

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

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

Task ID:	840
Risk Level:	10
Date Processed:	2016-05-18 10:44:56 (UTC)
Processing Time:	62.4 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\752d6fe81122349daf998a56f48e0b38.exe"
Sample ID:	3333
Type:	basic
Owner:	admin
Label:	752d6fe81122349daf998a56f48e0b38
Date Added:	2016-05-18 10:30:52 (UTC)
File Type:	PE32:win32:gui
File Size:	827904 bytes
MD5:	752d6fe81122349daf998a56f48e0b38
SHA256:	e36aa66b3e7928b47f8c4beb0ab46a2e886f9f87ca6de7cf7fd05d8f5457b020
Description:	None

Pattern Matching Results

6	Modifies registry autorun entries
6	Writes to system32 folder
10	Creates malicious events: Kelihos trojan 2 [Spam]
3	Connects to local host
5	Adds autostart object
5	PE: Contains compressed section
5	Creates file in drivers folder

Static Events

Anomaly:	PE: No DOS stub
----------	-----------------

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\752d6fe81122349daf998a56f48e0b38.exe
["c:\windows\temp\752d6fe81122349daf998a56f48e0b38.exe"]	
Loads service:	NPF [system32\drivers\NPF.sys]

Named Object Events

Creates mutex:	\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

Creates:	C:\WINDOWS\Temp\tmp.exe
Creates:	C:\WINDOWS\system32\Packet.dll
Creates:	C:\WINDOWS\system32\wpcap.dll
Creates:	C:\WINDOWS\system32\drivers\npf.sys
Opens:	C:\WINDOWS\Prefetch\752D6FE81122349DAF998A56F48E0-1635C0C2.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\comcat.dll
Opens:	C:\WINDOWS\system32\wmddmcs.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens:	C:\WINDOWS\system32\urlmon.dll.123.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
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\WININET.dll.123.Manifest
Opens:	C:\WINDOWS\system32\WININET.dll.123.Config
Opens:	C:\WINDOWS\Temp\752d6fe81122349daf998a56f48e0b38.exe
Opens:	C:\WINDOWS\system32\dnsapi.dll

Opens: C:\WINDOWS\system32\ws2_32.dll
 Opens: C:\WINDOWS\system32\ws2help.dll
 Opens: C:\WINDOWS\system32\iphlpapi.dll
 Opens: C:\WINDOWS\system32\mswsock.dll
 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\system32\comctl32.dll
 Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens: C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens: C:\WINDOWS\system32\hnetcfg.dll
 Opens: C:\WINDOWS\system32\wshtcpip.dll
 Opens: C:\WINDOWS\Temp
 Opens: C:\WINDOWS\Temp\tmp.exe
 Opens: C:\WINDOWS\Temp\8687eaa8-0e77-4e19-ad50-c3c35644151f
 Opens: C:\dev\urandom
 Opens: C:\
 Opens: C:\WINDOWS\system32
 Opens: C:\AUTOEXEC.BAT
 Opens: C:\WINDOWS\system32\drivers
 Opens: C:\WINDOWS\system32\wpcap.dll
 Opens: C:\boot.ini
 Opens: C:\CONFIG.SYS
 Opens: C:\Documents and Settings
 Opens: C:\Documents and Settings\Admin\Application Data
 Opens: C:\Documents and Settings\Admin\Application Data\Adobe
 Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat
 Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Acrobat\9.0\AdobeCMapFnt09.lst
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Acrobat\9.0\AdobeSysFnt09.lst
 Opens: C:\WINDOWS\system32\wpcap.dll.2.Manifest
 Opens: C:\WINDOWS\system32\wpcap.dll.2.Config
 Opens: C:\WINDOWS\system32\Packet.dll
 Opens: C:\WINDOWS\system32\packet.dll.2.Manifest
 Opens: C:\WINDOWS\system32\packet.dll.2.Config
 Opens: C:\WINDOWS\system32\npptools.dll
 Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0\Forms
 Opens: C:\WINDOWS\system32\mf42u.dll
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Acrobat\9.0\JavaScripts
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Acrobat\9.0\JavaScripts\glob.js
 Opens: C:\WINDOWS\system32\drivers\npf.sys
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Acrobat\9.0\JavaScripts\glob.settings.js
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Acrobat\9.0\SharedDataEvents
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Acrobat\9.0\UserCache.bin
 Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Flash Player
 Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Flash
 Player\AssetCache
 Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Flash
 Player\AssetCache\7PLTA3CP
 Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Linguistics
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Linguistics\Dictionaries
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\all
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\brt
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\can
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\eng
 Opens: C:\Documents and Settings\Admin\Application Data\Adobe\LogTransport2
 Opens: C:\Documents and Settings\Admin\Application
 Data\Adobe\LogTransport2\Logs
 Opens: C:\Documents and Settings\Admin\Application Data\desktop.ini
 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
 Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player
 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
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
Opens: C:\WINDOWS\system32\npp\ndisnpp.dll
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\npp
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\AddIns
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Credentials
Opens: C:\Documents and Settings\Admin\Application
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
Opens: C:\Documents and Settings\Admin\Application
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\2BF68F471409229550497DD56F57004
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\3130B1871A126520A8C47861EFE3ED4D
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\60E31627FDA0A46932B0E5948949F2A5
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\62B5AF9BE9ADC1085C3C56EC07A82BF6
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D49D759AD
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7396C420A8E1BC1DA97F1AF0D10BAD21
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE8E7EB5F575EC9
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\8DFDF057024880D7A081AFBF6D26B92F
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\A44F4E7CB3133FF765C39A53AD8FCFDD
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\F482C95F83F1B59228F1B1E720F2EDF1
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\0797C381B2F87EB5A1D5573BD15BA4F4
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\135BD6A358680A7BF1CCEC7C0172393D
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\2BF68F471409229550497DD56F57004
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\3130B1871A126520A8C47861EFE3ED4D
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\60E31627FDA0A46932B0E5948949F2A5
Opens: C:\WINDOWS\win.ini
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\62B5AF9BE9ADC1085C3C56EC07A82BF6
Opens: C:\Users\
Opens: C:\Documents and Settings\Admin\Application Data\AceBIT\
Opens: C:\Documents and Settings\All Users\Application Data\AceBIT\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\AceBIT\
Opens: C:\WINDOWS\system32\pstorec.dll
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD
Opens: C:\WINDOWS\system32\atl.dll
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
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
1-5-21-1757981266-507921405-1957994488-1003\6b29ae44e85efac3c72ff4d1865d73f1_fa860dc5-a965-4200-
a9d4-fb930ff1911b
Opens: 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
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
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
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\desktop.ini
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\Show Desktop.scf
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Media Player
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\MMC
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Office
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\Office\Excel12.pip
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Office\Recent
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\Office\Recent\Desktop.ini
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Protect
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\Protect\CREDHIST
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\3ea8a527-1704-4983-8596-ab49c663cca3
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\4f5d6884-c60c-4cd3-906b-3d677949fac1
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\fe1a937a-0ac9-4cf1-978d-5d0742ed2858
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\Preferred
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Speech
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Speech\Files
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons\SP_6A65DB879F95470886BD7EFE4977B10E.dat
Opens: C:\Documents and Settings\Admin\Application
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
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CRLs
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CTLs
Opens: C:\Documents and Settings\Admin\Application Data\Google\Chrome\
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Templates
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Chrome\
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Windows
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\Windows\Themes
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\Windows\Themes\Custom.theme
Opens: C:\Documents and Settings\All Users\Application Data\Google\Chrome\
Opens: C:\Documents and Settings\Admin\Application Data\Chromium\
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Chromium\
Opens: C:\Documents and Settings\All Users\Application Data\Chromium\
Opens: C:\Documents and Settings\Admin\Application Data\Oracle
Opens: C:\Documents and Settings\Admin\Application Data\ChromePlus\
Opens: C:\Documents and Settings\Admin\Application Data\Oracle\Java
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\ChromePlus\

Opens: C:\Documents and Settings\All Users\Application Data\ChromePlus\
Opens: C:\Documents and Settings\Admin\Application Data\Bromium\
Opens: C:\Documents and Settings\Admin\Application Data\Oracle\Java\Uninstall
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Bromium\
Opens: C:\Documents and Settings\Admin\Application Data\Sun
Opens: C:\Documents and Settings\All Users\Application Data\Bromium\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java
Opens: C:\Documents and Settings\Admin\Application Data\Nichrome\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\AU
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Nichrome\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment
Opens: C:\Documents and Settings\All Users\Application Data\Nichrome\
Opens: C:\Documents and Settings\Admin\Application Data\Comodo\
Opens: C:\Documents and Settings\Admin\Application
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\Local Settings\Application Data\Comodo\
Opens: C:\Documents and Settings\All Users\Application Data\Comodo\
Opens: C:\Documents and Settings\Admin\Application Data\RockMelt\
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\RockMelt\
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\0
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\1
Opens: C:\Documents and Settings\All Users\Application Data\RockMelt\
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\10
Opens: C:\Documents and Settings\Admin\Application Data\MapleStudio\ChromePlus\
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\MapleStudio\ChromePlus\
Opens: C:\Documents and Settings\All Users\Application
Data\MapleStudio\ChromePlus\
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\11
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\12
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\12\eeef218c-550e9171
Opens: C:\Documents and Settings\Admin\Application Data\browser.yandex\
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\browser.yandex\
Opens: C:\Documents and Settings\All Users\Application Data\browser.yandex\
Opens: C:\Documents and Settings\Admin\Desktop
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\12\eeef218c-550e9171.idx
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\13
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\14
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\15
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\16
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c.idx
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-6.0.lap
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\18
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1.idx
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-6.0.lap
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\2
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\20
Opens: C:\Documents and Settings\Admin\Application
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

