.0\11
```

```
Opens:
                                      C:\Documents and Settings\Admin\Application
Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171
                                      C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171.idx
                                      C:\Documents and Settings\Admin\Application
  Opens:
C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\14
                                      C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\15
                                      C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\16
                                      C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\17
                                      C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c
                                      C:\Documents and Settings\Admin\Application
  Opens:
C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-6.0.lap
  Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\18
  Opens:
                                      C:\Documents and Settings\Admin\Application
C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1
  Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1.idx
                                      C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-6.0.lap
  Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\2
  Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\20
                                      C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\21
  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
                                      C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\24
  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
  Opens:
                                      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
                                      C:\Documents and Settings\Admin\Application
  Opens:
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
                                      C:\Documents and Settings\Admin\Application
  Opens:
Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\33
  Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\34
                                      C:\Documents and Settings\Admin\Application
  Opens:
Data \S un \S ava \S eployment \S ava \S eployment \S ava \S eployment \S eployment \S ava \S eployment \S eplo
  Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\36
  Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\37
                                      C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\38
  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
  Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\40
                                      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
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\43
 Opens:
                         C:\Documents and Settings\Admin\Application
Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d.idx
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\44
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\45
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\46
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\47
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\48
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\49
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\5
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\50
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\51
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\52
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\53
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\54
                         {\tt C:\Documents\ and\ Settings\Admin\Application}
 Opens:
Data\Sun\Java\Deployment\cache\6.0\55
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\56
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\57
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\58
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\59
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\6
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\60
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\61
 Opens:
                         C:\Documents and Settings\Admin\Application
Opens:
                         C:\Documents and Settings\Admin\Application
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
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\9
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\host
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\lastAccessed
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\muffin
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\tmp
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\deployment.properties
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Sun\Java\Deployment\ext}}
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\log
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\security
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\security\trusted.certs
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\tmp
 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
                         C:\Documents and Settings\Admin\Cookies\admin@c1.microsoft[2].txt
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt
 Opens:
                         C: \verb|\Documents| and Settings \verb|\Admin| Cookies \verb|\admin| @rto.microsoft[1].txt|
                         C:\Documents and Settings\Admin\Cookies\admin@search.microsoft[1].txt
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt
```

```
Opens:
                         C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[3].txt
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Desktop
 Opens:
                         C:\Documents and Settings\Admin\Favorites
                         C:\Documents and Settings\Admin\Favorites\Desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Links
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Links\desktop.ini
                         C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Links\Suggested Sites.url
 Opens:
                         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
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Home.url
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Work.url
                         C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
 Opens:
Store.url
 Opens:
                         C:\Documents and Settings\Admin\Favorites\MSN.com.url
                         C:\Documents and Settings\Admin\Favorites\Radio Station Guide.url
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\IECompatCache
 Opens:
                         C:\Documents and Settings\Admin\IECompatCache\index.dat
                         {\tt C:\Documents\ and\ Settings\Admin\IETldCache}
 Opens:
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\IETldCache\index.dat}\\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings
                         C:\Documents and Settings\Admin\Local Settings\Application Data
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Acrobat
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Adobe\Acrobat\9.0
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Acrobat\9.0\Cache\AcroFnt09.1st
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Acrobat\9.0\Cache\Search
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\Acrobat\9.0\Updater
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Acrobat\9.0\Updater\updater.log
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Color
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\Color\ACECache10.lst
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Updater6
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Updater6\aum.log
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Updater6\aumLib.log
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Updater6\Install
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\GDIPFONTCACHEV1.DAT
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\IconCache.db
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\CD Burning
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Credentials
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-1003
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\FeedsStore.feedsdb-ms
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds\Microsoft Feeds~
 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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
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
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
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]
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\G4DZ1I7H
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\G4DZ1I7H\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\G4DZ1I7H\fwlink[1]
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\J3XY1QNV
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\J3XY1QNV\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\J3XY1QNV\fwlink[1]
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Microsoft\Feeds Cache\TLMHA51J
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\TLMHA51J\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\TLMHA51J\ieonline.microsoft[1]
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\brndlog.bak
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\brndlog.txt
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
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
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Internet Explorer\DOMStore
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\DOMStore\OWORJP5C
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK\www.microsoft[1].xml
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\LQLIM8KB
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\frameiconcache.dat
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Last Active
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{80236AC0-AAD6-11E3-AE20-
08002733366F}.dat
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Services
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
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
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
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
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Windows Media
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application Data\Sun
                         C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java
 Opens:
                         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
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\0
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
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
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\11
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\12
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Sun\Java\Deployment\cache\6.0\13
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\14
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\15
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\16
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\17
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\18
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\19
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\20
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\21
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\22
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\23
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\24
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\25
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\26
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\27
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\28
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\29
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
```

Data\Sun\Java\Deployment\cache\6.0\3			
, ,	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\30 Opens: C:\Documents		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\31	anu	Sectings (AdmitiveCotal	Sectings (Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\32		Settings\Admin\Local	Settings\Application
' '		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
Opens: C:\Documents		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\35 Opens: C:\Documents	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\36		Sectings (Mainth (Escat	Sectings (Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\37		Settings\Admin\Local	Settings\Application
Opens: C:\Documents	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\38 Opens: C:\Documents		Cottings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\39		Sectings (AdmitiveOcal	Sectings (Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\4	and	Settings\Admin\Local	Settings\Application
. ,	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\40			5 · · ·
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\41	and	Settings\Admin\Local	Settings\Application
Opens: C:\Documents		Settings\Admin\Local	${\tt Settings \verb \Application }$
Data\Sun\Java\Deployment\cache\6.0\42 Opens: C:\Documents		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\43		· ·	0 11
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 Opens: C:\Documents		Settings\Admin\Local	Settings\Annlication
Data\Sun\Java\Deployment\cache\6.0\45			Sectings (Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\45			Settings\Application
			Settings\Application
Data\Sun\Java\Deployment\cache\6.0\46	and	Cottings \ Admin \ Local	Settings\Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\47	anu	Settings (Admitit/Local	Settings (Application
•		•	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\47' Opens: C:\Documents			Settings\Application
Data\Sun\Java\Deployment\cache\6.0\47			5
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\48		Settings\Admin\Local	Settings\Application
Opens: C:\Documents	and	Settings\Admin\Local	${\tt Settings \verb \Application }$
Data\Sun\Java\Deployment\cache\6.0\49 Opens: C:\Documents		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\5		· ·	0 11
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\50	and	Settings\Admin\Local	Settings\Application
Opens: C:\Documents	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\51 Opens: C:\Documents	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\52		· ·	0 11
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\53		Settings\Admin\Local	Settings\Application
		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\54 Opens: C:\Documents		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\55	anu	Sectings (AdmitiveOcal	Sectings (Application
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\56		Settings\Admin\Local	Settings\Application
		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\57		C-++:\	C-++:\
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\58		Settings (Admith/Local	Settings\Application
Opens: C:\Documents		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\59 Opens: C:\Documents	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\6		•	
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\60		Settings\Admin\Local	Settings\Application
Opens: C:\Documents		Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\61 Opens: C:\Documents	and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment\cache\6.0\62		•	
Opens: C:\Documents Data\Sun\Java\Deployment\cache\6.0\63		Settings\Admin\Local	Settings\Application

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\7
 Opens:
                         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
 Opens:
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\8
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\lastAccessed
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\muffin
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\tmp
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\desktop.ini
                         C:\Documents and Settings\Admin\Local
 Opens:
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\History\History.IE5\MSHist012014031220140313\index.dat
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014033120140407
                         C:\Documents and Settings\Admin\Local
Settings \verb|\History\History\IE5\MSHist012014033120140407 \verb|\Index.dat| \\
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014041220140413\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Temp
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\296c0.msp
                         C:\Documents and Settings\Admin\Local Settings\Temp\AdobeARM.log
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\AdobeARM_NotLocked.log
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ASPNETSetup_00000.log
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ASPNETSetup_00001.log
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\AUCHECK_PARSER.txt
                         C:\Documents and Settings\Admin\Local Settings\Temp\Compatibility Pack
 Opens:
for the 2007 Office system (0).log
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_clwireg.txt
 Opens:
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_depcheck_NETFX_EXP_35.txt
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_dotnetfx35error.txt
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_dotnetfx35install.txt
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_NET_Framework20_Setup164F.txt
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework30_Setup16AE.txt
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework35_MSI16E2.txt
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_NET_Framework35_MSI63E0.txt
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_RGB9RAST_x86.msi601E.txt
                         {\tt 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
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA35A0.txt
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_XPS.txt
                         C:\Documents and Settings\Admin\Local Settings\Temp\gen_py
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\gen_py\2.7
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\gen_py\2.7\dicts.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\gen_py\2.7\__init__.py
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin
                         C:\Documents and Settings\Admin\Local Settings\Temp\JAUReg.log
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\java_install.log
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\java_install_reg.log
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\jusched.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft PowerPoint
 Opens:
```

Viewer (0).log

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_10.0.30319
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20131223_035827352-MSI_vc_red.msi.txt
                         {\tt 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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_152314679.html
                         \hbox{C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft\ Visual\ C++}
 Opens:
2010 x86 Redistributable Setup_20140312_152634747-MSI_vc_red.msi.txt
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_152634747.html
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_154212618-MSI_vc_red.msi.txt
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Opens:
2010 x86 Redistributable Setup_20140312_154212618.html
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\pywin32_postinstall.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\setup.log
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Silverlight0.log
                         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:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\AntiPhishing
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\AntiPhishing\2CEDBFBC-DBA8-43AA-B1FD-CC8E6316E3E2.dat
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5
 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 \verb|\CONTENT.IE5| CXCXW1MR \verb|\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
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\CXCXW1MR\ADSAdClient31[1].txt
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[2].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files \verb|\Content.IE5| CXCXW1MR \verb|\ADSAdClient31[3].txt|
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[4].txt
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[5].txt
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\adServer[1].htm
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\auth016[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\bimapping[2].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\broker[1].js
                         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
 Opens:
                         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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\event[3].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[5].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\install[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\js[2].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\LoginStatus[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\onemscomfooter[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[3].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\request[1].php
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\ScriptResource[1].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\ScriptResource[2].axd
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[3].axd
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\ScriptResource[4].axd
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[5].axd
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\script[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\script[1].jsx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\script[2].jsx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\true[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\true[2].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\views[1]
 Opens:
                         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 \verb|\| CXCXW1MR \verb|\| wtid[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
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
 Opens:
                         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
 Opens:
Files\Content.IE5\ONWV4FIP\auth016[2].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\bing[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\broker-config_s1[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\broker-config_s1[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\broker-config_s1[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\CA39W67Q.jsx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\CAANG12B.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\CAU35S9Y.isx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\ChangePassword[1].css
                         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
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\ONWV4FIP\core114[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\counter017[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\counter017[2].js
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\ONWV4FIP\css[1].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\css[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\details[2].htm
 Opens:
                         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
 Opens:
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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\Install[11.css
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[1].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[2].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[3].ashx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\js[4].ashx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\Login[1].css
                         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
                         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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\ScriptResource[1].axd
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\ONWV4FIP\ScriptResource[2].axd
```

```
Opens:
                                               C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\script[2].jsx
   Opens:
                                               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
   Opens:
Files\Content.IE5\ONWV4FIP\serverComponent[1].php
   Opens:
                                               C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\siteresource[1].ashx
   Opens:
                                               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
   Opens:
Files\Content.IE5\ONWV4FIP\style[1].cssx
   Opens:
                                               C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\Tracker[1].js
   Writes to:
                                               C:\WINDOWS\system32\Packet.dll
   Writes to:
                                               C:\WINDOWS\system32\wpcap.dll
   Writes to:
                                               C:\WINDOWS\system32\drivers\npf.sys
   Reads from:
                                               C:\AUTOEXEC.BAT
   Reads from:
                                               C:\boot.ini
                                               C:\CONFIG.SYS
   Reads from:
   Reads from:
                                               C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\AdobeCMapFnt09.lst
   Reads from:
                                               C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\AdobeSysFnt09.lst
   Reads from:
                                               C:\Documents and Settings\Admin\Application
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
                                               C:\Documents and Settings\Admin\Application
   Reads from:
Data\Adobe\Acrobat\9.0\SharedDataEvents
   Reads from:
                                               C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\UserCache.bin
                                               C:\Documents and Settings\Admin\Application Data\desktop.ini
   Reads from:
   Reads from:
                                               C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
                                               C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\0797C381B2F87EB5A1D5573BD15BA4F4
   Reads from:
                                               C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\135BD6A358680A7BF1CCEC7C0172393D
                                               C:\Documents and Settings\Admin\Application
   Reads from:
\label{lem:lambda} Data \\ \mbox{Microsoft} \\ \mbox{CryptnetUrlCache} \\ \mbox{Content} \\ \mbox{2BF68F4714092295550497DD56F57004} \\ \mbox{Content} \\ \mbox{Cont
                                               C:\Documents and Settings\Admin\Application
   Reads from:
Data\Microsoft\CryptnetUrlCache\Content\3130B1871A126520A8C47861EFE3ED4D
   Reads from:
                                               C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\60E31627FDA0A46932B0E5948949F2A5
                                               C:\Documents and Settings\Admin\Application
   Reads from:
Reads from:
                                               C:\WINDOWS\win.ini
   Reads from:
                                               C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D49D759AD
                                               C:\Documents and Settings\Admin\Application
   Reads from:
\label{lem:decomposition} Data \\ \mbox{Microsoft} \\ \mbox{CryptnetUrlCache} \\ \mbox{Content} \\ \mbox{7396C420A8E1BC1DA97F1AF0D10BAD21} \\ \mbox{Content} \\ \mb
   Reads from:
                                               C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE8E7EB5F575EC9
                                               C:\Documents and Settings\Admin\Application
   Reads from:
Data\Microsoft\CryptnetUrlCache\Content\8DFDF057024880D7A081AFBF6D26B92F
                                               C:\Documents and Settings\Admin\Application
   Reads from:
Data\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015
   Reads from:
                                               C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\A44F4E7CB3133FF765C39A53AD8FCFDD
   Reads from:
                                               C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\F482C95F83F1B59228F1B1E720F2EDF1
                                               C:\Documents and Settings\Admin\Application
   Reads from:
Data\Microsoft\CryptnetUrlCache\MetaData\0797C381B2F87EB5A1D5573BD15BA4F4
   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
                                               C:\Documents and Settings\Admin\Application
   Reads from:
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
```

C:\Documents and Settings\Admin\Application

Reads from:

```
Data\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015
                                   C:\Documents and Settings\Admin\Application
  Reads from:
Data\Microsoft\CryptnetUrlCache\MetaData\A44F4E7CB3133FF765C39A53AD8FCFDD
  Reads from:
                                   C:\Documents and Settings\Admin\Application
\label{lem:decomp} Data \\ \mbox{Microsoft} \\ \mbox{CryptnetUrlCache} \\ \mbox{MetaData} \\ \mbox{F482C95F83F1B59228F1B1E720F2EDF1} \\ \mbox{Microsoft} \\ \mbox{CryptnetUrlCache} \\ \mbox{MetaData} \\ \mbox{MetaData
  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:
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
1-5-21-1757981266-507921405-1957994488-1003\83aa4cc77f591dfc2374580bbd95f6ba_fa860dc5-a965-4200-
a9d4-fb930ff1911b
  Reads from:
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\brndlog.bak
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
  Reads from:
Explorer\brndlog.txt
  Reads from:
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Desktop.htt
  Reads from:
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\desktop.ini
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
  Reads from:
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
  Reads from:
Explorer\Ouick Launch\Show Desktop.scf
  Reads from:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\Office\Excel12.pip
                                   {\tt C:\Documents\ and\ Settings\Admin\Application}
  Reads from:
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
  Reads from:
                                   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-
5-21-1757981266-507921405-1957994488-1003\Preferred
                                   {\tt C:\Documents\ and\ Settings\Admin\Application}
  Reads from:
Data\Microsoft\Speech\Files\UserLexicons\SP_6A65DB879F95470886BD7EFE4977B10E.dat
                                   C:\Documents and Settings\Admin\Application
  Reads from:
Data\Microsoft\Windows\Themes\Custom.theme
                                   {\tt C:\Documents\ and\ Settings\Admin\Application}
  Reads from:
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171
  Reads from:
                                   C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171.idx
                                   C:\Documents and Settings\Admin\Application
  Reads from:
C:\Documents and Settings\Admin\Application
Reads from:
                                   C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-6.0.lap
                                   C:\Documents and Settings\Admin\Application
  Reads from:
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1
  Reads from:
                                   C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1.idx
  Reads from:
                                   C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-6.0.lap
                                   C:\Documents and Settings\Admin\Application
  Reads from:
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d
                                   C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d.idx
  Reads from:
                                   C:\Documents and Settings\Admin\Application
C:\Documents and Settings\Admin\Application
  Reads from:
Data\Sun\Java\Deployment\deployment.properties
                                   C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\security\trusted.certs
                                   C: \verb|\Documents| and Settings\\| Admin\\| Cookies\\| admin\\| @c1.microsoft[2].txt
  Reads from:
  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
                                   C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt
  Reads from:
  Reads from:
                                   C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[3].txt
  Reads from:
                                   C:\Documents and Settings\Admin\Cookies\index.dat
  Reads from:
                                   C:\Documents and Settings\Admin\Favorites\Desktop.ini
  Reads from:
                                   C:\Documents and Settings\Admin\Favorites\Links\desktop.ini
  Reads from:
                                   C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url
                                   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
 Reads from:
                         C:\Documents and Settings\Admin\Favorites\MSN.com.url
                         C:\Documents and Settings\Admin\Favorites\Radio Station Guide.url
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\IECompatCache\index.dat
 Reads from:
                         C:\Documents and Settings\Admin\IETldCache\index.dat
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache\AcroFnt09.lst
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Adobe\Acrobat\9.0\Updater\updater.log
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Color\ACECache10.lst
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Adobe\Updater6\aum.log
 Reads from:
                         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:
                         C:\Documents and Settings\Admin\Local Settings\Application
{\tt 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
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Suggested Sites~.feed-ms
                         {\tt 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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\FBANKAIW\desktop.ini
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Reads from:
Data\Microsoft\Feeds Cache\FBANKAIW\fwlink[1]
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\G4DZ1I7H\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\G4DZ1I7H\fwlink[1]
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY10NV\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY1QNV\fwlink[1]
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Feeds Cache\TLMHA51J\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Feeds Cache\TLMHA51J\ieonline.microsoft[1]
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\brndlog.bak
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Internet Explorer\brndlog.txt
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Custom Settings\CustomO\install.ins
 Reads from:
                         {\tt 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:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Internet Explorer\Recovery\Active\{49831954-C276-11E3-AE24-08002733366F}.dat
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{80236AC0-AAD6-11E3-AE20-
08002733366F}.dat
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Last Active\{69EE14A0-C276-11E3-AE24-08002733366F}.dat
 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:
{\tt Data\Microsoft\Media\ Player\CurrentDatabase\_59R.wmdb}
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
```

```
Data\Microsoft\Silverlight\mssl.lck
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc.idx
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\47\15572e2f-21932044.idx
                         C:\Documents and Settings\Admin\Local Settings\Application
 Reads from:
Data\Sun\Java\Deployment\cache\6.0\7\2bbaaf87-5ca9d237
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\7\2bbaaf87-5ca9d237.idx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\lastAccessed
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings \verb|\History\History.IE5\MSHist012014031220140313\index.dat
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings \verb|\History\History.IE5\MSHist012014033120140407 \verb|\index.dat| \\
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\History\History.IE5\MSHist012014041220140413\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Temp\296c0.msp
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\AdobeARM.log
 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
                         C:\Documents and Settings\Admin\Local Settings\Temp\AUCHECK_PARSER.txt
 Reads from:
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Compatibility\ Pack}
for the 2007 Office system (0).log
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_clwireg.txt
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\dd_depcheck_NETFX_EXP_35.txt
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\dd_dotnetfx35error.txt
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_dotnetfx35install.txt
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\dd_NET_Framework20_Setup164F.txt
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\dd_NET_Framework30_Setup16AE.txt
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework35_MSI16E2.txt
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework35_MSI63E0.txt
 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:
                         \label{lem:local_conditions} 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:
                         C:\Documents and Settings\Admin\Local Settings\Temp\gen_py\2.7\dicts.dat
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\gen_py\2.7\__init__.py
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\JAUReg.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\java_install.log
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\java_install_reg.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\jusched.log
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Microsoft\ PowerPoint}
 Reads from:
Viewer (0).log
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20131223_035827352-MSI_vc_red.msi.txt
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20131223_035827352.html
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Reads from:
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_154212618.html
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\pywin32_postinstall.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\setup.log
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\SilverlightO.log
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\SilverlightMSI.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\uxeventlog.txt
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\AntiPhishing\2CEDBFBC-DBA8-43AA-B1FD-CC8E6316E3E2.dat
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\300lo[1].json
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\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
 Reads from:
Files\Content.IE5\CXCXW1MR\93e33485-fea3-4687-a642-2c5dd233522f_12[1].eot
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\ADSAdClient31[1].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\ADSAdClient31[2].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\ADSAdClient31[3].txt
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\CXCXW1MR\ADSAdClient31[4].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\ADSAdClient31[5].txt
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\CXCXW1MR\adServer[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\auth016[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\bimapping[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\broker[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\CA9ATUDW.css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CAMLW29Z.jsx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CATM568T.jsx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
{\tt Files \content.IE5 \cxcxw1MR \cavlzJ9D.jsx}
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\core114[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\core114[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\css[1].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\css[2].css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\css[3].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\DataList[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\e64030e7-ad8c-4be8-a45a-b69a2df3caef_13[1].eot
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\event[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\event[5].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\false[1].htm
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\General[1].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\General[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
```

```
Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\georedirect[4].htm
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\LoginStatus[1].css
 Reads from:
                         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
 Reads from:
Files\Content.IE5\CXCXW1MR\omnibase[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\oneMscomBlade[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\onemscomfooter[2].css
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files \verb|\| Content.IE5 \verb|\| CXCXW1MR \verb|\| ScriptResource[2].axd \\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\ScriptResource[3].axd
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[4].axd
                         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
Files\Content.IE5\CXCXW1MR\true[1].htm
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\true[2].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\views[1]
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\WebResource[1].axd
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\CXCXW1MR\wtid[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\wt_capi[2].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\736e3781-6a19-4119-b717-e61f0d8982c0_12[1].eot
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\ADSAdClient31[1].txt
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\ADSAdClient31[2].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\auth016[1].js
                         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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\broker-config_s1[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\broker-config_s1[2].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\broker-config_s1[3].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\CA39W67Q.jsx
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\CAANG12B.css
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

Files\Content.IE5\ONWV4FIP\ClientBiSettings.Wol[1].js		
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\confirmation[1].aspx		
Reads from: C:\Documents and Settings\Admin\Local Files\Content.IE5\ONWV4FIP\core114[1].js	Settings\Temporary	Internet
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\counter017[1].js		
Reads from: C:\Documents and Settings\Admin\Local Files\Content.IE5\ONWV4FIP\counter017[2].js	Settings\Temporary	Internet
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\css[1].ashx		
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\css[1].css Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\css[2].css		
Reads from: C:\Documents and Settings\Admin\Local Files\Content.IE5\ONWV4FIP\desktop.ini	Settings\Temporary	Internet
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\details[1].htm		
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\details[2].htm Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\event[1].js	seccings (remporary	1110011100
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\event[3].js	Cottings\Tomporary	Intornat
Reads from: C:\Documents and Settings\Admin\Local Files\Content.IE5\ONWV4FIP\event[6].js	Settings (Temporary	mternet
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\General[1].js	C. I.I.	T
Reads from: C:\Documents and Settings\Admin\Local Files\Content.IE5\ONWV4FIP\gl_social[1].svg	Settings\Temporary	Internet
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\Install[1].css		_
Reads from: C:\Documents and Settings\Admin\Local Files\Content.IE5\ONWV4FIP\js[1].ashx	Settings\Temporary	Internet
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\js[2].ashx		
Reads from: C:\Documents and Settings\Admin\Local Files\Content.IE5\ONWV4FIP\js[3].ashx	Settings\Temporary	Internet
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporarv	Internet
Files\Content.IE5\ONWV4FIP\js[4].ashx		
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\Login[1].css Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\modernizr.wol[1].js	seccings (remper arry	1
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\nb-no[2].css Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\omniture_s_code[1].js	Sectings (Temporary	Internet
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\onemscomfooter[2].css	C-++:\ T	T
Reads from: C:\Documents and Settings\Admin\Local Files\Content.IE5\ONWV4FIP\onemscomsearch[2].css	Settings\Temporary	Internet
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\oneMscomSocial[2].css	S	-
Reads from: C:\Documents and Settings\Admin\Local Files\Content.IE5\ONWV4FIP\PasswordRecovery[1].css	Settings\Temporary	Internet
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\ScriptResource[1].axd		
Reads from: C:\Documents and Settings\Admin\Local Files\Content.IE5\ONWV4FIP\ScriptResource[2].axd	Settings\Temporary	Internet
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporarv	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 Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\serverComponent[1].php		
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\siteresource[1].ashx Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\siteresource[1].css	Sectings (Tempor at y	THECHIEC
Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\style[1].cssx Reads from: C:\Documents and Settings\Admin\Local	Settings\Temporary	Internet
Files\Content.IE5\ONWV4FIP\Tracker[1].js	Secretings (Tempor at y	THEFT
Deletes: C:\WINDOWS\Temp\tmp.exe		

Network Events

Connects to:	127.0.0.1:1041	
Connects to:	93.79.34.32:80	
Connects to:	127.0.0.1:1044	
Connects to:	92.115.167.103:80	

Connects to:	127.0.0.1:1047	
Connects to:	37.251.46.31:80	
Connects to:	127.0.0.1:1050	
Connects to:	89.215.5.55:80	
Connects to:	127.0.0.1:1053	
Connects to:	130.204.190.16:80	
Connects to:	127.0.0.1:1056	
Connects to:	176.110.230.73:80	
Sends data to:	127.0.0.1:1041	
Sends data to:	127.0.0.1:1044	
Sends data to:	127.0.0.1:1047	
Sends data to:	127.0.0.1:1050	
Sends data to:	127.0.0.1:1053	
Sends data to:	127.0.0.1:1056	
Receives data from:	127.0.0.1:1042	
Receives data from:	127.0.0.1:1045	
Receives data from:	127.0.0.1:1048	
Receives data from:	127.0.0.1:1051	
Receives data from:	127.0.0.1:1054	
Receives data from:	127.0.0.1:1057	