[illegible]

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

Data\Microsoft\Internet Explorer\Custom Settings
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Custom Settings\Custom0
Opens: C:\Documents and Settings\Admin\Cookies
Opens: C:\Documents and Settings\Admin\Cookies\admin@c1.microsoft[2].txt
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\0W0RJP5C
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\LQLIM8KB
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery
Opens: C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Active
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery>Last Active
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\Office
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Office\12.0
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Office\14.0
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Silverlight
Opens: C:\Documents and Settings\Admin\Cookies\admin@rto.microsoft[1].txt
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0
Opens: C:\Documents and Settings\Admin\Cookies\admin@search.microsoft[1].txt
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\0
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\1
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\10
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\11
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\12
Opens: C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\13
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\14
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\15
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\16
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\17
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\18
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\19
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\2
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\20
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\21
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\22

[illegible]

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

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

Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK\www.microsoft[1].xml
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\index.dat
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\frameiconcache.dat
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
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\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\Media Player\CurrentDatabase_59R.wmdb
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Silverlight\msssl.lck
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat.LOG
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc.idx
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\47\15572e2f-21932044
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\47\15572e2f-21932044.idx
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\7\2bbaaf87-5ca9d237
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\7\2bbaaf87-5ca9d237.idx
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\lastAccessed
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
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\desktop.ini
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014031220140313
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014031220140313\index.dat
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407\index.dat
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413\index.dat
Opens: C:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\296c0.msp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\AdobeARM.log
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\AdobeARM_NotLocked.log
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\ASPNETSetup_00000.log
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\ASPNETSetup_00001.log
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\AUCHECK_PARSER.txt
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Compatibility Pack
for the 2007 Office system (0).log
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_clwireg.txt
Opens: C:\Documents and Settings\Admin\Local
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
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework20_Setup164F.txt
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework30_Setup16AE.txt
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework35_MSI16E2.txt
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework35_MSI63E0.txt
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_RGB9RAST_x86.msi601E.txt
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA2A49.txt
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA3565.txt
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA35A0.txt
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_XPS.txt
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\gen_py
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
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\JAUReg.log
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
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft PowerPoint
Viewer (0).log
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_10.0.30319
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20131223_035827352-MSI_vc_red.msi.txt
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
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
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
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
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_154212618.html
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\pywin32_postinstall.log
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\setup.log
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Silverlight0.log
Opens: 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: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\AntiPhishing
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\AntiPhishing\2CEDBFC-DBA8-43AA-B1FD-CC8E6316E3E2.dat
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\300lo[1].json
Opens: 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\88666ccc6-d578-45c8-baf0-89d3837f41c3_89[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\93e33485-fea3-4687-a642-2c5dd233522f_12[1].eot
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[1].txt
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[2].txt
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[3].txt
Opens: 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
Opens: 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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\64030e7-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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\General[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\General[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\georedirect[1].htm
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\georedirect[2].htm
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\georedirect[3].htm
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\georedirect[4].htm
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\install[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\js[2].ashx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR>LoginStatus[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\Nebula[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\omnibase[2].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomBlade[2].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\onemscomfooter[2].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[2].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[3].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\request[1].php
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[1].axd
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[2].axd
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[3].axd
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR>true[2].htm
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\views[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\WebResource[1].axd
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP
Opens: 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\ADSAIClient31[1].txt
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\ADSAIClient31[2].txt
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\auth016[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\broker-config_s1[3].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\CA39W67Q.jsx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\CAANG12B.css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\CAU35S9Y.jsx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\ChangePassword[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\ClickToInstall[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\ClientBiSettings.Wol[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\confirmation[1].aspx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\core114[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\counter017[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\counter017[2].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\css[1].ashx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\css[1].css
Opens: 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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\details[1].htm
Opens: 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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\event[3].js
Opens: 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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\gl_social[1].svg
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\Install[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

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

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

Files\Content.IE5\UH4D6D6X\auth016[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\background_gradient[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bimapping[2].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[2].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[3].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[4].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[5].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker[2].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA01EF5H.jsx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA7GG9IO.css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA8VUH6F.css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CAI7MNGV.css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CallingControl[1].aspx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\confirmation[1].aspx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\confirmation[1].htm
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\Cookies[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\core114[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\counter017[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CreateUserWizard[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\css[1].ashx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\css[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\css[2].ashx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\desktop.ini
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\details-social[2].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\enable[2].htm
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\event[3].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\event[5].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\GridView[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\info_48[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\InstallPageReskin[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\Install[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\internet-explorer-8-details[1].htm
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\js[1].ashx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\js[2].ashx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\js[3].ashx
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\Marquee[1].css
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\inbox[1].js
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\MicrosoftAjax[1].js

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

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

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

Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Entertainment\desktop.ini
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\notepad.lnk
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Program Compatibility Wizard.lnk
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Synchronize.lnk
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Tour Windows XP.lnk
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Windows Explorer.lnk
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Remote Assistance.lnk
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Startup
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\desktop.ini
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Windows Media Player.lnk
Opens: C:\Documents and Settings\Administrator\Templates
Opens: C:\Documents and Settings\Administrator\Templates\amipro.sam
Opens: C:\Documents and Settings\Administrator\Templates\lotus.wk4
Opens: C:\Documents and Settings\Administrator\Templates\presenta.shw
Opens: C:\Documents and Settings\Administrator\Templates\quattro.wb2
Opens: C:\Documents and Settings\Administrator\Templates\wordpfct.wpd
Opens: C:\Documents and Settings\Administrator\Templates\wordpfct.wpg
Opens: C:\Documents and Settings\All Users
Opens: C:\Documents and Settings\All Users\Application Data\Adobe\Acrobat\9.0\Replicate\Security\directories.acrodata
Opens: C:\Documents and Settings\All Users\Application Data\Adobe\Reader\9.4\ARM\AdbeRdrUpd951_all_incr.msp
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:\WINDOWS\Temp\752d6fe81122349daf998a56f48e0b38.exe
Reads from: C:\AUTOEXEC.BAT
Reads from: C:\boot.ini
Reads from: C:\CONFIG.SYS
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
Reads from: C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0\JavaScripts\glob.settings.js
Reads from: C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0\SharedDataEvents
Reads from: C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0\UserCache.bin
Reads from: C:\Documents and Settings\Admin\Application Data\desktop.ini
Reads from: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\0797C381B2F87EB5A1D5573BD15BA4F4
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\135BD6A358680A7BF1CCEC7C0172393D
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\3130B1871A126520A8C47861EFE3ED4D
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\60E31627FDA0A46932B0E5948949F2A5
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\62B5AF9BE9ADC1085C3C56EC07A82BF6
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D49D759AD
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\7396C420A8E1BC1DA97F1AF0D10BAD21
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE87EB5F575EC9
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\8DFDF057024880D7A081AFBF6D26B92F
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\A44F4E7CB3133FF765C39A53AD8FCFDD
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\CryptnetUrlCache\Content\F482C95F83F1B59228F1B1E720F2EDF1
Reads from: C:\Documents and Settings\Admin\Application

Data\Microsoft\CryptnetUrlCache\MetaData\0797C381B2F87EB5A1D5573BD15BA4F4
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\135BD6A358680A7BF1CCEC7C0172393D
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497DD56F57004
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\3130B1871A126520A8C47861EFE3ED4D
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\60E31627FDA0A46932B0E5948949F2A5
Reads from: C:\WINDOWS\win.ini
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\62B5AF9BE9ADC1085C3C56EC07A82BF6
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7396C420A8E1BC1DA97F1AF0D10BAD21
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7B2238AACEDC3F1FFE8E7EB5F575EC9
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\8DFDF057024880D7A081AFBF6D26B92F
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\A44F4E7CB3133FF765C39A53AD8FCFDD
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\F482C95F83F1B59228F1B1E720F2EDF1
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
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
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
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\Show Desktop.scf
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\Office\Excel12.pip
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\Office\Recent\Desktop.ini
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\Protect\CREDHIST
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\3ea8a527-1704-4983-8596-ab49c663cca3
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\4f5d6884-c60c-4cd3-906b-3d677949fac1
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\fe1a937a-0ac9-4cf1-978d-5d0742ed2858
Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\Preferred
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons\SP_6A65DB879F95470886BD7EFE4977B10E.dat
Reads from: C:\Documents and Settings\Admin\Application
Data\Microsoft\Windows\Themes\Custom.theme
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\12\eeef218c-550e9171
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\12\eeef218c-550e9171.idx
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c.idx
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-6.0.lap
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1.idx
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-6.0.lap
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d.idx
Reads from: C:\Documents and Settings\Admin\Application