Windows Registry Events

vviildovva regia	dy Everits
Creates key:	<pre>HKLM\system\currentcontrolset\services\tcpip\parameters</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings</pre>
Creates key:	HKCU\software\microsoft\internet explorer\main
Creates key:	HKLM\software\microsoft\windows\currentversion\run
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\user shell</pre>
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:	HKLM\software\microsoft\windows nt\currentversion\image file execution
•	9673d957fcfe757877037611aa31c9d11179890201e276c5.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
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\winlogon
Opens key:	HKLM\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.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:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>
options\imm32.dll	
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>
options\ntdll.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clusapi.dll	
Opens key:	HKLM\system\currentcontrolset\control\error message instrument\
Opens key:	HKLM\system\currentcontrolset\control\error message instrument
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\gre_initialize</pre>
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\compatibility32</pre>
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\ime compatibility</pre>
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\windows</pre>
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:	HKCU\
Opens key:	<pre>HKCU\software\policies\microsoft\control panel\desktop</pre>
Opens key:	HKCU\control panel\desktop
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll	

options\version.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cmutil.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 HKLM\svstem\setup Opens key: Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters 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 kev: 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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\shlwapi.dll Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\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\ Opens key: HKCR\protocols\name-space handler Opens kev: HKCU\software\classes\protocols\name-space handler Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings HKLM\software\microsoft\windows\currentversion\internet settings Opens key: Opens key: $HKLM \verb|\software\policies\microsoft\windows\currentversion\ | internet$ settings Opens kev: 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\ HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens kev: Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol HKLM\software\microsoft\internet explorer\main\featurecontrol Opens key: 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 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\zonemap\domains\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ $\label{lem:hklmsoftware bolicies microsoft windows \current version \cite{thmsoftware} in the lemma of the$ Opens key: settings\zonemap\ranges\ Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\zonemap\ranges\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_unc_savedfilecheck Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wininet.dll Opens key: HKLM\system\currentcontrolset\control\wmi\security Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key:

Opens key:

```
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
   Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
   Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
   Opens key:
Opens key:
Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
                                          HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:
   Opens key:
                                          HKLM\software\microsoft\rpc
   Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe\rpcthreadpoolthrottle
                                          HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
                                          HKLM\software\microsoft\rpc\securityservice
   Opens kev:
   Opens key:
                                          HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:
                                          HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
   Opens key:
                                          HKLM\system\currentcontrolset\control\nls\locale
                                          HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
   Opens kev:
                                          \label{lem:hklm} \verb+HKLM\+ system \current control \ \ language groups
   Opens key:
   Opens key:
                                          HKCU\software
   Opens key:
                                          HKCU\software\adobe
   Opens key:
                                          HKCU\software\adobe\acrobat reader
                                          HKCU\software\adobe\acrobat reader\9.0
   Opens key:
   Opens kev:
                                          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
                                          \label{lem:hkcu} \mbox{HKCU\software\adobe\acrobat reader\9.0\avconversionfrompdf}
   Opens key:
   Opens key:
                                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \adobe \acrobat reader \end{tabular} $0 \avconversion from pdf \csettings \csett
   Opens key:
                                          HKCU\software\adobe\acrobat reader\9.0\avconversiontopdf
   Opens key:
                                          HKCU\software\adobe\acrobat reader\9.0\avconversiontopdf\csettings
   Opens key:
                                          HKCU\software\adobe\acrobat reader\9.0\avdisplay
   Opens key:
                                          HKCU\software\adobe\acrobat reader\9.0\avgeneral
                                          \label{local_hammon_hammon} \begin{tabular}{ll} HKCU\software\adobe\acrobat reader\9.0\avgeneral\cdockables \end{tabular}
   Opens key:
   Opens key:
                                          HKCU \ software \ a crobat \ reader \ 9.0 \ avgeneral \ ctool bars
                                          HKCU\software\adobe\acrobat
   Opens kev:
reader\9.0\avgeneral\ctoolbars\cadvcommenting
                                          HKCU\software\adobe\acrobat
   Opens kev:
reader\9.0\avgeneral\ctoolbars\cbasiccommenting
   Opens key:
                                          HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars\ccommenting
   Opens key:
                                          HKCU\software\adobe\acrobat reader\9.0\avtracker
   Opens key:
                                          HKCU\software\adobe\acrobat reader\9.0\collab
   Opens key:
                                          HKCU\software\adobe\acrobat reader\9.0\collab\cdocumentcenter
                                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \adobe \acrobat reader \end{tabular} $$ 1.0 \collab \cdocument \center \csettings $$ 1.0 \collab \cdocument \center \csettings $$ 1.0 \collab \cdocument \center \csettings $$ 1.0 \collab \cdocument \csettings $$ 1.0 \collab \cdocument \csettings $$ 1.0 \cdocument \cdocument \csettings $$ 1.0 \cdocument \csett
   Opens key:
                                          HKCU\software\adobe\acrobat reader\9.0\collab\cemaildistribution
   Opens kev:
   Opens key:
                                          HKCU\software\adobe\acrobat
```

 $\label{lem:continuous} Period of the continuous continuous of the continuous continuou$

```
\label{local-continuity} \mbox{HKCU\software\adobe\acrobat reader\9.0\collab\cserversettings}
      Opens key:
      Opens key:
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\formsprefs
                                                                                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \adobe \acrobat reader \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \end{tabular} $$ 1.0 forms prefs \crequired field hl color \crequired field hl \crequired field hl color \crequired field hl color \crequired field hl \crequire
      Opens key:
      Opens key:
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\formsprefs\cruntimebgidlecolor
      Opens key:
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\fullscreen
      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
      Opens key:
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\language
      Opens key:
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\language\current
      Opens key:
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\language\next
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\multimedia
      Opens key:
      Opens key:
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\multimedia\ccolorandborder
      Opens key:
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\optionalcontent
      Opens kev:
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\originals
      Opens key:
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\prefsdialog
      Opens key:
                                                                                                      HKCU\software\adobe\acrobat reader\9.0\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 kev:
      Opens key:
                                                                                                      HKCU\software\adobe\adobe acrobat\9.0
      Opens key:
                                                                                                      HKCU\software\adobe\adobe acrobat\9.0\diskcabs
                                                                                                      HKCU\software\adobe\adobe arm
      Opens key:
      Opens key:
                                                                                                      HKCU\software\adobe\adobe arm\1.0
      Opens key:
                                                                                                      HKCU\software\adobe\adobe arm\1.0\arm
      Opens key:
                                                                                                      HKCU\software\adobe\adobe synchronizer
      Opens key:
                                                                                                      HKCU\software\adobe\adobe synchronizer\9.0
      Opens key:
                                                                                                      HKCU\software\adobe\adobe synchronizer\9.0\acrobat.com
                                                                                                      HKCU\software\adobe\commonfiles
      Opens key:
      Opens key:
                                                                                                      HKCU\software\adobe\commonfiles\usage
      Opens key:
                                                                                                      HKCU\software\adobe\commonfiles\usage\demographic
                                                                                                      HKCU\software\adobe\commonfiles\usage\reader 9
      Opens key:
      Opens key:
                                                                                                      HKCU\software\intel
      Opens key:
                                                                                                      HKCU\software\intel\indeo
      Opens key:
                                                                                                      HKCU\software\intel\indeo\4.1
      Opens key:
                                                                                                      HKCU\software\javasoft
      Opens key:
                                                                                                      HKCU\software\javasoft\java update
      Opens key:
                                                                                                      HKCU\software\javasoft\java update\policy
      Opens key:
                                                                                                      HKCU\software\javasoft\prefs
      Opens kev:
                                                                                                      HKCU\software\macromedia
      Opens key:
                                                                                                      HKCU\software\macromedia\flashplayer
      Opens key:
                                                                                                      {\tt HKCU \ } software \ \\ {\tt macromedia \ } flash player update
      Opens key:
                                                                                                      HKCU\software\microsoft
      Opens key:
                                                                                                      HKCU\software\microsoft\active setup
      Opens key:
                                                                                                      HKCU\software\microsoft\active setup\installed components
      Opens key:
                                                                                                      HKCU\software\microsoft\active setup\installed components\<{12d0ed0d-
0ee0-4f90-8827-78cefb8f4988}
                                                                                                      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}
                                                                                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \active setup \slightly installed components \active setup \end{tabular} $$ (60b49e34-b) $$ (60b49e34-b) $$ (60b49e34-b) $$ (100b49e34-b) $$ (100
      Opens key:
c7cc-11d0-8953-00a0c90347ff}micros
      Opens key:
                                                                                                      HKCU\software\microsoft\active setup\installed components\>{881dd1c5-
3dcf-431b-b061-f3f88e8be88a}
                                                                                                      HKCU \ software \ \verb|microsoft| active setup \ installed components \ \verb|\{2179c5d3-195d3-195d4| active setup \ 
      Opens key:
ebff-11cf-b6fd-00aa00b4e220}
      Opens key:
                                                                                                      HKCU\software\microsoft\active setup\installed components\{22d6f312-
b0f6-11d0-94ab-0080c74c7e95}
                                                                                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \active setup \slightly installed components \cite{Components} \cite{Comp
      Opens key:
2b09-4501-b3f3-f3508c9228ed}
                                                                                                      Opens key:
cc51-11cf-aafa-00aa00b6015c}
                                                                                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \active setup \slightly installed components \end{tabular} $$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba842-$$44bba8
      Opens key:
cc51-11cf-aafa-00aa00b6015b}
      Opens key:
                                                                                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{$microsoft$ active setup$ installed components$ \end{tabular} $$ \{44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44bba848-44b
cc51-11cf-aafa-00aa00b6015c}
      Opens key:
                                                                                                      HKCU\software\microsoft\active setup\installed components\{4b218e3e-
bc98-4770-93d3-2731b9329278}
      Opens key:
                                                                                                      HKCU\software\microsoft\active setup\installed components\{5945c046-
1e7d-11d1-bc44-00c04fd912be}
      Opens key:
                                                                                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \active setup \slightly installed components \end{tabular} \label{lem:hkcu} \end{tabular} $$ Akcount \slight 
394a-11d3-b153-00c04f79faa6}
      Opens key:
                                                                                                      HKCU\software\microsoft\active setup\installed components\{7790769c-
0471-11d2-af11-00c04fa35d02}
      Opens key:
                                                                                                      HKCU\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4340}
      Opens key:
                                                                                                      HKCU\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4383}
      Opens key:
                                                                                                      HKCU\software\microsoft\active setup\installed components\{89b4c1cd-
```

```
b018-4511-b0a1-5476dbf70820}
```

Opens key: HKCU\software\microsoft\activemovie

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

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

00a0c911ce86}
Opens key: HKCU\software\microsoft\activemovie\devenum\{083863f1-70de-11d0-bd40-

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

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

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

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

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

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

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

nt\regbackup\0.map

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

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

Opens key: HKCU\software\microsoft\advanced inf

setup\ie.hkcuzoneinfo\regbackup\0.map

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

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

Opens key: ${\tt HKCU \backslash software \backslash microsoft \backslash advanced\ inf}$

setup\ie40.useragent\regbackup\0.map

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

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

Opens key: HKCU\software\microsoft\advanced inf

setup\iehomepageinfo\regbackup\0.map

Opens key: HKCU\software\microsoft\clock

Opens key: HKCU\software\microsoft\command processor

Opens key: HKCU\software\microsoft\ctf

Opens key: HKCU\software\microsoft\ctf\assemblies
Opens key: HKCU\software\microsoft\ctf\compartment

Opens key: HKCU\software\microsoft\ctf\compartment\{544d6a63-e2e8-4752-bbd1-

000960bca083}

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

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

Opens key: $\label{lem:hkcusoftwaremicrosoft} $$ HKCU \sim \frac{\mbox{\colored}}{\colored} = \frac{\mbox{\colored}}{\colored} $$ HKCU \sim \frac{\mbox{\colored}}{\colored} = \frac{\mbox{\colored}}{\colored}$

00c04fc324a1}\languageprofile

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

00c04fc324a1}\languageprofile\0x00000409

Opens key: HKCU\software\microsoft\direct3d

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

Opens key: HKCU\software\microsoft\eventsystem

Opens key: HKCU\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}

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

00805fc79216}\subscriptions

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

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

Opens key: HKCU\software\microsoft\ftp
Opens key: HKCU\software\microsoft\gdiplus
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: HKCU\software\microsoft\internet explorer\browseremulation
Opens key: HKCU\software\microsoft\internet explorer\caretbrowsing
Opens key: HKCU\software\microsoft\internet explorer\desktop

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

Opens key: HKCU\software\microsoft\internet explorer\desktop\scheme
Opens key: HKCU\software\microsoft\internet explorer\document windows
Opens key: HKCU\software\microsoft\internet explorer\domstorage
Opens key: HKCU\software\microsoft\internet explorer\domstorage\total
Opens key: HKCU\software\microsoft\internet explorer\download

Opens key: HKCU\software\microsoft\internet explorer\extensions
Opens key: HKCU\software\microsoft\internet explorer\extensions\cmdmapping

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

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

```
HKCU\software\microsoft\internet explorer\informationbar
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts
      Opens kev:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\10
      Opens kev:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\11
      Opens key:
                                                                                                 HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus international \setminus scripts \setminus 12
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\13
      Opens key:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\14
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\15
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\16
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\17
      Opens key:
                                                                                                 HKCU \ software \ microsoft \ internet\ explorer \ international \ scripts \ 18
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\19
                                                                                                 \label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| internet explorer expl
      Opens key:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\21
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\22
      Opens key:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\23
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\24
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\25
      Opens key:
                                                                                                 \label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| internet explorer expl
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\27
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\28
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\29
      Opens kev:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\3
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\30
                                                                                                 \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \microsoft \sin explorer \sin explorer \sin explorer) and the local \sin explorer \si explorer \sin explorer \si explorer \sin explorer \sin explorer \si explorer \s
      Opens key:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\35
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\37
                                                                                                 Opens kev:
      Opens key:
                                                                                                 \label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| internet explorer expl
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\4
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\5
      Opens key:
                                                                                                 \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\international\sc ripts\sc } \mbox{\sc of tware\sc of the lember of
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\7
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\8
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\international\scripts\9
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\internetregistry
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\linksbar
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\linksbar\itemcache
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\linksbar\itemcache\0
                                                                                                 \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\linksbar\itemcache\label{lem:hkcu} 1} \mbox{\sc microsoft\sc explorer\linksbar\sc explorer\linksbar\s
      Opens key:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\lowregistry
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\lowregistry\domstorage
                                                                                                 \label{thm:lower} \begin{tabular}{ll} HKCU \software \microsoft \ internet explorer \loweright \ explorer \ loweright \ explorer \ loweright \ explorer 
      Opens key:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\lowregistry\extensions
      Opens key:
                                                                                                 HKCU\software\microsoft\internet
explorer\lowregistry\extensions\cmdmapping
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\main
                                                                                                 HKCU\software\microsoft\internet explorer\main\default feeds
      Opens kev:
                                                                                                \label{lem:hkcu} \begin{tabular}{ll} HKCU software \end{tabular} internet explorer \end{tabular} all the desired feeds \end{tabular} all
      Opens key:
c7e7-48ac-bfba-7b9c1f5b42a7}
      Opens key:
                                                                                                HKCU\software\microsoft\internet explorer\main\default feeds\{8dd206d8-
e6a9-4797-bfe9-b6a7783eb157}
                                                                                                HKCU\software\microsoft\internet
      Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                                                                                               HKCU\software\microsoft\internet
      Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown\settings
      Opens key:
                                                                                                HKCU\software\microsoft\internet explorer\main\windowssearch
                                                                                                 HKCU\software\microsoft\internet explorer\new windows
      Opens kev:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\new windows\allow
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\phishingfilter
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\privacy
      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}
                                                                                                 HKCU\software\microsoft\internet explorer\searchurl
      Opens key:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\security
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\security\antiphishing
                                                                                                 HKCU\software\microsoft\internet
      Opens key:
explorer\security\antiphishing\2cedbfbc-dba8-43aa-b1fd-cc8e6316e3e2
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\security\p3global
                                                                                                 HKCU\software\microsoft\internet explorer\security\p3sites
      Opens key:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\services
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\settings
                                                                                                 HKCU\software\microsoft\internet explorer\sqm
      Opens key:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\suggested sites
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\tabbedbrowsing
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\toolbar
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\toolbar\explorer
                                                                                                 HKCU\software\microsoft\internet explorer\toolbar\shellbrowser
      Opens kev:
      Opens key:
                                                                                                 HKCU\software\microsoft\internet explorer\toolbar\webbrowser
```

```
Opens key:
                                                                         HKCU\software\microsoft\internet explorer\typedurls
     Opens key:
                                                                         HKCU\software\microsoft\internet explorer\urlsearchhooks
     Opens key:
                                                                         HKCU\software\microsoft\internet explorer\user preferences
     Opens key:
                                                                         HKCU\software\microsoft\internet explorer\zoom
     Opens key:
                                                                         HKCU\software\microsoft\iava vm
     Opens key:
                                                                         HKCU\software\microsoft\keyboard
     Opens key:
                                                                         HKCU\software\microsoft\keyboard\native media players
                                                                         HKCU\software\microsoft\keyboard\native media players\wmp
     Opens key:
     Opens key:
                                                                         HKCU\software\microsoft\mediaplayer
     Opens key:
                                                                         HKCU\software\microsoft\mediaplayer\battery
                                                                         HKCU\software\microsoft\mediaplayer\battery\presets
     Opens key:
     Opens key:
                                                                         HKCU\software\microsoft\mediaplayer\battery\presets\brightsphere
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\brightsphere\currentshiftinfo
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\brightsphere\preshiftinfo
     Opens kev:
                                                                         HKCU\software\microsoft\mediaplaver\batterv\presets\circledance
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\circledance\currentshiftinfo
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\circledance\postshiftinfo
     Opens key:
Opens key:
                                                                         HKCU\software\microsoft\mediaplayer\battery\presets\cominatya
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\cominatya\preshiftinfo
     Opens kev:
                                                                         HKCU\software\microsoft\mediaplayer\battery\presets\cottonstar
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\cottonstar\currentshiftinfo
     Opens key:
HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus cotton star \setminus preshift in formula in the property of the pro
     Opens key:
                                                                         HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus dandelionaid
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\dandelionaid\currentshiftinfo
    Opens kev:
HKCU \ software \ `microsoft \ mediaplayer \ battery \ presets \ dandelionaid \ postshift infollowed by the control of the c
     Opens key:
\label{thm:linear} HKCU \ software \ \ icrosoft \ \ mediap layer \ \ battery \ \ presets \ \ dandelionaid \ \ preshift info
     Opens key:
                                                                         \label{lem:hkcu} \mbox{HKCU\software\mbox{$\mbox{$med$} iaplayer\battery\presets\drowningflower}} \mbox{$\mbox{$\mbox{$d$} iaplayer\battery\presets\drowningflower}} \mbox{$\mbox{$\mbox{$d$} iaplayer\battery\presets\drowningflower}} \mbox{$\mbox{$\mbox{$d$} iaplayer\battery\presets\drowningflower}} \mbox{$\mbox{$\mbox{$d$} iaplayer\battery\presets\drowningflower}} \mbox{$\mbox{$\mbox{$d$} iaplayer\battery\presets\drowningflower}} \mbox{$\mbox{$\mbox{$d$} iaplayer\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\battery\b
     Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\drowningflower\currentshiftinfo
     Opens key:
\label{lem:hccu} \begin{tabular}{l} HKCU \software \microsoft \mediaplayer \battery \presets \drowning flower \postshift info
     Opens key:
Opens key:
                                                                         \label{lem:hkcu} \verb+KKCU\software\microsoft\mediaplayer\battery\presets\eletriar nation
    Opens key:
Opens kev:
HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus eletriar nation \setminus postshift info
     Opens key:
HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus eventhorizon
     Opens kev:
     Opens key:
HKCU \ software \ \ icrosoft \ \ mediaplayer \ \ battery \ \ presets \ \ eventhorizon \ \ \ currents hiftinfo
     Opens key:
HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus battery \setminus presets \setminus eventhorizon \setminus postshift info
\label{lem:hkcu} \verb+kkcu\+ software \verb+microsoft\+ mediaplayer \verb+\battery\+ presets\+ eventhorizon\+ preshift info
    Opens key:
                                                                         HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick ascii
                                                                         HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick
     Opens key:
ascii\currentshiftinfo
    Opens key:
                                                                         HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick
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 kev:
                                                                         HKCU\software\microsoft\mediaplayer\battery\presets\gemstone
matrix\currentshiftinfo
     Opens kev:
                                                                         HKCU\software\microsoft\mediaplayer\battery\presets\gemstone
matrix\preshiftinfo
     Opens key:
                                                                         HKCU\software\microsoft\mediaplayer\battery\presets\grooveswirl
     Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \mediaplayer \mediaplay
HKCU\software\microsoft\mediaplayer\battery\presets\grooveswirl\postshiftinfo
    Opens kev:
HKCU\software\microsoft\mediaplayer\battery\presets\grooveswirl\preshiftinfo
     Opens key:
                                                                         HKCU\software\microsoft\mediaplayer\battery\presets\illuminator
     Opens key:
HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ illuminator \ currents \ hiftinfo
```

```
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\illuminator\postshiftinfo
   Opens 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 kev:
HKCU\software\microsoft\mediaplayer\battery\presets\iseethetruth\preshiftinfo
                                                   HKCU\software\microsoft\mediaplayer\battery\presets\kaleidoscope
   Opens key:
   Opens kev:
HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ kale idoscope \ currents hiftinfo
   Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\kaleidoscope\postshiftinfo
   Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\kaleidoscope\preshiftinfo
   Opens key:
                                                  HKCU\software\microsoft\mediaplayer\battery\presets\khemicalnova
   Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\khemicalnova\currentshiftinfo
   Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\khemicalnova\postshiftinfo
   Opens key:
\label{thm:cu} \begin{tabular}{l} HKCU \software \microsoft \mediap layer \battery \presets \khemical nova \preshift in formal layer \mediap layer \cite{All thm: Cut of the layer \mediap layer} \end{tabular} \begin{tabular}{l} HKCU \software \microsoft \mediap layer \mediap \
   Opens key:
                                                  HKCU\software\microsoft\mediaplayer\battery\presets\lotus
   Opens key:
Opens key:
                                                  HKCU\software\microsoft\mediaplayer\battery\presets\lotus\postshiftinfo
   Opens key:
                                                   HKCU\software\microsoft\mediaplayer\battery\presets\lotus\preshiftinfo
   Opens key:
                                                  HKCU\software\microsoft\mediaplayer\battery\presets\nerds are cool
   Opens key:
                                                   HKCU\software\microsoft\mediaplayer\battery\presets\nerds are
cool\currentshiftinfo
                                                  HKCU\software\microsoft\mediaplayer\battery\presets\nerds are
   Opens key:
cool\postshiftinfo
   Opens key:
                                                   HKCU\software\microsoft\mediaplayer\battery\presets\nerds are
cool\preshiftinfo
   Opens key:
                                                   HKCU\software\microsoft\mediaplayer\battery\presets\relativelycalm
   Opens key:
HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ relatively calm \ currents hiftinfo
HKCU\software\microsoft\mediaplayer\battery\presets\relativelycalm\postshiftinfo
   Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\relativelycalm\preshiftinfo
                                                  HKCU\software\microsoft\mediaplayer\battery\presets\sleepyspray
   Opens kev:
   Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\sleepyspray\currentshiftinfo
   Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \mediaplayer \battery \presets \sleepy spray \postshift in formula \end{tabular} \begin{tabular}{ll} HKCU \software \microsoft \mediaplayer \presets \sleepy spray \postshift \noindent \noinde
   Opens key:
                                                   HKCU\software\microsoft\mediaplayer\battery\presets\smoke or water
   Opens key:
                                                   HKCU\software\microsoft\mediaplayer\battery\presets\smoke or
water\currentshiftinfo
                                                   HKCU\software\microsoft\mediaplayer\battery\presets\smoke or
   Opens kev:
water\preshiftinfo
   Opens key:
                                                   HKCU\software\microsoft\mediaplayer\battery\presets\spiderslastmoment
   Opens key:
HKCU \ software \ microsoft \ mediaplayer \ battery \ presets \ spiders last moment \ currents hiftinfo
   Opens key:
\label{lem:hccu} \begin{tabular}{l} HKCU \software \microsoft \mediaplayer \battery \presets \spiders \mbox{last moment \postshift info} \end{tabular}
                                                  HKCU\software\microsoft\mediaplayer\battery\presets\strawberryaid
   Opens key:
   Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\strawberryaid\currentshiftinfo
   Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\strawberryaid\postshiftinfo
   Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\strawberryaid\preshiftinfo
                                                  HKCU\software\microsoft\mediaplayer\battery\presets\the world
   Opens key:
   Opens key:
                                                   HKCU\software\microsoft\mediaplayer\battery\presets\the
world\currentshiftinfo
                                                  \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\mediaplayer\battery\presets\the}} \\
   Opens key:
world\preshiftinfo
   Opens kev:
                                                   HKCU\software\microsoft\mediaplayer\batterv\presets\tornado
   Opens key:
Opens key:
                                                  HKCU\software\microsoft\mediaplayer\batterv\presets\tornado\preshiftinfo
                                                  HKCU\software\microsoft\mediaplayer\battery\presets\what is an egab
   Opens key:
   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\nlayer

Opens key: HKCU\software\microsoft\mediaplayer\player
Opens key: HKCU\software\microsoft\mediaplayer\player\settings

Opens key: HKCU\software\microsoft\mediaplayer\player\setting
Opens key: HKCU\software\microsoft\mediaplayer\player\skins
Opens key: HKCU\software\microsoft\mediaplayer\player\tasks