Data\Sun\Java\Deployment\cache\6.0\lastAccessed
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\deployment.properties
Reads from: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\security\trusted.certs
Reads from: C:\Documents and Settings\Admin\Cookies\admin@c1.microsoft[2].txt
Reads from: C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt
Reads from: C:\Documents and Settings\Admin\Cookies\admin@rto.microsoft[1].txt
Reads from: C:\Documents and Settings\Admin\Cookies\admin@search.microsoft[1].txt
Reads from: C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt
Reads from: 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
Reads from: C:\Documents and Settings\Admin\Favorites\Links\Suggested Sites.url
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
Reads from: C:\Documents and Settings\Admin\Favorites\Radio Station Guide.url
Reads from: C:\Documents and Settings\Admin\IECompatCache\index.dat
Reads from: C:\Documents and Settings\Admin\IETldCache\index.dat
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache\AcroFnt09.lst
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Updater\updater.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Color\ACECache10.lst
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Updater6\aum.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Updater6\aumLib.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\GDIPFONTCACHEV1.DAT
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\IconCache.db
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\FeedsStore.feedsdb-ms
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Suggested Sites~.feed-ms
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-
ms
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
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\FBANKAIW\fwlink[1]
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\G4DZ1I7H\desktop.ini
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\G4DZ1I7H\fwlink[1]
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\index.dat
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY1QNV\desktop.ini
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\J3XY1QNV\fwlink[1]
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\TLMHA51J\desktop.ini
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\TLMHA51J\ieonline.microsoft[1]
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\brndlog.bak
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\brndlog.txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Custom Settings\Custom0\install.ins
Reads from: C:\Documents and Settings\Admin\Local Settings\Application

Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK\www.microsoft[1].xml
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\index.dat
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\frameiconcache.dat
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Active\{49831954-C276-11E3-AE24-08002733366F}.dat
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{80236AC0-AAD6-11E3-AE20-08002733366F}.dat
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
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
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Silverlight\mssl.lck
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc.idx
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\47\15572e2f-21932044
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\47\15572e2f-21932044.idx
Reads from: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\7\2bbaaf87-5ca9d237
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
Reads from: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014031220140313\index.dat
Reads from: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407\index.dat
Reads from: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413\index.dat
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\296c0.msp
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\AdobeARM.log
Reads from: C:\Documents and Settings\Admin\Local
Settings\Temp\AdobeARM_NotLocked.log
Reads from: C:\Documents and Settings\Admin\Local
Settings\Temp\ASPNETSetup_00000.log
Reads from: C:\Documents and Settings\Admin\Local
Settings\Temp\ASPNETSetup_00001.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\AUCHECK_PARSER.txt
Reads from: 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
Reads from: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_depcheck_NETFX_EXP_35.txt
Reads from: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_dotnetfx35error.txt
Reads from: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_dotnetfx35install.txt
Reads from: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework20_Setup164F.txt
Reads from: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework30_Setup16AE.txt
Reads from: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework35_MSI16E2.txt
Reads from: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_NET_Framework35_MSI63E0.txt
Reads from: C:\Documents and Settings\Admin\Local
Settings\Temp\dd_RGB9RAST_x86.msi601E.txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA2A49.txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA3565.txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA35A0.txt

Reads from: 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: C:\Documents and Settings\Admin\Local
Settings\Temp\gen_py\2.7__init__.py
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\JAUReg.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\java_install.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\java_install_reg.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\jusched.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft PowerPoint
Viewer (0).log
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20131223_035827352-MSI_vc_red.msi.txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20131223_035827352.html
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_152314679-MSI_vc_red.msi.txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_152314679.html
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_152634747-MSI_vc_red.msi.txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_152634747.html
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\setup.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Silverlight0.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\SilverlightMSI.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\uxeventlog.txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\AntiPhishing\2CEDBFC-DBA8-43AA-B1FD-CC8E6316E3E2.dat
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\300lo[1].json
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\300lo[2].json
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\88666cc6-d578-45c8-baf0-89d3837f41c3_89[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\93e33485-fea3-4687-a642-2c5dd233522f_12[1].eot
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAAdClient31[1].txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAAdClient31[2].txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAAdClient31[3].txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAAdClient31[4].txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAAdClient31[5].txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\adServer[1].htm
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\auth016[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\bimapping[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\broker[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CA9ATUDW.css
Reads from: 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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\DataList[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\desktop.ini
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\CXCXW1MR\64030e7-ad8c-4be8-a45a-b69a2df3caef_13[1].eot
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[3].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\event[5].js
Reads from: 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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\georedirect[2].htm
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\omnibase[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomBlade[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\onemscomfooter[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[3].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\request[1].php
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[1].axd
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[2].axd
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[3].axd
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[4].axd
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ScriptResource[5].axd
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\script[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\script[1].jsx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\script[2].jsx
Reads from: 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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
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: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\wtid[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\wt_capi[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\desktop.ini
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\736e3781-6a19-4119-b717-e61f0d8982c0_12[1].eot
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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\auth016[1].js

Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\auth016[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\bing[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet 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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\CA39W67Q.jsx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\CAANG12B.css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\CAU35S9Y.jsx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\ChangePassword[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet 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 Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\core114[1].js
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 Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\counter017[2].js
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 Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\desktop.ini
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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\event[3].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\event[6].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\General[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\gl_social[1].svg
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\Install[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\js[1].ashx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\js[2].ashx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\js[3].ashx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\js[4].ashx
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
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
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\onemscomfooter[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\onemscomsearch[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\oneMscSocial[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP>PasswordRecovery[1].css
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 Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\ScriptResource[2].axd
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\ONWV4FIP\script[2].jsx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\SearchMSStoreClient[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\serverComponent[1].php
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\siteresource[1].ashx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\siteresource[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\style[1].cssx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\Tracker[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\true[1].htm
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\wol.common[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\wt_capi[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\08ce8e54-41ba-4695-9963-a7669022faec_12[1].eot
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\15d2470f-0fcf-45e9-bf5b-c943236a61cf_27[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\300lo[1].json
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\67706439-4969-4bc3-9e3b-50770f40b20e_36[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ADSAdClient31[1].txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\ADSAdClient31[2].txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\auth016[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\broker-config_s1[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\broker-config_s1[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\broker-config_s1[3].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\broker-config_s2[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[1]
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\CA9P88JQ.css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\core114[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\counter017[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\counter017[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\css[1].ashx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\css[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\css[2].ashx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\css[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\desktop.ini
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\DetailView[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\event[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\event[3].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\feedback[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\FormView[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\GlobalResources[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\gl_site[1].svg
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\Import[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\Install[1].css

Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\js[1].ashx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\js[2].ashx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\js[3].ashx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\js[4].ashx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\Menu[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\omnibase[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\oneMscBlade[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\oneMscComponents[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\oneMscNav[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\onemscsearch[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\oneMscSocial[2].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\ScriptResource[1].axd
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\script[1].jsx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\script[2].jsx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\SilverlightAtlas-MSCOM-Tracking[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\Silverlight[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\styles[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\uninstall-arp-win[1].htm
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\WebResource[1].axd
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\welcome[1].htm
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBF\windows8_site_ltr[1].css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\300lo[1].json
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\300lo[2].json
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\AD5AdClient31[1].txt
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\adServer[1].htm
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\auth016[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\background_gradient[1]
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bimapping[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[3].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[4].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker-config_s1[5].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker[1].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\broker[2].js
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA01EFSH.jsx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA7GG9I0.css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CA8VUH6F.css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CAI7MNGV.css
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\CallingControl[1].aspx
Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

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

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

Settings\History\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Local

Settings\History\History.IE5\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Local

Settings\History\History.IE5\index.dat
 Reads from: C:\Documents and Settings\Administrator\Local Settings\Temporary

Internet Files\Content.IE5\CXCXW1MR\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Local Settings\Temporary

Internet Files\Content.IE5\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Local Settings\Temporary

Internet Files\Content.IE5\index.dat
 Reads from: C:\Documents and Settings\Administrator\Local Settings\Temporary

Internet Files\Content.IE5\ONWV4FIP\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Local Settings\Temporary

Internet Files\Content.IE5\QXMNQBF\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Local Settings\Temporary

Internet Files\Content.IE5\UH4D6D6X\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Local Settings\Temporary

Internet Files\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\NTUSER.DAT
 Reads from: C:\Documents and Settings\Administrator\NTUSER.DAT.LOG
 Reads from: C:\Documents and Settings\Administrator\ntuser.ini
 Reads from: C:\Documents and Settings\Administrator\SendTo\Compressed (zipped)

Folder.ZFSendToTarget
 Reads from: C:\Documents and Settings\Administrator\SendTo\Desktop (create

shortcut).DeskLink
 Reads from: C:\Documents and Settings\Administrator\SendTo\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\SendTo\Mail Recipient.MAPIMail
 Reads from: C:\Documents and Settings\Administrator\Start Menu\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Accessibility\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Accessibility\Magnifier.lnk
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Accessibility\Narrator.lnk
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Command Prompt.lnk
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Entertainment\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Notepad.lnk
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Program Compatibility Wizard.lnk
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Synchronize.lnk
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Tour Windows XP.lnk
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Windows Explorer.lnk
 Reads from: C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Start Menu\Programs\Remote

Assistance.lnk
 Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Startup\desktop.ini
 Reads from: C:\Documents and Settings\Administrator\Start Menu\Programs\Windows

Media Player.lnk
 Reads from: C:\Documents and Settings\Administrator\Templates\amipro.sam
 Reads from: C:\Documents and Settings\Administrator\Templates\lotus.wk4
 Reads from: C:\Documents and Settings\Administrator\Templates\presenta.shw
 Reads from: C:\Documents and Settings\Administrator\Templates\quattro.wb2
 Reads from: C:\Documents and Settings\Administrator\Templates\wordpfct.wpd
 Reads from: C:\Documents and Settings\Administrator\Templates\wordpfct.wpg
 Reads from: C:\Documents and Settings\All Users\Application