```
HKCU\software\microsoft\mediaplayer\player\tasks\nowplaying
 Opens key:
 Opens key:
                         HKCU\software\microsoft\mediaplayer\preferences
 Opens key:
                         HKCU\software\microsoft\mediaplayer\preferences\proxysettings
 Opens key:
                         HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http
 Opens kev:
                         HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms
 Opens key:
                         \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc mediaplayer\preferences\proxysettings\rtsp.}} \\
                         HKCU\software\microsoft\mediaplayer\setup
 Opens key:
 Opens key:
                         HKCU\software\microsoft\mediaplayer\setup\createdlinks
                         HKCU\software\microsoft\messengerservice
 Opens key:
 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
                         HKCU\software\microsoft\ms design tools\mdtdbd
 Opens key:
 Opens key:
                         HKCU\software\microsoft\msdaipp
 Opens key:
                         HKCU\software\microsoft\msdaipp\providers
 Opens key:
                         HKCU\software\microsoft\msdaipp\providers\{9fecd570-b9d4-11d1-9c78-
0000f875ac61}
 Opens key:
                         HKCU\software\microsoft\msdaipp\providers\{9fecd571-b9d4-11d1-9c78-
0000f875ac61}
 Opens key:
                         HKCU\software\microsoft\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
                         HKCU\software\microsoft\multimedia\audio compression manager\priority
 Opens key:
v4.00
 Opens key:
                         HKCU\software\microsoft\narrator
 Opens key:
                         HKCU\software\microsoft\netdde
 Opens key:
                         HKCU\software\microsoft\netdde\dde trusted shares
 Opens key:
                         HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a
                         HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a\chat$
 Opens key:
 Opens key:
                         HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a\clpbk$
 Opens key:
                         HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a\hearts$
                         HKCU\software\microsoft\netshow
 Opens key:
 Opens key:
                         HKCU\software\microsoft\netshow\player
 Opens key:
                         HKCU\software\microsoft\netshow\player\remote
                         HKCU\software\microsoft\notepad
 Opens key:
 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
 Opens key:
                         HKCU\software\microsoft\office\11.0\common\drawalerts
                         HKCU\software\microsoft\office\11.0\common\drawalerts\ftp sites
 Opens key:
 Opens key:
                         HKCU\software\microsoft\office\11.0\common\dspadaptermru
 Opens key:
                         HKCU\software\microsoft\office\11.0\common\general
                         Opens key:
 Opens key:
                         Opens key:
                         HKCU\software\microsoft\office\11.0\common\migration\office
 Opens key:
                         HKCU \setminus software \setminus microsoft \setminus office \setminus 11.0 \setminus ommon \setminus migration \setminus word
 Opens key:
                         HKCU\software\microsoft\office\11.0\common\open find
 Opens key:
                         HKCU\software\microsoft\office\11.0\common\open find\microsoft office
word
 Opens key:
                         HKCU\software\microsoft\office\11.0\common\open find\places
 Opens kev:
                         HKCU\software\microsoft\office\11.0\common\research
                         HKCU\software\microsoft\office\11.0\common\research\translation
 Opens key:
 Opens key:
                         HKCU \ software \ `microsoft \ office \ '11.0 \ common \ 'toolbars'
 Opens key:
                         HKCU\software\microsoft\office\11.0\common\toolbars\settings
 Opens key:
                         HKCU\software\microsoft\office\11.0\common\userinfo
 Opens key:
                         HKCU\software\microsoft\office\11.0\word
 Opens key:
                         HKCU\software\microsoft\office\11.0\word\options
                         HKCU\software\microsoft\office\11.0\word\userinfo
 Opens key:
 Opens key:
                         HKCU\software\microsoft\office\11.0\word\wizards
 Opens key:
                         HKCU\software\microsoft\office\11.0\wordview
                         HKCU\software\microsoft\office\11.0\wordview\data
 Opens key:
 Opens key:
                         HKCU\software\microsoft\office\12.0
 Opens key:
                         HKCU\software\microsoft\office\12.0\common
                         HKCU\software\microsoft\office\12.0\common\drawalerts
 Opens key:
 Opens key:
                         HKCU \ software \ icrosoft \ office \ 12.0 \ common \ drawalerts \ ftp \ sites
 Opens key:
                         HKCU\software\microsoft\office\12.0\common\general
                         Opens key:
```

Opens key:

HKCU\software\microsoft\office\12.0\common\languageresources\enabledlanguages Opens key: HKCU\software\microsoft\office\12.0\common\migration Opens key: HKCU\software\microsoft\office\12.0\common\migration\excel Opens key: $HKCU \setminus software \setminus microsoft \setminus office \setminus 12.0 \setminus common \setminus migration \setminus office$ $HKCU\software\microsoft\office\12.0\common\open$ find Opens key:

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

excel viewer

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

Opens key: HKCU\software\microsoft\office\12.0\common\research Opens kev:

HKCU\software\microsoft\office\12.0\common\research\translation

Opens key: HKCU\software\microsoft\office\12.0\excel

```
HKCU\software\microsoft\office\12.0\excel\options
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\office\12.0\excel viewer
                                              HKCU\software\microsoft\office\12.0\excel viewer\viewer options
   Opens kev:
                                              HKCU\software\microsoft\office\12.0\user settings
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\office\12.0\user settings\excel_intl
   Opens key:
                                              HKCU\software\microsoft\office\12.0\user settings\mso_intl
                                              HKCU\software\microsoft\office\12.0\user settings\powerpoint_intl
   Opens key:
                                              HKCU\software\microsoft\office\14.0
   Opens key:
                                              HKCU\software\microsoft\office\14.0\common
   Opens key:
                                              HKCU\software\microsoft\office\14.0\common\drawalerts
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\office\14.0\common\drawalerts\ftp sites
   Opens key:
                                              HKCU\software\microsoft\office\14.0\common\general
   Opens key:
                                              HKCU\software\microsoft\office\14.0\common\languageresources
   Opens key:
HKCU\software\microsoft\office\14.0\common\languageresources\enabledlanguages
                                              HKCU\software\microsoft\office\14.0\common\open find
   Opens key:
                                              HKCU\software\microsoft\office\14.0\common\open find\microsoft
   Opens kev:
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:
                                              HKCU \setminus software \setminus microsoft \setminus office \setminus 14.0 \setminus common \setminus research \setminus translation
                                              HKCU\software\microsoft\office\14.0\powerpoint
   Opens key:
   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
                                              HKCU\software\microsoft\office\common\smart tag
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\office\common\smart tag\actions
   Opens key:
                                              455d-a40b-c95f1f91ff8a}
   Opens key:
                                              4b0c-b7bf-fec0f9401edd}
                                              HKCU\software\microsoft\office\common\smart tag\actions\{64ab6c69-b40e-
   Opens key:
40af-9b7f-f5687b48e2b6}
   Opens key:
                                              HKCU\software\microsoft\office\common\smart tag\actions\{c3754d1a-04d3-
4085-8cfb-97705b57a98f}
   Opens key:
                                              HKCU \setminus software \setminus microsoft \setminus office \setminus common \setminus smart \ tag \setminus actions \setminus \{f114ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-1331-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae61-14ae6
4238-92c9-bbe330af25fd}
                                              HKCU\software\microsoft\office\common\smart tag\recognizers
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\office\common\smart tag\recognizers\{64ab6c69-
b40e-40af-9b7f-f5687b48e2b6}
                                              \label{thm:local_hammon} \begin{tabular}{l} HKCU \software \microsoft \office \common \small tag \recognizers \end{tabular} \begin{tabular}{l} 487ef1 \common \small tag \recognizers \end{tabular} \begin{tabular}{l} 487ef1 \common \small tag \small tag
   Opens key:
51ca-4e6b-8c76-e576aa926888}
   Opens key:
                                              HKCU\software\microsoft\office\common\userinfo
                                              HKCU\software\microsoft\outlook express
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\outlook express\5.0
   Opens key:
                                              HKCU\software\microsoft\outlook express\5.0\shared settings
                                              \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\outlook} express\sc .0\sc ared settings\sc tup} \\
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\plus!
                                              HKCU\software\microsoft\plus!\themes
   Opens kev:
                                              HKCU\software\microsoft\plus!\themes\apply
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\plus!\themes\current
   Opens key:
                                              HKCU\software\microsoft\protected storage system provider
   Opens key:
                                              HKCU\software\microsoft\protected storage system provider\s-1-5-21-
1757981266-507921405-1957994488-1003
   Opens kev:
                                              HKCU\software\microsoft\ras phonebook
                                              HKCU\software\microsoft\regedt32
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\regedt32\settings
   Opens key:
                                              HKCU\software\microsoft\sapi layer
                                              HKCU\software\microsoft\schedule+
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\schedule+\microsoft schedule+
   Opens key:
                                              HKCU\software\microsoft\search assistant
                                              HKCU\software\microsoft\security center
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\shared
   Opens key:
                                              HKCU\software\microsoft\shared tools
                                              HKCU\software\microsoft\shared tools\font mapping
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\shared tools\proofing tools
   Opens key:
                                              HKCU\software\microsoft\shared tools\proofing tools\custom dictionaries
   Opens key:
                                              HKCU\software\microsoft\speech
   Opens key:
                                              HKCU\software\microsoft\speech\applexicons
   Opens key:
                                              HKCU\software\microsoft\speech\audiooutput
                                              {\tt HKCU \backslash software \backslash microsoft \backslash speech \backslash current user lexicon}
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\speech\currentuserlexicon\applexicons
   Opens key:
                                              HKCU\software\microsoft\speech\currentuserlexicon\{c9e37c15-df92-4727-
85d6-72e5eeb6995a}
   Opens key:
                                              85d6-72e5eeb6995a}\files
   Opens key:
                                              HKCU\software\microsoft\speech\phoneconverters
   Opens key:
                                              HKCU\software\microsoft\speech\voices
   Opens key:
                                              HKCU\software\microsoft\samclient
   Opens key:
                                              HKCU\software\microsoft\systemcertificates
   Opens key:
                                              HKCU\software\microsoft\systemcertificates\ca
   Opens kev:
                                              HKCU\software\microsoft\systemcertificates\ca\certificates
   Opens key:
                                              HKCU\software\microsoft\systemcertificates\ca\crls
```

```
HKCU\software\microsoft\systemcertificates\ca\ctls
   Opens key:
   Opens key:
                                                           HKCU\software\microsoft\systemcertificates\disallowed
   Opens key:
                                                           Opens key:
                                                           HKCU\software\microsoft\systemcertificates\disallowed\crls
   Opens kev:
                                                           HKCU\software\microsoft\systemcertificates\disallowed\ctls
   Opens key:
                                                           HKCU\software\microsoft\systemcertificates\my
                                                           HKCU\software\microsoft\systemcertificates\root
   Opens key:
   Opens key:
                                                           HKCU\software\microsoft\systemcertificates\root\certificates
   Opens key:
                                                           HKCU\software\microsoft\systemcertificates\root\crls
   Opens key:
                                                           HKCU\software\microsoft\systemcertificates\root\ctls
   Opens key:
                                                           HKCU\software\microsoft\systemcertificates\root\protectedroots
   Opens key:
                                                           HKCU \ \ software \ \ \ icrosoft \ \ \ system certificates \ \ \ trust
   Opens key:
                                                           HKCU\software\microsoft\systemcertificates\trust\certificates
                                                           HKCU\software\microsoft\systemcertificates\trust\crls
   Opens key:
   Opens key:
                                                           HKCU\software\microsoft\systemcertificates\trust\ctls
   Opens key:
                                                           HKCU\software\microsoft\systemcertificates\trustedpublisher
   Opens key:
                                                           HKCU\software\microsoft\systemcertificates\trustedpublisher\certificates
   Opens key:
                                                           HKCU\software\microsoft\systemcertificates\trustedpublisher\crls
   Opens key:
                                                           \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\system} certificates\trusted publisher\ctls} \\
   Opens key:
                                                           HKCU\software\microsoft\visualstudio
                                                           HKCU \ software \ microsoft \ visual studio \ \ 9.0
   Opens key:
                                                           HKCU\software\microsoft\visualstudio\9.0\downloadmanager
   Opens key:
   Opens key:
                                                           HKCU\software\microsoft\wbem
   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 key:
                                                           HKCU\software\microsoft\windows\currentversion\applets
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\applets\regedit
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\applets\systray
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\applets\tour
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\controls folder
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
                                                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+bitbucket+ \\
   Opens key:
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\cabinetstate
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\cd burning
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\cd
burning\drives
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\clsid
   Opens key:
                                                           HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus 
ad25-11d0-98a8-0800361b1103}
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\clsid\{645ff040-
5081-101b-9f08-00aa002f954e}
                                                           HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus current version \setminus explorer \setminus clsid \setminus 
   Opens key:
42a0-1069-a2ea-08002b30309d}
                                                           HKCU \ software \ microsoft \ windows \ current version \ explorer \ comdlg 32
   Opens key:
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\lastvisitedmru
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\opensavemru
                                                           HKCU\software\microsoft\windows\currentversion\explorer\desktop
   Opens key:
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\cleanupwiz
   Opens kev:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\discardable
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\discardable\postsetup
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts
   Opens key:
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.aif
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.aifc
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.aiff
   Opens kev:
Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.asf
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.asx
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.au
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.avi
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.bmp
   Opens key:
                                                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+.css+ \\
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dib
                                                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\.. doc
   Opens key:
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.docm
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.docx
   Opens key:
                                                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.dot}
   Opens key:
                                                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \file exts \label{lem:hkcu}. dvr-ms \end{tabular}
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.egg-
info
   Opens key:
                                                           HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus file exts \setminus .emf
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.gif
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm
   Opens key:
                                                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.html}
   Opens kev:
                                                           HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ico
   Opens key:
                                                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\.ivf+ \\
```

```
Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ipe
   Opens kev:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.jpeg
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.jpg
   Opens key:
   Opens kev:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.m1v
   Opens key:
                                                          HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus file exts \setminus .m3u
   Opens key:
                                                          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
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mp3
   Opens key:
                                                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\.mpa+ \\
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpe
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpeg
   Opens key:
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpg
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.mpv2
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.msc
   Opens kev:
   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:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.potm
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.potx
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ppsm
   Opens kev:
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ppsx
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.ppt
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.pptm
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.pptx
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.rmi
   Opens kev:
                                                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\.rtf} \\
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.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\file}. tiff
   Opens key:
                                                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\.txt}
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wav
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wax
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wdp
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wm
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wma
   Opens key:
   Opens key:
                                                          HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus file exts \setminus .wmf
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.wmv
                                                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.wmx} \\
   Opens key:
   Opens key:
                                                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\fileexts \verb+\.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 key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xbap
   Opens key:
                                                          \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+explorer\+fileexts\+.xlam
   Opens key:
                                                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \file exts \c. xls \end{tabular}
   Opens kev:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlsb
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlsm
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlsx
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xlt
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.xltm
   Opens key:
                                                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\fileexts\label{lem:hkcu}.xltx} \\
   Opens kev:
                                                          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 key:
HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites
   Opens key:
                                                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\mbox{\tt menuorder\start}} \\
menu
   Opens key:
                                                          HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2
   Opens key:
                                                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\mbox{\tt mountpoints2\cd}} \mbox{\tt currentversion\explorer\mbox{\tt mountpoints2\cd}} \mbox{\tt currentversion\explorer\mbox{\tt mountpoints2\cd}} \mbox{\tt currentversion\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\exp
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\d
   Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints \\ 2 \setminus \{f90255c0-6bc4-11e3-9fc7-12e3-12e4\} \setminus factor \\ 2 \setminus \{f90255c0-6bc4-11e3-9fc7-12e4\} \setminus factor \\ 3 \setminus \{f90255c0-6bc4-11e3-9fc7-12e4\} \setminus factor \\ 4 \setminus \{f9025c0-6bc4-11e3-9fc7-12e4\} \setminus factor \\ 4 \setminus \{f9025c0-6bc4-12e4\} \setminus factor \\ 4 \setminus \{f9025c0-6bc4-12e4\} \setminus factor \\ 4 \setminus \{f9025c0-6bc4-12e4\} \setminus factor \\ 4 \setminus \{f9025c0
806d6172696f}
   Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ \{f90255c2-6bc4-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11e3-9fc7-11
806d6172696f}
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\mycomputer
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mycomputer\namespace
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\newshortcuthandlers
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\recentdocs
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\recentdocs\.zip
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\runmru
```

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

Opens key:

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\recentdocs\.z
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\runmru
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\startpage
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\streammru
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\streammru
HKCU\software\microsoft\windows\currentversion\explorer\streams

```
Opens key:
                                                                                                                                                                    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
                                                                                                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\stuckrects2
           Opens key:
           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:
                                                                                                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\userassist
           Opens key:
HKCU \ software \ microsoft \ windows \ current version \ (5e6ab780-7743-11cf-a12b-microsoft) \ windows \ (2e6ab780-7743-11cf-a12b-microsoft) \ windows \ (2e6ab780-7743-11c
 00aa004ae837}
           Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\userassist\{75048700-ef1f-11d0-9888-
 006097deacf9}
           Opens key:
                                                                                                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\visualeffects
           Opens kev:
Opens key:
 Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\cursorshadow
           Opens kev:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dragfullwindows
          Opens key:
 Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\fontsmoothing
           Opens kev:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listboxsmoothscrolling
          Opens kev:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewalphaselect
           Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewshadow
           Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewwatermark
          Opens kev:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\menuanimation
           Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\selectionfade
           Opens key:
 Opens kev:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\themes
           Opens kev:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\tooltipanimation
           Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\webview
                                                                                                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\webview
           Opens kev:
           Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\webview\barricadedfolders
                                                                                                                                                                   HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo
           Opens kev:
           Opens key:
 \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version} \end{tabular} explorer \software \mbox{$\mathbb{N}$ indows} \end{tabular} and \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows} \end{tabular} explorer \softw
                                                                                                                                                                   HKCU\software\microsoft\windows\currentversion\ext
           Opens kev:
           Opens key:
                                                                                                                                                                    HKCU\software\microsoft\windows\currentversion\ext\settings
                                                                                                                                                                    HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-
           Opens key:
 e8ad-4283-a596-fa578c2ebdc3}
                                                                                                                                                                   HKCU\software\microsoft\windows\currentversion\ext\settings\{4eb89ff4-
           Opens key:
  7f78-4a0f-8b8d-2bf02e94e4b2}
          Opens key:
                                                                                                                                                                   HKCU\software\microsoft\windows\currentversion\ext\settings\{4edcb26c-
  d24c-4e72-af07-b576699ac0de}
                                                                                                                                                                    HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{7390f3d8-microsoft \setminus windows \setminus current version \setminus ext \setminus set in version \setminus ext \setminus set in version \setminus ext 
           Opens key:
 0439-4c05-91e3-cf5cb290c3d0}
           Opens key:
                                                                                                                                                                    HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{754ff233 - 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986 + 1986
  5d4e-11d2-875b-00a0c93c09b3}
                                                                                                                                                                   HKCU\software\microsoft\windows\currentversion\ext\settings\{7584c670-
          Opens key:
  2274-4efb-b00b-d6aaba6d3850}
           Opens key:
                                                                                                                                                                    HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{761497bb-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{761497bb-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{761497bb-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{761497bb-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{761497bb-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{761497bb-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{761497bb-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{761497bb-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{761497bb-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{761497bb-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{761497bb-microsoft \setminus ext \setminus
 d6f0-462c-b6eb-d4daf1d92d43}
           Opens key:
                                                                                                                                                                   HKCU\software\microsoft\windows\currentversion\ext\settings\{9059f30f-
  4eb1-4bd2-9fdc-36f43a218f4a}
                                                                                                                                                                   HKCU\software\microsoft\windows\currentversion\ext\settings\{b1549e58-
          Opens kev:
 3894-11d2-bb7f-00a0c999c4c1}
           Opens key:
                                                                                                                                                                    HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307c3-bdd307
  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 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 ext \setminus ext
  0c80-11d1-8c54-00a02468f316}
                                                                                                                                                                   HKCU\software\microsoft\windows\currentversion\ext\settings\{d27cdb6e-
          Opens key:
  ae6d-11cf-96b8-444553540000}
           Opens key:
                                                                                                                                                                   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 current version \setminus ext \setminus settings \setminus \{e7e6f031-microsoft \setminus windows \setminus ext \setminus set in version \setminus ext \setminus ex
```

```
17ce-4c07-bc86-eabfe594f69c}
                                   HKCU\software\microsoft\windows\currentversion\ext\stats
  Opens kev:
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-
11cf-aaa5-00401c608501}
                                   HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
  Opens kev:
4283-a596-fa578c2ebdc3}
  Opens key:
                                   11cf-8fd0-00aa00686f13}
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\ext\stats\{761497bb-d6f0-
462c-b6eb-d4daf1d92d43}
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\ext\stats\{8856f961-340a-
11d0-a96b-00c04fd705a2}
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\ext\stats\{cfbfae00-17a6-
11d0-99cb-00c04fd64497}
  Opens key:
                                   11cf-96b8-444553540000}
                                   HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
  Opens kev:
435b-bc74-9c25c1c588a9}
  Opens key:
                                   HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus stats \setminus \{dfeaf 541 - f3e1 -
4c24-acac-99c30715084a}
                                   Opens key:
4134-82b7-f2ba38496583}
                                   HKCU\software\microsoft\windows\currentversion\ext\stats\{e7e6f031-17ce-
  Opens kev:
4c07-bc86-eabfe594f69c}
  Opens key:
                                   11d2-bb9e-00c04f795683}
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\group policy
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\group policy\appmgmt
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\group
policy\groupmembership
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\group policy\history
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\group
policy \verb|\history|{a2e30f80-d7de-11d2-bbde-00c04f86ae3b}|
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\group policy objects
                                   HKCU\software\microsoft\windows\currentversion\group policy
  Opens kev:
objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}machine
                                   HKCU\software\microsoft\windows\currentversion\group policy
  Opens kev:
objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}machine\software
                                   HKCU\software\microsoft\windows\currentversion\group policy
  Opens key:
objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}user
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\grpconv
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\grpconv\mapgroups
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet settings\5.0
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\activities
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\activities\blog
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\activities\email
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\activities\map
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\activities\translate
                                   HKCU\software\microsoft\windows\currentversion\internet settings\cache
  Opens key:
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\cache\content
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\cache\cookies
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\cache\history
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\connections
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\1
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\4
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet settings\p3p
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history
```

```
HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\passport
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\passport\damap
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\protocols
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\protocols\mailto
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\selections.} \mbox{\tt lem:hkcu} \mbox{\tt 
  Opens key:
history
  Opens kev:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zonemap
  Opens key:
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\zonemap\domains
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\escdomains
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
  Opens key:
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 key:
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\policies
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\run
                                      HKCU\software\microsoft\windows\currentversion\runonce
  Opens kev:
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\settings
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\settings\zonemap
  Opens key:
HKCU \ software \ microsoft \ windows \ current version \ settings \ zone map \ protocol defaults
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\shell extensions
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\shell extensions\approved
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\shell
extensions\approved\{bdeadf00-c265-11d0-bced-00a0c90ab50f}
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
  Opens key:
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\shell} extensions\cached}
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\syncmgr
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\syncmgr\handlers
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\telephony
  Opens key:
HKCU\software\microsoft\windows\currentversion\telephony\handoffpriorities
  Opens kev:
HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\themes
  Opens key:
\label{lem:hkcu} \mbox{\tt KKCU\software\mbox{\tt microsoft\windows\currentversion\themes\defaultvisualstyleoff}} \\
HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleon
                                      HKCU\software\microsoft\windows\currentversion\themes\lasttheme
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\webcheck
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\webcheck\store.1
  Opens key:
00002cc2cb62}
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\windowsupdate
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\wintrust
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\wintrust\trust providers
                                      HKCU\software\microsoft\windows\currentversion\wintrust\trust
  Opens key:
providers\software publishing
  Opens key:
                                      HKCU\software\microsoft\windows\shell
  Opens key:
                                      HKCU\software\microsoft\windows\shell\bagmru
  Opens key:
                                      HKCU\software\microsoft\windows\shell\bags
  Opens key:
                                      HKCU\software\microsoft\windows\shell\bags\1
                                      HKCU \setminus software \setminus microsoft \setminus windows \setminus shell \setminus bags \setminus 1 \setminus desktop
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\windows\shell\localizedresourcename
  Opens key:
                                      HKCU\software\microsoft\windows\shellnoroam
                                      HKCU\software\microsoft\windows\shellnoroam\bagmru
  Opens key:
  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
  Opens key:
                                      HKCU\software\microsoft\windows\shellnoroam\bagmru\2
```

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus bagmru \setminus 2 \setminus 0$

HKCU\software\microsoft\windows\shellnoroam\bags\1\shell HKCU\software\microsoft\windows\shellnoroam\bags\10

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus bags \setminus 10 \setminus shell$

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

HKCU\software\microsoft\windows\shellnoroam\bags

HKCU\software\microsoft\windows\shellnoroam\bags\1

Opens key: Opens key:

Opens key:

Opens key:

Opens key:

Opens key: Opens key:

```
Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\11\shell
     Opens kev:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\12
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\12\shell
     Opens key:
     Opens kev:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\13
     Opens key:
                                                                               HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus bags \setminus 13 \setminus 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 \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus bags \setminus 16 \setminus 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 kev:
     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\shellnoroam\bags\21
     Opens kev:
     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
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\23\shell
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\24
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\24\shell
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\25
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\25\shell
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\26
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\26\shell
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\27
     Opens key:
     Opens key:
                                                                               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:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\29\shell
                                                                               HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus bags \setminus 3
     Opens key:
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\3\shell
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\30
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\30\shell
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\31
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\31\shell
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\32
     Opens key:
                                                                               HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus bags \setminus 32 \setminus shell
     Opens kev:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\4
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\4\shell
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\5
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\5\shell
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\6
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\6\shell
     Opens kev:
                                                                               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
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\9
     Opens key:
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\bags\9\shell
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\duibags
     Opens key:
                                                                               HKCU\software\microsoft\windows\shellnoroam\duibags\shellfolders
     Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus duibags \setminus shell folders \setminus \{20d04fe0-3aea-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a200-a200-a2
08002b30309d}
\label{twindows} HKCU\software\microsoft\windows\shellnoroam\duibags\shellfolders\{21ec2020-3aea-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2
08002b30309d}
     Opens key:
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}
HKCU \ software \ microsoft \ windows \ shell no roam \ duibags \ shell folders \ \{e88dcce0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7b3-11d1-a9f0-b7
00aa0060fa31}
     Opens key:
HKCU \ software \ microsoft \ windows \ shell no roam \ duibags \ shell folders \ \{f3364ba0-65b9-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9ba-11ce-a9
00aa004ae837}
     Opens kev:
                                                                               HKCU\software\microsoft\windows\shellnoroam\muicache
     Opens key:
                                                                               HKCU\software\microsoft\windows help
     Opens key:
                                                                               HKCU\software\microsoft\windows media
     Opens key:
                                                                               HKCU\software\microsoft\windows media\wmsdk
                                                                               HKCU\software\microsoft\windows media\wmsdk\audiodecode
     Opens kev:
```

HKCU\software\microsoft\windows media\wmsdk\general

HKCU\software\microsoft\windows\shellnoroam\bags\11

Opens key:

Opens key:

```
Opens key:
                         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
 Opens kev:
                         HKCU\software\microsoft\windows nt
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion
                         HKCU\software\microsoft\windows nt\currentversion\devices
 Opens key:
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\extensions
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\network
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\network\event viewer
 Opens kev:
                         HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\network\persistent
connections
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\network\server manager
                         HKCU\software\microsoft\windows nt\currentversion\network\user manager
 Opens key:
 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 key:
                         HKCU\software\microsoft\windows nt\currentversion\time zones
                         HKCU\software\microsoft\windows nt\currentversion\truetype
 Opens kev:
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\windows
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\winlogon
                         HKCU\software\microsoft\windows nt\currentversion\winlogon\gpextensions
 Opens key:
 Opens key:
                         HKCU\software\microsoft\windows
nt\currentversion\winlogon\gpextensions\{a2e30f80-d7de-11d2-bbde-00c04f86ae3b}
 Opens key:
                         HKCU\software\microsoft\windows script
 Opens key:
                         HKCU\software\microsoft\windows script\settings
 Opens key:
                         HKCU\software\netscape
 Opens key:
                         HKCU\software\netscape\netscape navigator
 Opens key:
                         HKCU\software\netscape\netscape navigator\suffixes
 Opens key:
                         HKCU\software\netscape\netscape navigator\user trusted external
applications
 Opens key:
                         HKCU\software\netscape\netscape navigator\viewers
 Opens key:
                         HKCU\software\policies
                         HKCU\software\policies\microsoft
 Opens key:
 Opens key:
                         HKCU\software\policies\microsoft\systemcertificates
 Opens key:
                         HKCU\software\policies\microsoft\systemcertificates\ca
                         HKCU\software\policies\microsoft\systemcertificates\ca\certificates
 Opens key:
 Opens key:
                         HKCU\software\policies\microsoft\systemcertificates\ca\crls
 Opens key:
                         HKCU\software\policies\microsoft\systemcertificates\ca\ctls
 Opens key:
                         HKCU\software\policies\microsoft\systemcertificates\disallowed
 Opens key:
HKCU\software\policies\microsoft\systemcertificates\disallowed\certificates
                         HKCU\software\policies\microsoft\systemcertificates\disallowed\crls
 Opens key:
 Opens key:
                         HKCU\software\policies\microsoft\systemcertificates\disallowed\ctls
 Opens key:
                         HKCU\software\policies\microsoft\systemcertificates\trust
 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
 Opens key:
                         HKCU\software\policies\microsoft\systemcertificates\trust\ctls
 Opens key:
                         HKCU\software\policies\microsoft\systemcertificates\trustedpublisher
 Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\certificates
 Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\crls
 Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\ctls
 Opens key:
                         HKCU\software\classes
 Opens key:
                         HKCU\software\classes\clsid
                         HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-
00805f499d93}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0000-0003-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0000-0003-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0000-0004-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0000-0004-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0013-0000-0005-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0000-0005-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0000-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0000-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-abcdeffedcba}
```

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

abcdeffedcbb}\inprocserver32

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