Data\Adobe\Acrobat\9.0\Replicate\Security\directories.acrodata
 Reads from: C:\Documents and Settings\All Users\Application

Data\Adobe\Reader\9.4\ARM\AdbeRdrUpd951_all_incr.msp
 Deletes: C:\WINDOWS\Temp\tmp.exe

Network Events

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

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

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

Windows Registry Events

Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key:	HKCU\software\microsoft\internet explorer\main
Creates key:	HKLM\software\microsoft\windows\currentversion\run
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key:	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 options\752d6fe81122349daf998a56f48e0b38.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\msvcrt.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\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\wmdmps.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\comcat.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\shlwapi.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.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: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wininet.dll
 Opens key: HKLM\system\currentcontrolset\control\error message instrument\
 Opens key: HKLM\system\currentcontrolset\control\error message instrument
 Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
 Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
 Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
 Opens key: HKLM\software\microsoft\ole
 Opens key: HKCR\interface
 Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
 Opens key: HKLM\software\microsoft\oleaut
 Opens key: HKLM\software\microsoft\oleaut\userera
 Opens key: HKCU\
 Opens key: HKCU\software\policies\microsoft\control panel\desktop
 Opens key: HKCU\control panel\desktop
 Opens key:

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

options\comctl32.dll
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
 Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
 Opens key: HKCU\software\classes\
 Opens key: HKCU\software\classes\protocols\name-space handler\
 Opens key: HKCR\protocols\name-space handler
 Opens key: HKCU\software\classes\protocols\name-space handler
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings
 Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings
 Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\
 Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
 Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
 Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
 Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\zonemap\domains\
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zonemap\domains\
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\zonemap\ranges\
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zonemap\ranges\
 Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key: HKLM\system\currentcontrolset\control\wmi\security
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\ws2help.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\ws2_32.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dnsapi.dll
 Opens key: HKLM\system\currentcontrolset\services\dns\parameters
 Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
 Opens key: HKLM\system\setup
 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 key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
 Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\mswsock.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\psapi.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\shell32.dll
 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
Opens key: HKLM\software\microsoft\rpc\pagedbuffers
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\752d6fe81122349daf998a56f48e0b38.exe\rpc\threadpool\throttle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\microsoft\rpc\securityservice
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKCU\software
Opens key: HKCU\software\adobe
Opens key: HKCU\software\adobe\acrobat reader
Opens key: HKCU\software\adobe\acrobat reader\9.0
Opens key: HKCU\software\adobe\acrobat reader\9.0\access
Opens key: HKCU\software\adobe\acrobat reader\9.0\accessibility
Opens key: HKCU\software\adobe\acrobat reader\9.0\adobeviewer
Opens key: HKCU\software\adobe\acrobat reader\9.0\annots
Opens key: HKCU\software\adobe\acrobat reader\9.0\annots\cannots
Opens key: HKCU\software\adobe\acrobat reader\9.0\annots\cannots\cannot
Opens key: HKCU\software\adobe\acrobat reader\9.0\autosavedocs
Opens key: HKCU\software\adobe\acrobat reader\9.0\avconversionfrompdf
Opens key: HKCU\software\adobe\acrobat reader\9.0\avconversionfrompdf\csettings
Opens key: HKCU\software\adobe\acrobat reader\9.0\avconversiontopdf
Opens key: HKCU\software\adobe\acrobat reader\9.0\avconversiontopdf\csettings
Opens key: HKCU\software\adobe\acrobat reader\9.0\avdisplay
Opens key: HKCU\software\adobe\acrobat reader\9.0\avgeneral
Opens key: HKCU\software\adobe\acrobat reader\9.0\avgeneral\cdockables
Opens key: HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars
Opens key: HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars\cadvcommenting
Opens key: HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars\cbasiccommenting
Opens key: HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars\ccommenting
Opens key: HKCU\software\adobe\acrobat reader\9.0\avtracker
Opens key: HKCU\software\adobe\acrobat reader\9.0\collab
Opens key: HKCU\software\adobe\acrobat reader\9.0\collab\cdocumentcenter
Opens key: HKCU\software\adobe\acrobat reader\9.0\collab\cdocumentcenter\csettings

Opens key: HKCU\software\adobe\acrobat reader\9.0\collab\cemaildistribution
Opens key: HKCU\software\adobe\acrobat
reader\9.0\collab\cemaildistribution\csettings
Opens key: HKCU\software\adobe\acrobat
reader\9.0\collab\cinitiationwizardfirstlaunch
Opens key: HKCU\software\adobe\acrobat reader\9.0\collab\cserversettings
Opens key: HKCU\software\adobe\acrobat reader\9.0\formsprefs
Opens key: HKCU\software\adobe\acrobat reader\9.0\formsprefs\crequiredfieldhlcolor
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
Opens key: HKCU\software\adobe\acrobat reader\9.0\installer\migrated
Opens key: HKCU\software\adobe\acrobat reader\9.0\installpath
Opens key: HKCU\software\adobe\acrobat reader\9.0\jsprefs
Opens key: HKCU\software\adobe\acrobat reader\9.0\language
Opens key: HKCU\software\adobe\acrobat reader\9.0\language\current
Opens key: HKCU\software\adobe\acrobat reader\9.0\language\next
Opens key: HKCU\software\adobe\acrobat reader\9.0\multimedia
Opens key: HKCU\software\adobe\acrobat reader\9.0\multimedia\ccolorandborder
Opens key: HKCU\software\adobe\acrobat reader\9.0\optionalcontent
Opens key: HKCU\software\adobe\acrobat reader\9.0\originals
Opens key: HKCU\software\adobe\acrobat reader\9.0\prefsdialog
Opens key: HKCU\software\adobe\acrobat reader\9.0\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
Opens key: HKCU\software\adobe\adobe acrobat
Opens key: HKCU\software\adobe\adobe acrobat\9.0
Opens key: HKCU\software\adobe\adobe acrobat\9.0\diskcabs
Opens key: HKCU\software\adobe\adobe arm
Opens key: HKCU\software\adobe\adobe arm\1.0
Opens key: HKCU\software\adobe\adobe arm\1.0\arm
Opens key: HKCU\software\adobe\adobe synchronizer
Opens key: HKCU\software\adobe\adobe synchronizer\9.0
Opens key: HKCU\software\adobe\adobe synchronizer\9.0\acrobat.com
Opens key: HKCU\software\adobe\adobe\commonfiles
Opens key: HKCU\software\adobe\commonfiles\usage
Opens key: HKCU\software\adobe\commonfiles\usage\demographic
Opens key: HKCU\software\adobe\commonfiles\usage\reader 9
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 key: HKCU\software\macromedia
Opens key: HKCU\software\macromedia\flashplayer
Opens key: HKCU\software\macromedia\flashplayerupdate
Opens key: HKCU\software\microsoft
Opens key: HKCU\software\microsoft\active setup
Opens key: HKCU\software\microsoft\active setup\installed components
Opens key: HKCU\software\microsoft\active setup\installed components\<{12d0ed0d-0ee0-4f90-8827-78cefb8f4988}
Opens key: HKCU\software\microsoft\active setup\installed components\>{26923b43-4d38-484f-9b9e-de460746276c}
Opens key: HKCU\software\microsoft\active setup\installed components\>{60b49e34-c7cc-11d0-8953-00a0c90347ff}
Opens key: HKCU\software\microsoft\active setup\installed components\>{60b49e34-c7cc-11d0-8953-00a0c90347ff}micros
Opens key: HKCU\software\microsoft\active setup\installed components\>{881dd1c5-3dcf-431b-b061-f3f88e8be88a}
Opens key: HKCU\software\microsoft\active setup\installed components\{2179c5d3-ebff-11cf-b6fd-00aa00b4e220}
Opens key: HKCU\software\microsoft\active setup\installed components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}
Opens key: HKCU\software\microsoft\active setup\installed components\{2c7339cf-2b09-4501-b3f3-f3508c9228ed}
Opens key: HKCU\software\microsoft\active setup\installed components\{44bba840-cc51-11cf-aafa-00aa00b6015c}
Opens key: HKCU\software\microsoft\active setup\installed components\{44bba842-cc51-11cf-aafa-00aa00b6015b}
Opens key: HKCU\software\microsoft\active setup\installed components\{44bba848-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: HKCU\software\microsoft\active setup\installed components\{6bf52a52-394a-11d3-b153-00c04f79faa6}
Opens key: HKCU\software\microsoft\active setup\installed components\{7790769c-0471-11d2-af11-00c04fa35d02}

Opens key: HKCU\software\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4340}
Opens key: HKCU\software\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4383}
Opens key: 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.hkczoneinfo
Opens key: HKCU\software\microsoft\advanced inf setup\ie.hkczoneinfo\regbackup
Opens key: HKCU\software\microsoft\advanced inf setup\ie.hkczoneinfo\regbackup\0
Opens key: HKCU\software\microsoft\advanced inf
setup\ie.hkczoneinfo\regbackup\0.map
Opens key: HKCU\software\microsoft\advanced inf setup\ie40.useragent
Opens key: HKCU\software\microsoft\advanced inf setup\ie40.useragent\regbackup
Opens key: HKCU\software\microsoft\advanced inf setup\ie40.useragent\regbackup\0
Opens key: HKCU\software\microsoft\advanced inf
setup\ie40.useragent\regbackup\0.map
Opens key: HKCU\software\microsoft\advanced inf setup\iehomepageinfo
Opens key: HKCU\software\microsoft\advanced inf setup\iehomepageinfo\regbackup
Opens key: HKCU\software\microsoft\advanced inf setup\iehomepageinfo\regbackup\0
Opens key: HKCU\software\microsoft\advanced inf
setup\iehomepageinfo\regbackup\0.map
Opens key: HKCU\software\microsoft\clock
Opens key: HKCU\software\microsoft\command processor
Opens key: HKCU\software\microsoft\ctf
Opens key: HKCU\software\microsoft\ctf\assemblies
Opens key: HKCU\software\microsoft\ctf\compartment
Opens key: HKCU\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: HKCU\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-00c04fc324a1}\languageprofile
Opens key: HKCU\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-00c04fc324a1}\languageprofile\0x00000409
Opens key: HKCU\software\microsoft\direct3d
Opens key: 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\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
Opens key:	HKCU\software\microsoft\internet explorer\informationbar
Opens key:	HKCU\software\microsoft\internet explorer\international
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\10
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\11
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\12
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\13
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\14
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\15
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\16
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\17
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\18
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\19
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\20
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\21
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\22
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\23
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\24
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\25
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\26
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\27
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\28
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\29
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\3
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\30
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\34
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\35
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\37
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\38
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\39
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\4
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\5
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\6
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\7
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\8
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\9
Opens key:	HKCU\software\microsoft\internet explorer\internetregistry
Opens key:	HKCU\software\microsoft\internet explorer\linksbar
Opens key:	HKCU\software\microsoft\internet explorer\linksbar\itemcache
Opens key:	HKCU\software\microsoft\internet explorer\linksbar\itemcache\0
Opens key:	HKCU\software\microsoft\internet explorer\linksbar\itemcache\1
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry\domstorage
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry\domstorage\total
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry\extensions
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry\extensions\cmdmapping
Opens key:	HKCU\software\microsoft\internet explorer\main
Opens key:	HKCU\software\microsoft\internet explorer\main\default feeds
Opens key:	HKCU\software\microsoft\internet explorer\main\default feeds\{292f3d25-c7e7-48ac-bfba-7b9c1f5b42a7}
Opens key:	HKCU\software\microsoft\internet explorer\main\default feeds\{8dd206d8-e6a9-4797-bfe9-b6a7783eb157}
Opens key:	HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key:	HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown\settings
Opens key:	HKCU\software\microsoft\internet explorer\main\windowssearch
Opens key:	HKCU\software\microsoft\internet explorer\new windows
Opens key:	HKCU\software\microsoft\internet explorer\new windows\allow
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}
Opens key:	HKCU\software\microsoft\internet explorer\searchurl
Opens key:	HKCU\software\microsoft\internet explorer\security
Opens key:	HKCU\software\microsoft\internet explorer\security\antiphishing
Opens key:	HKCU\software\microsoft\internet explorer\security\antiphishing\2cedbfbc-dba8-43aa-b1fd-cc8e6316e3e2
Opens key:	HKCU\software\microsoft\internet explorer\security\p3global
Opens key:	HKCU\software\microsoft\internet explorer\security\p3sites
Opens key:	HKCU\software\microsoft\internet explorer\services
Opens key:	HKCU\software\microsoft\internet explorer\settings
Opens key:	HKCU\software\microsoft\internet explorer\sqm
Opens key:	HKCU\software\microsoft\internet explorer\suggested sites

Opens key: HKCU\software\microsoft\internet explorer\tabbedbrowsing
Opens key: HKCU\software\microsoft\internet explorer\toolbar
Opens key: HKCU\software\microsoft\internet explorer\toolbar\explorer
Opens key: HKCU\software\microsoft\internet explorer\toolbar\shellbrowser
Opens key: HKCU\software\microsoft\internet explorer\toolbar\webbrowser
Opens key: HKCU\software\microsoft\internet explorer\typedurls
Opens key: HKCU\software\microsoft\internet explorer\urlsearchhooks
Opens key: HKCU\software\microsoft\internet explorer\user preferences
Opens key: HKCU\software\microsoft\internet explorer\zoom
Opens key: HKCU\software\microsoft\java vm
Opens key: HKCU\software\microsoft\keyboard
Opens key: HKCU\software\microsoft\keyboard\native media players
Opens key: HKCU\software\microsoft\keyboard\native media players\wmp
Opens key: HKCU\software\microsoft\mediaplayer
Opens key: HKCU\software\microsoft\mediaplayer\battery
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets
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 key: HKCU\software\microsoft\mediaplayer\battery\presets\circledance
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\circledance\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\circledance\postshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\circledance\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\cominatya
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\cominatya\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\cominatya\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\cottonstar
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\cottonstar\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\cottonstar\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\dandelionaid
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\dandelionaid\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\dandelionaid\postshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\dandelionaid\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\drowningflower
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\drowningflower\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\drowningflower\postshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\drowningflower\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\eletriarnation
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\eletriarnation\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\eletriarnation\postshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\eletriarnation\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\eventhorizon
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\eventhorizon\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\eventhorizon\postshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\eventhorizon\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick ascii
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick
ascii\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick
ascii\postshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\geeks kick
ascii\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\gemstone matrix
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\gemstone
matrix\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\gemstone
matrix\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\grooveswirl
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\grooveswirl\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\grooveswirl\postshiftinfo

Opens key:
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\currentshiftinfo
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\illuminator\postshiftinfo
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\illuminator\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\iseethetruth
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\iseethetruth\currentshiftinfo
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\iseethetruth\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\kaleidoscope
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\kaleidoscope\currentshiftinfo
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\kchemicalnova
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\kchemicalnova\currentshiftinfo
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\kchemicalnova\postshiftinfo
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\kchemicalnova\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\lotus
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\lotus\currentshiftinfo
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
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\nerds are
cool\postshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\nerds are
cool\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\relativelycalm
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\relativelycalm\currentshiftinfo
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\relativelycalm\postshiftinfo
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\relativelycalm\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\sleepyspray
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\sleepyspray\currentshiftinfo
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\sleepyspray\postshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\smoke or water
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\smoke or
water\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\smoke or
water\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\spiderslastmoment
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\spiderslastmoment\currentshiftinfo
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\spiderslastmoment\postshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\strawberryaid
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
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\the world
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\the
world\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\the
world\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\tornado
Opens key:
HKCU\software\microsoft\mediaplayer\battery\presets\tornado\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\tornado\preshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\what is an egab
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\what is an
egab\currentshiftinfo
Opens key: HKCU\software\microsoft\mediaplayer\battery\presets\what is an
egab\postshiftinfo

Opens key: HKCU\software\microsoft\mediaplayer\health
 Opens key: HKCU\software\microsoft\mediaplayer\player
 Opens key: HKCU\software\microsoft\mediaplayer\player\settings
 Opens key: HKCU\software\microsoft\mediaplayer\player\skins
 Opens key: HKCU\software\microsoft\mediaplayer\player\tasks
 Opens key: HKCU\software\microsoft\mediaplayer\player\tasks\nowplaying
 Opens key: HKCU\software\microsoft\mediaplayer\preferences
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp
 Opens key: HKCU\software\microsoft\mediaplayer\setup
 Opens key: HKCU\software\microsoft\mediaplayer\setup\createdlinks
 Opens key: HKCU\software\microsoft\messenger\service
 Opens key: HKCU\software\microsoft\microsoft management console
 Opens key: HKCU\software\microsoft\microsoft management console\recent file list
 Opens key: HKCU\software\microsoft\microsoft management console\settings
 Opens key: HKCU\software\microsoft\ms design tools
 Opens key: HKCU\software\microsoft\ms design tools\mdtdbd
 Opens key: HKCU\software\microsoft\msdaipp
 Opens key: HKCU\software\microsoft\msdaipp\providers
 Opens key: HKCU\software\microsoft\msdaipp\providers\{9fec570-b9d4-11d1-9c78-000f875ac61}
 Opens key: HKCU\software\microsoft\msdaipp\providers\{9fec571-b9d4-11d1-9c78-000f875ac61}
 Opens key: HKCU\software\microsoft\multimedia
 Opens key: HKCU\software\microsoft\multimedia\audio
 Opens key: HKCU\software\microsoft\multimedia\audio\waveformats
 Opens key: HKCU\software\microsoft\multimedia\audio compression manager
 Opens key: HKCU\software\microsoft\multimedia\audio compression manager\msacm
 Opens key: HKCU\software\microsoft\multimedia\audio compression manager\priority
 v4.00
 Opens key: HKCU\software\microsoft\narrator
 Opens key: HKCU\software\microsoft\netdde
 Opens key: HKCU\software\microsoft\netdde\dde trusted shares
 Opens key: HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a
 Opens key: HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a\chat\$
 Opens key: HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a\clpbk\$
 Opens key: HKCU\software\microsoft\netdde\dde trusted shares\d06176d5a\hearts\$
 Opens key: HKCU\software\microsoft\netshow
 Opens key: HKCU\software\microsoft\netshow\player
 Opens key: HKCU\software\microsoft\netshow\player\remote
 Opens key: HKCU\software\microsoft\notepad
 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
 Opens key: HKCU\software\microsoft\office\11.0\common\drawalerts\ftp sites
 Opens key: HKCU\software\microsoft\office\11.0\common\dsppadaptermru
 Opens key: HKCU\software\microsoft\office\11.0\common\general
 Opens key: HKCU\software\microsoft\office\11.0\common\languageresources
 Opens key: HKCU\software\microsoft\office\11.0\common\migration
 Opens key: HKCU\software\microsoft\office\11.0\common\migration\office
 Opens key: HKCU\software\microsoft\office\11.0\common\migration\word
 Opens key: HKCU\software\microsoft\office\11.0\common\open find
 Opens key: HKCU\software\microsoft\office\11.0\common\open find\microsoft office word
 Opens key: HKCU\software\microsoft\office\11.0\common\open find\places
 Opens key: HKCU\software\microsoft\office\11.0\common\research
 Opens key: HKCU\software\microsoft\office\11.0\common\research\translation
 Opens key: HKCU\software\microsoft\office\11.0\common\toolbars
 Opens key: HKCU\software\microsoft\office\11.0\common\toolbars\settings
 Opens key: HKCU\software\microsoft\office\11.0\common\userinfo
 Opens key: HKCU\software\microsoft\office\11.0\word
 Opens key: HKCU\software\microsoft\office\11.0\word\options
 Opens key: HKCU\software\microsoft\office\11.0\word\userinfo
 Opens key: HKCU\software\microsoft\office\11.0\word\wizards
 Opens key: HKCU\software\microsoft\office\11.0\wordview
 Opens key: HKCU\software\microsoft\office\11.0\wordview\data
 Opens key: HKCU\software\microsoft\office\12.0
 Opens key: HKCU\software\microsoft\office\12.0\common
 Opens key: HKCU\software\microsoft\office\12.0\common\drawalerts
 Opens key: HKCU\software\microsoft\office\12.0\common\drawalerts\ftp sites
 Opens key: HKCU\software\microsoft\office\12.0\common\general
 Opens key: HKCU\software\microsoft\office\12.0\common\languageresources
 Opens key: HKCU\software\microsoft\office\12.0\common\languageresources\enabledlanguages
 Opens key: HKCU\software\microsoft\office\12.0\common\migration
 Opens key: HKCU\software\microsoft\office\12.0\common\migration\excel
 Opens key: HKCU\software\microsoft\office\12.0\common\migration\office
 Opens key: HKCU\software\microsoft\office\12.0\common\open find
 Opens key: HKCU\software\microsoft\office\12.0\common\open find\microsoft office