```
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0002-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0002-
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
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0003-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0003-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0003-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0003-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0004-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0004-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0004-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0004-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0005-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0006-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0006-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0006-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0006-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0007-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0007-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0007-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0001-0007-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0000-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0000-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0000-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0000-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0001-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0001-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0001-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0001-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0002-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0002-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0002-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0002-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0003-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0003-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0003-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0003-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0004-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0004-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0004-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0004-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         \label{local_equation} \begin{tabular}{ll} HKCU \software \classes \clsid \cafeefac-0014-0002-0005-abcdeffedcba \end{tabular}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0005-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0005-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0005-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0006-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0006-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0006-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0006-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0007-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0007-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0007-abcdeffedcbb}
```

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0007-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0008-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0008-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0008-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0008-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0009-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0009-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0009-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0009-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0010-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0010-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0010-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0010-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0011-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0011-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0011-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0011-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0012-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0012-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0012-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0012-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-abcdeffedcba}
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0013-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0014-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0014-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0014-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0014-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0015-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0015-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0015-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0015-
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
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0016-abcdeffedcbb}
                         Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0017-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0017-
 Opens key
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0017-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0017-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0018-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0018-
 Opens kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0018-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0018-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0019-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0019-
 Opens kev
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
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0020-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0021-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0014-0002-0021-
 Opens key:
```

abcdeffedcba}\inprocserver32

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

```
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-
abcdeffedcba}\inprocserver32
 Opens kev:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0000-
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-abcdeffedcbc}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0001-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-abcdeffedcbb}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0002-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0003-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-
 Opens key:
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-abcdeffedcbc}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0004-
 Opens kev:
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-
abcdeffedcba}\inprocserver32
                          \label{local-condition} \begin{tabular}{l} HKCU \software \classes \clsid \cafeefac-0015-0000-0005-abcdeffedcbb} \end{tabular}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-
 Opens kev:
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-abcdeffedcbc}
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0005-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-abcdeffedcba}
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-abcdeffedcbc}
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0006-
 Opens key:
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-
 Opens kev:
abcdeffedcba}\inprocserver32
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \cafeefac-0015-0000-0007-abcdeffedcbb \end{tabular}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-abcdeffedcbc}
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0007-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-
abcdeffedcba}\inprocserver32
 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}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0008-
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-abcdeffedcba}
```

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-
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
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0009-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0010-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0011-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-abcdeffedcbc}
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0012-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0013-
 Opens kev:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0014-abcdeffedcba}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0014-
 Opens key:
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
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-abcdeffedcba}
                         Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-
 Opens key
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0015-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-
 Opens kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0016-
 Opens kev
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
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0017-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-abcdeffedcba}
                         Opens key:
```

abcdeffedcba}\inprocserver32

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0018-
 Opens kev:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0019-
 Opens key:
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
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-abcdeffedcbb}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0020-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-abcdeffedcbc}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0021-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-abcdeffedcba}
                         Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0022-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-abcdeffedcba}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0023-abcdeffedcbc}
 Opens kev:
 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 kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0024-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0025-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-abcdeffedcbb}
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0026-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-abcdeffedcbb}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-
```

```
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0027-
abcdeffedcbc}\inprocserver32
 Opens kev:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-abcdeffedcbc}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0028-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-abcdeffedcbb}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0029-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-abcdeffedcba}
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0030-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-abcdeffedcba}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-abcdeffedcbb}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0031-
abcdeffedcbc}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-
 Opens kev:
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-0032-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0015-0000-ffff-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0015-0000-ffff-
 Opens kev:
abcdeffedcba}\inprocserver32
                         \label{local-equation} \mbox{HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-abcdeffedcba\}}}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-abcdeffedcbb}
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-
 Opens kev:
abcdeffedcbb}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-abcdeffedcbc}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0000-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-abcdeffedcba}
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-
 Opens key:
abcdeffedcba}\inprocserver32
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-
 Opens kev:
abcdeffedcbb}\inprocserver32
                         \label{local-condition} \begin{tabular}{l} HKCU \software \classes \clsid \cafeefac-0016-0000-0001-abcdeffedcbc} \end{tabular}
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0001-
abcdeffedcbc}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-abcdeffedcba}
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-
 Opens kev:
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-abcdeffedcbb}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-
abcdeffedcbb}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-abcdeffedcbc}
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0002-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-abcdeffedcba}
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-
abcdeffedcba}\inprocserver32
 Opens key:
                          HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-abcdeffedcbb}
```

```
Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0003-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0004-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-abcdeffedcba}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-abcdeffedcbc}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0005-
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0006-
 Opens kev:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-abcdeffedcba}
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-
 Opens key:
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0007-
 Opens key:
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-
 Opens kev:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-abcdeffedcbc}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0008-
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-
 Opens key
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-abcdeffedcbb}
                         Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0009-
 Opens key
abcdeffedcbc}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-
 Opens key:
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-abcdeffedcbb}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-
 Opens kev
abcdeffedcbb}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-abcdeffedcbc}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0010-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-abcdeffedcba}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-
 Opens kev
abcdeffedcba}\inprocserver32
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-abcdeffedcbb}
 Opens kev:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-abcdeffedcbc}
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0011-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-abcdeffedcba}
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-
abcdeffedcba}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{cafeefac-0016-0000-0012-abcdeffedcbb}
                         Opens key:
```

abcdeffedcbb}\inprocserver32

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

```
abcdeffedcbc}\inprocserver32
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-abcdeffedcba}
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-
abcdeffedcba}\inprocserver32
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-abcdeffedcbb}
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-abcdeffedcbc}
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-
abcdeffedcbc}\inprocserver32
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-abcdeffedcba}
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-abcdeffedcbb}
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-
abcdeffedcbb}\inprocserver32
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-abcdeffedcbc}
  Opens kev:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-
abcdeffedcbc}\inprocserver32
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcdeffedcba}
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-
abcdeffedcba}\inprocserver32
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcdeffedcbb}
  Opens kev:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcdeffedcbc}
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-
abcdeffedcbc}\inprocserver32
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcdeffedcba}
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-
abcdeffedcba}\inprocserver32
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcdeffedcbb}
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-
  Opens key:
abcdeffedcbb}\inprocserver32
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcdeffedcbc}
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-
abcdeffedcbc}\inprocserver32
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-abcdeffedcba}
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-
abcdeffedcba}\inprocserver32
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-abcdeffedcbb}
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-
  Opens key:
abcdeffedcbb}\inprocserver32
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-abcdeffedcbc}
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-
  Opens kev:
abcdeffedcbc}\inprocserver32
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-abcdeffedcba}
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-
abcdeffedcba}\inprocserver32
  Opens key:
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-abcdeffedcbb}
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-
  Opens kev:
abcdeffedcbb}\inprocserver32
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-abcdeffedcbc}
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-
  Opens key:
abcdeffedcbc}\inprocserver32
  Opens key:
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-abcdeffedcba}
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-
  Opens key:
abcdeffedcba}\inprocserver32
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-abcdeffedcbb}
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-
abcdeffedcbb}\inprocserver32
  Opens key:
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-abcdeffedcbc}
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-
  Opens key:
abcdeffedcbc}\inprocserver32
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-abcdeffedcba}
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-
  Opens kev:
abcdeffedcba}\inprocserver32
                                    \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \cafeefac-0016-0000-0029-abcdeffedcbb \end{tabular}
  Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-
abcdeffedcbb}\inprocserver32
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-abcdeffedcbc}
                                     HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-
  Opens kev:
abcdeffedcbc}\inprocserver32
  Opens key:
                                    HKCU\software\classes\clsid\{cafeefac-0016-0000-ffff-abcdeffedcba}
  Opens key:
                                     HKCU \setminus software \setminus classes \setminus clsid \setminus \{cafee fac-0016-0000-ffff-10000-ffff-10000-ffff-10000-ffff-10000-ffff-10000-ffff-10000-ffff-10000-ffff-10000-ffff-10000-ffff-10000-ffff-10000-ffff-10000-fff-10000-fff-10000-fff-10000-fff-10000-fff-10000-fff-10000-fff-10000-fff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff-10000-ff
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
  Opens key:
                                    HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-abcdeffedcbb}
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-
abcdeffedcbb}\inprocserver32
  Opens key:
                                     HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-abcdeffedcbc}
```

```
Opens key:
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-
abcdeffedcbc}\inprocserver32
 Opens key:
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-abcdeffedcba}
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-
 Opens key:
abcdeffedcba}\inprocserver32
 Opens key:
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-abcdeffedcbb}
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-
 Opens key:
abcdeffedcbb}\inprocserver32
 Opens key:
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-abcdeffedcbc}
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-
 Opens key:
abcdeffedcbc}\inprocserver32
 Opens key:
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}
 Opens key:
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcba}\inprocserver32
 Opens key:
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}
 Opens key:
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprocserver32
 Opens key:
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}
 Opens key:
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbc}\inprocserver32
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-abcdeffedcba}
 Opens key:
 Opens key:
                      HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-
abcdeffedcba}\inprocserver32
 Opens key:
                      HKCU\software\classes\clsid\{e19f9331-3110-11d4-991c-005004d3b3db}
 Opens key:
                      HKCU\software\classes\clsid\{e19f9331-3110-11d4-991c-
005004d3b3db}\inprocserver32
 Opens key:
                      HKCU\software\classes\javaplugin.1020
 Opens key:
                      HKCU\software\classes\javaplugin.1020\clsid
                      HKCU\software\classes\software
 Opens key:
 Opens key:
                      HKCU\software\classes\software\microsoft
 Opens key:
                      HKCU\software\classes\software\microsoft\mediaplayer
                      HKCU\software\classes\software\microsoft\mediaplayer\preferences
 Opens key:
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\run
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
 Opens kev:
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mfc42u.dll
 Opens key:
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\npptools.dll
 Opens key:
                      \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\packet.dll
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens kev:
options\wpcap.dll
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}
 Opens key:
                      08002be10318}\0000
                      HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens kev:
08002be10318}\0000\linkage
 Opens key:
                      HKLM\system\currentcontrolset\services\npf
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001
 Opens key:
                      08002be10318}\0001\linkage
 Opens key:
                      HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\ms
tcp loopback interface
 Opens key:
                      HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002
 Opens key:
                      08002be10318}\0002\linkage
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\linkage
                      Opens key:
08002be10318}\0004
 Opens key:
                      08002be10318}\0004\linkage
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
08002be10318}\0005\linkage
 Opens key:
                      08002be10318}\0006
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\linkage
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007
 Opens key:
                      08002be10318}\0007\linkage
 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
 Opens key:
                        08002be10318}\0010
 Opens key:
                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010\linkage
 Opens key:
                        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 key:
HKLM\software\microsoft\ctf\compatibility\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe
 Opens key:
                        HKLM\software\microsoft\ctf\systemshared\
                        HKCU\keyboard layout\toggle
 Opens kev:
 Opens key:
                        HKLM\software\microsoft\ctf\
 Opens key:
                        HKCU\software\far\plugins\ftp\hosts
 Opens key:
                        HKCU\software\far2\plugins\ftp\hosts
 Opens key:
                        HKCU\software\far\saveddialoghistory\ftphost
 Opens key:
                        HKCU\software\far2\saveddialoghistory\ftphost
 Opens kev:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
 Opens key:
                        HKLM\system\currentcontrolset\control\productoptions
                        HKLM\software\policies\microsoft\windows\system
 Opens key:
 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:
 Opens key:
                        HKCU\software\flashfxp
 Opens key:
                        HKCU\software\flashfxp\3
                        HKCU\software\flashfxp\4
 Opens key:
 Opens key:
                        HKLM\software\flashfxp
 Opens key:
                        HKLM\software\flashfxp\3
                        HKLM\software\flashfxp\4
 Opens key:
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\addressbook
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash
player activex
 Opens kev:
                        HKLM\software\microsoft\windows\currentversion\uninstall\branding
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\connection
manager
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\directanimation
                        HKLM\software\microsoft\windows\currentversion\uninstall\directdrawex
 Opens key:
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\dxm_runtime
 Opens kev:
                        HKLM\software\microsoft\windows\currentversion\uninstall\fontcore
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\icw
 Opens kev:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus idnmitigation apis
                        HKLM \verb|\software\microsoft\windows\currentversion\uninstall\ie 40
 Opens kev:
 Opens key:
                        HKLM \verb|\software\microsoft\windows\currentversion\uninstall\ie4d at a
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\ie5bakex
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\ie7
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\ie8
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\iedata
                        HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-v5
 Opens key:
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\microsoft .net
framework 3.5 sp1
 Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus mobile option pack
                        HKLM\software\microsoft\windows\currentversion\uninstall\mplayer2
 Opens kev:
 Opens key:
                        HKLM\software\microsoft\windows\currentversion\uninstall\netmeeting
 Opens key:
HKLM\software\microsoft\windows\currentversion\uninstall\nlsdownlevelmapping
 Opens key:
                        Opens key:
                        HKLM \ software \ microsoft \ windows \ current version \ uninstall \ pchealth
```