excel viewer

Opens key: HKCU\software\microsoft\office\12.0\common\open find\places
Opens key: HKCU\software\microsoft\office\12.0\common\research
Opens key: HKCU\software\microsoft\office\12.0\common\research\translation
Opens key: HKCU\software\microsoft\office\12.0\excel
Opens key: HKCU\software\microsoft\office\12.0\excel\options
Opens key: HKCU\software\microsoft\office\12.0\excel viewer
Opens key: HKCU\software\microsoft\office\12.0\excel viewer\viewer options
Opens key: HKCU\software\microsoft\office\12.0\user settings
Opens key: HKCU\software\microsoft\office\12.0\user settings\excel_intl
Opens key: HKCU\software\microsoft\office\12.0\user settings\mso_intl
Opens key: HKCU\software\microsoft\office\12.0\user settings\powerpoint_intl
Opens key: HKCU\software\microsoft\office\14.0
Opens key: HKCU\software\microsoft\office\14.0\common
Opens key: HKCU\software\microsoft\office\14.0\common\drawalerts
Opens key: HKCU\software\microsoft\office\14.0\common\drawalerts\ftp sites
Opens key: HKCU\software\microsoft\office\14.0\common\general
Opens key: HKCU\software\microsoft\office\14.0\common\language resources
Opens key:

HKCU\software\microsoft\office\14.0\common\language resources\enabled languages

Opens key: HKCU\software\microsoft\office\14.0\common\open find
Opens key: HKCU\software\microsoft\office\14.0\common\open find\microsoft

powerpoint viewer

Opens key: HKCU\software\microsoft\office\14.0\common\open find\places
Opens key: HKCU\software\microsoft\office\14.0\common\research
Opens key: HKCU\software\microsoft\office\14.0\common\research\translation
Opens key: HKCU\software\microsoft\office\14.0\powerpoint
Opens key: HKCU\software\microsoft\office\14.0\powerpoint viewer
Opens key: HKCU\software\microsoft\office\14.0\powerpoint viewer\options
Opens key: HKCU\software\microsoft\office\common
Opens key: HKCU\software\microsoft\office\common\smart tag
Opens key: HKCU\software\microsoft\office\common\smart tag\actions
Opens key: HKCU\software\microsoft\office\common\smart tag\actions\{339361cd-6723-

455d-a40b-c95f1f91ff8a}

Opens key: HKCU\software\microsoft\office\common\smart tag\actions\{49df3409-46b3-

4b0c-b7bf-fec0f9401edd}

Opens key: HKCU\software\microsoft\office\common\smart tag\actions\{64ab6c69-b40e-

40af-9b7f-f5687b48e2b6}

Opens key: HKCU\software\microsoft\office\common\smart tag\actions\{c3754d1a-04d3-

4085-8cfb-97705b57a98f}

Opens key: HKCU\software\microsoft\office\common\smart tag\actions\{f114ae61-1331-

4238-92c9-bbe330af25fd}

Opens key: HKCU\software\microsoft\office\common\smart tag\recognizers

Opens key: HKCU\software\microsoft\office\common\smart tag\recognizers\{64ab6c69-

b40e-40af-9b7f-f5687b48e2b6}

Opens key: HKCU\software\microsoft\office\common\smart tag\recognizers\{87ef1cfe-

51ca-4e6b-8c76-e576aa926888}

Opens key: HKCU\software\microsoft\office\common\userinfo

Opens key: HKCU\software\microsoft\outlook express

Opens key: HKCU\software\microsoft\outlook express\5.0

Opens key: HKCU\software\microsoft\outlook express\5.0\shared settings

Opens key: HKCU\software\microsoft\outlook express\5.0\shared settings\setup

Opens key: HKCU\software\microsoft\plus!

Opens key: HKCU\software\microsoft\plus!\themes

Opens key: HKCU\software\microsoft\plus!\themes\apply

Opens key: HKCU\software\microsoft\plus!\themes\current

Opens key: HKCU\software\microsoft\protected storage system provider

Opens key: HKCU\software\microsoft\protected storage system provider\s-1-5-21-

1757981266-507921405-1957994488-1003

Opens key: HKCU\software\microsoft\ras phonebook

Opens key: HKCU\software\microsoft\regedt32

Opens key: HKCU\software\microsoft\regedt32\settings

Opens key: HKCU\software\microsoft\sapi layer

Opens key: HKCU\software\microsoft\schedule+

Opens key: HKCU\software\microsoft\schedule+\microsoft schedule+

Opens key: HKCU\software\microsoft\search assistant

Opens key: HKCU\software\microsoft\security center

Opens key: HKCU\software\microsoft\shared

Opens key: HKCU\software\microsoft\shared tools

Opens key: HKCU\software\microsoft\shared tools\font mapping

Opens key: HKCU\software\microsoft\shared tools\proofing tools

Opens key: HKCU\software\microsoft\shared tools\proofing tools\custom dictionaries

Opens key: HKCU\software\microsoft\speech

Opens key: HKCU\software\microsoft\speech\applexicons

Opens key: HKCU\software\microsoft\speech\audiooutput

Opens key: HKCU\software\microsoft\speech\currentuserlexicon

Opens key: HKCU\software\microsoft\speech\currentuserlexicon\applexicons

Opens key: HKCU\software\microsoft\speech\currentuserlexicon\{c9e37c15-df92-4727-

85d6-72e5eeb6995a}

Opens key: HKCU\software\microsoft\speech\currentuserlexicon\{c9e37c15-df92-4727-

85d6-72e5eeb6995a}\files

Opens key: HKCU\software\microsoft\speech\phoneconverters

Opens key: HKCU\software\microsoft\speech\voices

Opens key: HKCU\software\microsoft\sqlclient
 Opens key: HKCU\software\microsoft\systemcertificates
 Opens key: HKCU\software\microsoft\systemcertificates\ca
 Opens key: HKCU\software\microsoft\systemcertificates\ca\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\ca\crls
 Opens key: HKCU\software\microsoft\systemcertificates\ca\ctls
 Opens key: HKCU\software\microsoft\systemcertificates\disallowed
 Opens key: HKCU\software\microsoft\systemcertificates\disallowed\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\disallowed\crls
 Opens key: HKCU\software\microsoft\systemcertificates\disallowed\ctls
 Opens key: HKCU\software\microsoft\systemcertificates\my
 Opens key: HKCU\software\microsoft\systemcertificates\root
 Opens key: HKCU\software\microsoft\systemcertificates\root\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\root\crls
 Opens key: HKCU\software\microsoft\systemcertificates\root\ctls
 Opens key: HKCU\software\microsoft\systemcertificates\root\protectedroots
 Opens key: HKCU\software\microsoft\systemcertificates\trust
 Opens key: HKCU\software\microsoft\systemcertificates\trust\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\trust\crls
 Opens key: HKCU\software\microsoft\systemcertificates\trust\ctls
 Opens key: HKCU\software\microsoft\systemcertificates\trustedpublisher
 Opens key: HKCU\software\microsoft\systemcertificates\trustedpublisher\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\trustedpublisher\crls
 Opens key: HKCU\software\microsoft\systemcertificates\trustedpublisher\ctls
 Opens key: HKCU\software\microsoft\visualstudio
 Opens key: HKCU\software\microsoft\visualstudio\9.0
 Opens key: HKCU\software\microsoft\visualstudio\9.0\downloadmanager
 Opens key: HKCU\software\microsoft\wbem
 Opens key: HKCU\software\microsoft\wbem\wmic
 Opens key: HKCU\software\microsoft\windows
 Opens key: HKCU\software\microsoft\windows\currentversion
 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
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\bitbucket
 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\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
 ad25-11d0-98a8-0800361b1103}
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{645ff040-
 5081-101b-9f08-00aa002f954e}
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
 42a0-1069-a2ea-08002b30309d}
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\comdlg32
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\lastvisitedmru
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\opensavemru
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\desktop
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\desktop\cleanupwiz
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\discardable
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\discardable\postsetup
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .aif
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .aifc
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .aiff
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .application
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .asf
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .asx
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .au
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .avi
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .bmp
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .css
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .dib
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .doc
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .docm
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .docx
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .dot
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .dvr-ms
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .egg-
 info
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .emf

[illegible]

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\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
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\stuckrects2
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\tips
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\traynotify
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\userassist
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{5e6ab780-7743-11cf-a12b-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 key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\animatemax
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\comboboxanimation
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\cursorshadow
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dragfullwindows
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dropshadow
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\fontsmoothing
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listboxsmoothscrolling
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewalphaselect
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewshadow
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewwatermark
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\menuanimation
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\selectionfade
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\taskbaranimations
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\themes
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\tooltipanimation
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\webview
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\webview
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\webview\barricadedfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\00000000000083a1
Opens key: HKCU\software\microsoft\windows\currentversion\ext
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-e8ad-4283-a596-fa578c2ebdc3}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{4eb89ff4-7f78-4a0f-8b8d-2bf02e94e4b2}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{4edcb26c-d24c-4e72-af07-b576699ac0de}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{7390f3d8-0439-4c05-91e3-cf5cb290c3d0}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{754ff233-5d4e-11d2-875b-00a0c93c09b3}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{7584c670-2274-4efb-b00b-d6aaba6d3850}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{761497bb-d6f0-462c-b6eb-d4daf1d92d43}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{9059f30f-4eb1-4bd2-9fdc-36f43a218f4a}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{b1549e58-3894-11d2-bb7f-00a0c999c4c1}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{bdd307c3-7bc0-4542-9f8f-a9611fe6c1bf}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{c533adf1-0c80-11d1-8c54-00a02468f316}

Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{d27cdb6e-ae6d-11cf-96b8-444553540000}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{e7e6f031-17ce-4c07-bc86-eabfe594f69c}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{25336920-03f9-11cf-8fd0-00aa00686f13}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{761497bb-d6f0-462c-b6eb-d4daf1d92d43}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{8856f961-340a-11d0-a96b-00c04fd705a2}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{cfbfae00-17a6-11d0-99cb-00c04fd64497}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{d27cdb6e-ae6d-11cf-96b8-444553540000}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{dfeaf541-f3e1-4c24-acac-99c30715084a}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{e2e2dd38-d088-4134-82b7-f2ba38496583}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{e7e6f031-17ce-4c07-bc86-eabfe594f69c}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{fb5f1910-f110-11d2-bb9e-00c04f795683}
Opens key: HKCU\software\microsoft\windows\currentversion\group policy
Opens key: HKCU\software\microsoft\windows\currentversion\group policy\apppgmt
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\history\{a2e30f80-d7de-11d2-bbde-00c04f86ae3b}
Opens key: HKCU\software\microsoft\windows\currentversion\group policy objects
Opens key: HKCU\software\microsoft\windows\currentversion\group policy objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}machine
Opens key: HKCU\software\microsoft\windows\currentversion\group policy objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}machine\software
Opens key: HKCU\software\microsoft\windows\currentversion\group policy objects\{4b317659-5c00-4b7a-9031-b30cb0cca9f5}user
Opens key: HKCU\software\microsoft\windows\currentversion\grpconv
Opens key: HKCU\software\microsoft\windows\currentversion\grpconv\mapgroups
Opens key: HKCU\software\microsoft\windows\currentversion\internet
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings
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
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\activities\blog
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\activities\email
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\activities\map
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\activities\translate
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\cache\content
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\cache\cookies
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\cache\history
Opens key: HKCU\software\microsoft\windows\currentversion\internet 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
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\3

Opens key: HKCU\software\microsoft\windows\currentversion\internet
 settings\lockdown_zones\4
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\p3p
 Opens key: HKCU\software\microsoft\windows\currentversion\internet
 settings\p3p\history
 Opens key: HKCU\software\microsoft\windows\currentversion\internet
 settings\passport
 Opens key: HKCU\software\microsoft\windows\currentversion\internet
 settings\passport\damap
 Opens key: HKCU\software\microsoft\windows\currentversion\internet
 settings\protocols
 Opens key: HKCU\software\microsoft\windows\currentversion\internet
 settings\protocols\mailto
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\url
 history
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap
 Opens key: HKCU\software\microsoft\windows\currentversion\internet
 settings\zonemap\domains
 Opens key: HKCU\software\microsoft\windows\currentversion\internet
 settings\zonemap\esdomains
 Opens key: HKCU\software\microsoft\windows\currentversion\internet
 settings\zonemap\protocoldefaults
 Opens key: HKCU\software\microsoft\windows\currentversion\internet
 settings\zonemap\ranges
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
 Opens key: HKCU\software\microsoft\windows\currentversion\policies
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
 Opens key: HKCU\software\microsoft\windows\currentversion\run
 Opens key: HKCU\software\microsoft\windows\currentversion\runonce
 Opens key: HKCU\software\microsoft\windows\currentversion\settings
 Opens key: HKCU\software\microsoft\windows\currentversion\settings\zonemap
 Opens key:
 HKCU\software\microsoft\windows\currentversion\settings\zonemap\protocoldefaults
 Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions
 Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\approved
 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: HKCU\software\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 key:
 HKCU\software\microsoft\windows\currentversion\telephony\handoffpriorities\mediamodes
 Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
 Opens key: HKCU\software\microsoft\windows\currentversion\themes
 Opens key:
 HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleoff
 Opens key:
 HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleon
 Opens key: HKCU\software\microsoft\windows\currentversion\themes\lasttheme
 Opens key: HKCU\software\microsoft\windows\currentversion\webcheck
 Opens key: HKCU\software\microsoft\windows\currentversion\webcheck\store.1
 Opens key:
 HKCU\software\microsoft\windows\currentversion\webcheck\store.1\{462932d0-0018-01cf-0000-
 00002cc2cb62}
 Opens key: HKCU\software\microsoft\windows\currentversion\windowsupdate
 Opens key: HKCU\software\microsoft\windows\currentversion\wintrust
 Opens key: HKCU\software\microsoft\windows\currentversion\wintrust\trust providers
 Opens key: HKCU\software\microsoft\windows\currentversion\wintrust\trust
 providers\software publishing
 Opens key: HKCU\software\microsoft\windows\shell
 Opens key: HKCU\software\microsoft\windows\shell\bagmru
 Opens key: HKCU\software\microsoft\windows\shell\bags
 Opens key: HKCU\software\microsoft\windows\shell\bags\1
 Opens key: HKCU\software\microsoft\windows\shell\bags\1\desktop
 Opens key: HKCU\software\microsoft\windows\shell\localizedresourcename
 Opens key: HKCU\software\microsoft\windows\shell\noroam
 Opens key: HKCU\software\microsoft\windows\shell\noroam\bagmru
 Opens key: HKCU\software\microsoft\windows\shell\noroam\bagmru\0
 Opens key: HKCU\software\microsoft\windows\shell\noroam\bagmru\0\0
 Opens key: HKCU\software\microsoft\windows\shell\noroam\bagmru\0\1
 Opens key: HKCU\software\microsoft\windows\shell\noroam\bagmru\1
 Opens key: HKCU\software\microsoft\windows\shell\noroam\bagmru\2
 Opens key: HKCU\software\microsoft\windows\shell\noroam\bagmru\2\0
 Opens key: HKCU\software\microsoft\windows\shell\noroam\bagmru\3

[illegible]

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

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

```
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-abcddeffedcb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-abcddeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0021-abcddeffedcbc}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-abcddeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-abcddeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0022-abcddeffedcbd}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-abcddeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-abcddeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0023-abcddeffedcbc}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcddeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcddeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0024-abcddeffedcbd}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcddeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcddeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0025-abcddeffedcbc}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-abcddeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0026-abcddeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0027-abcddeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0028-abcddeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0016-0000-0029-abcddeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0000-abcddeffedcba}
```

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}
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-
abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-abcdeffedcbb}
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-abcdeffedcbc}
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0001-
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
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-abcdeffedcba}
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
Opens key: HKCU\software\classes\software
Opens key: HKCU\software\classes\software\microsoft
Opens key: HKCU\software\classes\software\microsoft\mediaplayer
Opens key: HKCU\software\classes\software\microsoft\mediaplayer\preferences
Opens key: HKLM\software\microsoft\windows\currentversion\run
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mf42u.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\npptools.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\packet.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wpcap.dll
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage
Opens key: HKLM\system\currentcontrolset\services\npf
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
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: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
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: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004\linkage
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005\linkage
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006