HKLM\software\microsoft\windows\currentversion\uninstall\schedulingagent Opens kev:

HKLM\software\microsoft\windows\currentversion\uninstall\wic Opens key:

HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-Opens key:

3d01-b289-befc77a11a1e}

Opens key: $HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{26a24ae4-039d-1$

4ca4-87b4-2f83217002ff}

Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{350c97b0-3d7c-

4ee8-baa9-00bcb3d54227}

```
Opens key:
                                  4037-7777-5f2748764d10}
  Opens key:
                                  HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-
0409-0000-0000000ff1ce}
  Opens key:
                                  11d3-8cfe-0150048383c9}
  Opens key:
                                  HKLM\software\microsoft\windows\currentversion\uninstall\{95120000-003f-
0409-0000-0000000ff1ce}
  Opens key:
                                  0409-0000-0000000ff1ce}
  Opens kev:
                                  HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-
3813-a88d-b8dccde8f8c7}
  Opens key:
                                  1033-7b44-a93000000001}
  Opens key:
                                  3f2d-899a-6a1d67f2073f}
                                  HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-
  Opens kev:
4027-b136-2b3e1f5ab6e2}
  Opens key:
                                  36ca-84d3-9f4dcf5c5bd9}
  Opens key:
                                  HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-
36ca-84d3-9f4dcf5c5bd9}.kb953595
                                  \label{lem:hkcu} \mbox{HKCU\software\bpftp\bullet proof ftp\main} \\
  Opens kev:
  Opens key:
                                  HKCU\software\bulletproof software\bulletproof ftp client\main
  Opens key:
                                  HKCU\software\bpftp\bullet proof ftp\options
                                  HKCU\software\bulletproof software\bulletproof ftp client\options
  Opens key:
  Opens key:
                                  HKCU\software\bulletproof software\bulletproof ftp client 2010\options
  Opens key:
                                  HKCU\software\bpftp
                                  HKCU\software\turboftp
  Opens key:
  Opens key:
                                  HKCU\software\cryer\websitepublisher
  Opens key:
                                  HKLM\system\currentcontrolset\control\computername
                                  HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:
  Opens key:
                                  HKU\
  Opens key:
                                  HKCU\software\ftpclient\sites
                                  HKCU\software\softx.org\ftpclient\sites
  Opens key:
  Opens key:
                                  HKCU\software\martin prikryl\winscp 2\sessions
  Opens key:
                                  HKCU\software\vandyke\securefx
  Opens key:
                                  HKLM\software\microsoft\windows\currentversion
  Opens key:
                                  HKCU\software\globalscape\cuteftp 6 home\qctoolbar
  Opens key:
                                  HKCU\software\globalscape\cuteftp 6 professional\qctoolbar
                                  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
                                  HKCU\software\globalscape\cuteftp 8 professional\qctoolbar
  Opens key:
  Opens key:
                                  HKCU\software\sota\ffftp\options
  Opens key:
                                  HKCU\software\ftpware\coreftp\sites
                                  \label{lem:hkcu} \verb+KKCU\software\south river technologies\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solvebdrive\solveb
  Opens key:
  Opens key:
                                  HKCU\software\nch software\classicftp\ftpaccounts
  Opens kev:
                                  HKLM\software\nch software\fling\accounts
  Opens key:
                                  HKCU\software\filezilla
  Opens key:
                                  HKCU\software\filezilla\recent servers
                                  HKCU\software\filezilla\site manager
  Opens key:
  Opens key:
                                  HKCU\software\ftp explorer\profiles
  Opens key:
                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ uninstall\+ ultrafxp
                                  HKLM\software
  Opens key:
  Queries value:
                                  HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Oueries value:
                                  HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
                                  HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:
                                  HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
                                  HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
                                  HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\compatibility32[188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5]
                                  HKLM\software\microsoft\windows nt\currentversion\ime
  Oueries value:
compatibility[188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5]
  Queries value:
                                 HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:
                                  HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
                                  {\tt HKLM \backslash software \backslash microsoft \backslash ole[rwlock resource timeout]}
  Queries value:
                                  HKCR\interface[interfacehelperdisableall]
  Oueries value:
  Oueries value:
                                  HKCR\interface[interfacehelperdisableallforole32]
  Queries value:
                                  HKCR\interface[interfacehelperdisabletypelib]
  Queries value:
                                  HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
                                  Queries value:
00000000046}[interfacehelperdisableallforole32]
  Oueries value:
                                 HKCU\control panel\desktop[multiuilanguageid]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Oueries value:
```

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$ 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] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] $\label{lem:hklm} \verb+kklm \system \current control set \services \dnscache \parameters [useedns]$ Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\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] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel] Oueries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[multicastsendlevel] Oueries value: HKLM\system\setup[systemsetupinprogress]

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

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts] Queries value: HKCU\control panel\desktop[smoothscroll] Oueries value: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced \ [enable balloon tips]$ Oueries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe] Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*] Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45ab78-1084642581fb1 Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-0000000000000 Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num] 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] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem] Oueries 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\00000000005[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem] Oueries value: Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath] Queries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000001[displaystring])$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[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: Queries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000001 \ [version]$ Queries value: Queries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace _catalog5 \ catalog_entries \ 000000000002 [library path]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000002[supported name space]$

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]

Queries value:

Queries value:

Oueries value:

Queries value:

Queries value:

```
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus namespace\_catalog \\ \setminus catalog\_entries \setminus 000000000003[library path]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[displaystring]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ name space\_catalog \ name space\_cata
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 000000000003 \ [address family]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5 \setminus catalog\_entries \setminus 000000000003[supported names pace]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus names pace\_catalog \\ \setminus catalog\_entries \setminus 0000000000003 [enabled]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
                                            HKLM\software\microsoft\rpc[maxrpcsize]
   Queries value:
                                             HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
   Queries value:
   Queries value:
                                             HKLM\system\currentcontrolset\services\winsock\parameters[transports]
                                            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
   Oueries value:
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                                            HKLM \ system \ current controls et \ \ control \ nls \ \ language \ groups [5]
   Queries value:
                                             HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:
   Queries value:
                                             HKLM\system\currentcontrolset\control\nls\language groups[2]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\nls\language groups[4]
   Queries value:
                                             HKLM\system\currentcontrolset\control\nls\locale[00000419]
                                             HKCU\software\microsoft\internet explorer\main[]
   Oueries value:
                                             \label{lem:hkcu} \verb+KKCU\software\microsoft\nternet explorer\main[hidecompleted line]
   Oueries value:
                                             HKCU\software\microsoft\internet explorer\main[lineloadedquick]
   Queries value:
                                             HKCU\software\microsoft\internet explorer\main[keycompressedinvalid]
   Queries value:
   Oueries value:
                                             HKCU\software\microsoft\internet explorer\main[dirloadedquick]
                                             HKCU\software\microsoft\internet explorer\main[folderupdatedvalid]
   Queries value:
   Oueries value:
                                             HKLM\software\microsoft\windows\currentversion\run[sonvagent]
   Queries value:
                                             HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
c7d49d7cecdc}[enabledhcp]
   Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[leaseobtainedtime]
   Oueries value:
c7d49d7cecdc}[leaseterminatestime]
   Queries value:
c7d49d7cecdc}[dhcpserver]
                                             Queries value:
08002be10318}\0000[componentid]
   Oueries value:
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage[export]
                                            Queries value:
08002be10318}\0001[componentid]
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Queries value:
08002be10318}\0001\linkage[export]
   Queries value:
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]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
   Oueries 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-abe3-4636-4303-abe3-4636-4303-abe3-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4
c7d49d7cecdc}[usezerobroadcast1
   Oueries 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-
c7d49d7cecdc}[dhcpsubnetmask]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002[componentid]
   Oueries value:
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002\linkage[export]
   Queries value:
                                             08002be10318}\0003[componentid]
   Queries value:
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\linkage[export]
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Oueries value:
08002be10318}\0004[componentid]
                                            Queries value:
08002be10318}\0004\linkage[export]
   Queries value:
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[componentid]
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Oueries value:
08002be10318}\0005\linkage[export]
                                             Queries value:
08002be10318}\0006[componentid]
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Queries value:
08002be10318}\0006\linkage[export]
   Oueries value:
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[componentid]
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Oueries value:
08002be10318}\0007\linkage[export]
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Queries value:
08002be10318}\0008[componentid]
   Oueries value:
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\linkage[export]
  Oueries value:
                                             HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009[componentid]
                                             Queries value:
08002be10318}\0009\linkage[export]
   Queries value:
                                            08002be10318}\0010[componentid]
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Oueries value:
08002be10318}\0010\linkage[export]
                                             Oueries value:
08002be10318}\0011[componentid]
   Queries value:
                                            08002be10318}\0011\linkage[export]
                                            HKLM\software\microsoft\ctf\svstemshared[cuas]
   Oueries value:
   Queries value:
                                             HKCU\keyboard layout\toggle[language hotkey]
                                             HKCU\keyboard layout\toggle[hotkey]
   Oueries value:
                                             HKCU\keyboard layout\toggle[layout hotkey]
   Oueries value:
   Queries 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:
   Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
                                             HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\winlogon[rsopdebuglevel]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
                                             \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and the current version \
1757981266-507921405-1957994488-1003[profileimagepath]
   Queries value:
                                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}
folders[appdata]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\uninstall\addressbook[uninstallstring]
                                             HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash
   Oueries value:
player activex[uninstallstring]
   Queries value:
                                            HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash
player activex[displayname]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\uninstall\branding[uninstallstring]
   Oueries value:
                                             HKLM \verb|\software\m| icrosoft \verb|\windows\currentversion\uninstall\connection| \\
manager[uninstallstring]
   Oueries value:
Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ uninstall \ direct drawex \ [uninstalls tring]
```

Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\dxm_runtime[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\fontcore[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\icw[uninstallstring] Oueries value: $HKLM \ software \ microsoft \ windows \ current version \ uninstall \ idnmitigation apis [uninstall string]$ Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\ie40[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\ie4data[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\ie5bakex[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\ie7[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\ie8[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\ie8[displayname] Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\iedata[uninstallstring] HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-Oueries value: v5[uninstallstring] HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-Queries value: v5[displayname] Queries value: framework 3.5 sp1[uninstallstring] HKLM\software\microsoft\windows\currentversion\uninstall\microsoft .net Oueries value: framework 3.5 sp1[displayname] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\mobileoptionpack[uninstallstring] HKLM\software\microsoft\windows\currentversion\uninstall\mplayer2[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\netmeeting[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\nlsdownlevelmapping[uninstallstring] HKLM\software\microsoft\windows\currentversion\uninstall\outlookexpress[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\pchealth[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\pchealth[displayname] HKLM\software\microsoft\windows\currentversion\uninstall\schedulingagent[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\wic[uninstallstring] HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-Oueries value: 3d01-b289-befc77a11a1e}[uninstallstring] Oueries value: 3d01-b289-befc77a11a1e}[displayname] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{26a24ae4-039d-1$ 4ca4-87b4-2f83217002ff}[uninstallstring] HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-Oueries value: 4ca4-87b4-2f83217002ff}[displayname] Oueries value: 4ee8-baa9-00bcb3d54227}[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\{4a03706f-666a-4037-7777-5f2748764d10}[uninstallstring] HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-Queries value: 0409-0000-0000000ff1ce}[uninstallstring] Queries value: 0409-0000-0000000ff1ce}[displayname] Oueries value: 11d3-8cfe-0150048383c9}[uninstallstring] HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-Queries value: 11d3-8cfe-0150048383c9}[displayname] Queries value: 0409-0000-0000000ff1ce}[uninstallstring] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{95120000-003f-00000\} \ description \ desc$ 0409-0000-0000000ff1ce}[displayname] HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-Oueries value: 0409-0000-0000000ff1ce}[uninstallstring] Queries value: 0409-0000-0000000ff1ce}[displayname] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{a3051cd0-2f64-4d64, a3051cd0-2f64-4d64, a3051cd0-2f64, a3051cd0-2f64$ 3813-a88d-b8dccde8f8c7}[uninstallstring] Oueries value: HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-3813-a88d-b8dccde8f8c7}[displayname] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{ac76ba86-7ad7-4ac76-4ac$

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus \{ac76ba86-7ad7-ba86-7ad7$

1033-7b44-a9300000001}[uninstallstring]

Queries value:

1033-7b44-a9300000001}[displayname]

HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-Oueries value:

3f2d-899a-6a1d67f2073f}[uninstallstring]

Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-

3f2d-899a-6a1d67f2073f}[displayname]

Queries value: $HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{c3cc4df5-39a5-40f6-39a5-40f6-39a6$

4027-b136-2b3e1f5ab6e2}[uninstallstring]

HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-Oueries value:

4027-b136-2b3e1f5ab6e2}[displayname]

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

36ca-84d3-9f4dcf5c5bd9}[uninstallstring]

Queries value: 36ca-84d3-9f4dcf5c5bd9}[displayname]

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

folders[common appdata]

Queries value:

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

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

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

HKCU\software\microsoft\internet explorer\main[hidecompletedline] Sets/Creates value: Sets/Creates value: HKCU\software\microsoft\internet explorer\main[lineloadedquick] Sets/Creates value: HKCU\software\microsoft\internet explorer\main[keycompressedinvalid] Sets/Creates value: HKCU\software\microsoft\internet explorer\main[dirloadedquick] Sets/Creates value: HKCU\software\microsoft\internet explorer\main[folderupdatedvalid]

HKLM\software\microsoft\windows\currentversion\run[sonyagent] Sets/Creates value:

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

Value changes: $\label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+explorer\+shell$

folders[appdata]

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

folders[local appdata]

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

folders[common appdata]