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: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\linkage
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\linkage
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0009
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0009\linkage
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010\linkage
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\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\752d6fe81122349daf998a56f48e0b38.exe
Opens key: HKLM\software\microsoft\ctf\systemshared\
Opens key: HKCU\keyboard layout\toggle
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKCU\software\flashfxp
Opens key: HKCU\software\flashfxp\3
Opens key: HKCU\software\flashfxp\4
Opens key: HKLM\software\flashfxp
Opens key: HKLM\software\flashfxp\3
Opens key: HKLM\software\flashfxp\4
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 key: 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
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\directdrawex
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\dxm_runtime
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\fontcore
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\icw
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\idnmitigationapis
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\ie40
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\ie4data
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\ie5bakex
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\ie7
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\ie8
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\iedata
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-v5
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\microsoft .net framework 3.5 sp1
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\mobileoptionpack
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\mplayer2
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\netmeeting
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\nlsdownlevelmapping
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\outlookexpress
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\pchealth
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\schedulingagent
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\wic
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-3d01-b289-befc77a11a1e}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-4ca4-87b4-2f83217002ff}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{350c97b0-3d7c-4ee8-baa9-00bcb3d54227}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{4a03706f-666a-4037-7777-5f2748764d10}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-0000000ff1ce}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-11d3-8cfe-0150048383c9}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{95120000-003f-

0409-0000-0000000ff1ce}
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-
 0409-0000-0000000ff1ce}
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-
 3813-a88d-b8dccde8f8c7}
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-
 1033-7b44-a93000000001}
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-
 3f2d-899a-6a1d67f2073f}
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-
 4027-b136-2b3e1f5ab6e2}
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-
 36ca-84d3-9f4dcf5c5bd9}
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-
 36ca-84d3-9f4dcf5c5bd9}.kb953595
 Opens key: HKCU\software\bpftp\bullet proof ftp\main
 Opens key: HKCU\software\bulletproof software\bulletproof ftp client\main
 Opens key: HKCU\software\bpftp\bullet proof ftp\options
 Opens key: HKCU\software\bulletproof software\bulletproof ftp client\options
 Opens key: HKCU\software\bulletproof software\bulletproof ftp client 2010\options
 Opens key: HKCU\software\bpftp
 Opens key: HKCU\software\turboftp
 Opens key: HKCU\software\cryer\websitepublisher
 Opens key: HKLM\system\currentcontrolset\control\computername
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens key: HKU\
 Opens key: HKCU\software\ftpclient\sites
 Opens key: HKCU\software\softx.org\ftpclient\sites
 Opens key: HKCU\software\vandyke\securefx
 Opens key: HKLM\software\microsoft\windows\currentversion
 Opens key: HKCU\software\globalscape\cuteftp 6 home\qctoolbar
 Opens key: HKCU\software\globalscape\cuteftp 6 professional\qctoolbar
 Opens key: HKCU\software\globalscape\cuteftp 7 home\qctoolbar
 Opens key: HKCU\software\globalscape\cuteftp 7 professional\qctoolbar
 Opens key: HKCU\software\globalscape\cuteftp 8 home\qctoolbar
 Opens key: HKCU\software\globalscape\cuteftp 8 professional\qctoolbar
 Opens key: HKCU\software\sota\ffftp\options
 Opens key: HKCU\software\south river technologies\webdrive\connections
 Opens key: HKCU\software\nch software\classicftp\ftpaccounts
 Opens key: HKLM\software\nch software\fling\accounts
 Opens key: HKCU\software\filezilla
 Opens key: HKCU\software\filezilla\recent servers
 Opens key: HKCU\software\filezilla\site manager
 Opens key: HKCU\software\ftp explorer\profiles
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\ultraftp
 Opens key: HKCU\software\martin prikryl
 Opens key: HKLM\software\martin prikryl
 Opens key: HKCU\software\ftpware\coreftp\sites
 Opens key: HKCU\software\far\plugins\ftp\hosts
 Opens key: HKCU\software\far2\plugins\ftp\hosts
 Opens key: HKCU\software\far\saveddialoghistory\ftpghost
 Opens key: HKCU\software\far2\saveddialoghistory\ftpghost
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\userenv.dll
 Opens key: HKLM\system\currentcontrolset\control\productoptions
 Opens key: HKLM\software\policies\microsoft\windows\system
 Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 1757981266-507921405-1957994488-1003
 Opens key: HKCU\software\ghisler\windows commander
 Opens key: HKCU\software\ghisler\total commander
 Opens key: HKLM\software\ghisler\windows commander
 Opens key: HKLM\software\ghisler\total commander
 Opens key: HKCU\software\acebit
 Opens key: HKLM\software\acebit
 Opens key: HKCR\typelib\{cb1f2c0f-8094-4aac-bcf5-41a64e27f777}
 Opens key: HKCR\typelib\{9ea55529-e122-4757-bc79-e4825f80732c}
 Opens key: HKLM\software
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\atl.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\pstorec.dll
 Opens key: HKCU\software\mozilla
 Opens key: HKLM\software\mozilla
 Opens key: HKLM\software\mozilla\firefox
 Opens key: HKLM\software\mozilla\firefox\extensions
 Opens key: HKCU\software\chromeplus
 Opens key: HKCU\software\leechftp
 Opens key: HKLM\software\classes
 Opens key: HKCU\software\flashpeak\blazeftp\settings
 Opens key: HKCR\typelib\{f9043c88-f6f2-101a-a3c9-08002b2f49fb}\1.2\0\win32
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[752d6fe81122349daf998a56f48e0b38]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[752d6fe81122349daf998a56f48e0b38]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[752d6fe81122349daf998a56f48e0b38.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[appendtomultilabelname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[screenbadtlds]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[screenunreachableservers]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[filterclusterip]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usedns]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usehostsfile]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerreverselookup]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerwanadapters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationttl]
Queries value:

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

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationrefreshinterval]
Queries value:

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

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationmaxaddresscount]
Queries value:

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

HKLM\system\currentcontrolset\services\dnsCache\parameters[updatesecuritylevel]
Queries 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]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachesize]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachettl]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[maxnegativecachettl]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[adapertimeoutlimit]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[serverprioritytimelimit]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachedsockets]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastlistenlevel]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsendlevel]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[systemsetupinprogress]
Queries value:

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

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

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

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

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value:

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

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

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value:

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storiesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storiesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storiesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKLM\system\currentcontrolset\control\nls\language_groups[5]
Queries value: HKLM\system\currentcontrolset\control\nls\language_groups[1]
Queries value: HKLM\system\currentcontrolset\control\nls\language_groups[2]
Queries value: HKLM\system\currentcontrolset\control\nls\language_groups[4]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000419]
Queries value: HKCU\software\microsoft\internet explorer\main[]
Queries value: HKCU\software\microsoft\internet explorer\main[shownotifysize]
Queries value: HKCU\software\microsoft\internet explorer\main[recordsavedactive]
Queries value: HKCU\software\microsoft\internet explorer\main[widthlocalizeduse]
Queries value: HKCU\software\microsoft\internet explorer\main[pagecompressedinvalid]
Queries value: HKCU\software\microsoft\internet explorer\main[textcompletedmin]
Queries value: HKLM\software\microsoft\windows\currentversion\run[sonyagent]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseobtainedtime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseterminatestime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpserver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000[componentid]

Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000\linkage[export]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\linkage[export]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationenabled]
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]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpnameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[usezerobroadcast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpipaddress]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpcsubnetmask]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002\linkage[export]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003\linkage[export]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004\linkage[export]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005\linkage[export]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006\linkage[export]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\linkage[export]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\linkage[export]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0009[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0009\linkage[export]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010\linkage[export]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011\linkage[export]
Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\addressbook[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash

player activex[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash
player activex[displayname]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\branding[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\connection
manager[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\directanimation[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\directdrawex[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\dxm_runtime[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\fontcore[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\icw[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\idnmitigationapis[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie40[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie4data[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie5bakex[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie7[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie8[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie8[displayname]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\iedata[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-
v5[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\kb954550-
v5[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\microsoft .net
framework 3.5 sp1[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\microsoft .net
framework 3.5 sp1[displayname]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\mobileoptionpack[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\mplayer2[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\netmeeting[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\nlsdownlevelmapping[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\outlookexpress[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\pchealth[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\pchealth[displayname]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\schedulingagent[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\wic[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-
3d01-b289-befc77a11a1e}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-
3d01-b289-befc77a11a1e}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-
4ca4-87b4-2f83217002ff}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-
4ca4-87b4-2f83217002ff}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{350c97b0-3d7c-
4ee8-baa9-00bcb3d54227}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{4a03706f-666a-
4037-7777-5f2748764d10}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-
0409-0000-00000000ff1ce}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-
0409-0000-00000000ff1ce}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-
11d3-8cfe-0150048383c9}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-
11d3-8cfe-0150048383c9}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{95120000-003f-
0409-0000-00000000ff1ce}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{95120000-003f-
0409-0000-00000000ff1ce}[displayname]

Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-0000000ff1ce}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-0000000ff1ce}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-3813-a88d-b8dccde8f8c7}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-3813-a88d-b8dccde8f8c7}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-a93000000001}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-a93000000001}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-3f2d-899a-6a1d67f2073f}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-3f2d-899a-6a1d67f2073f}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-4027-b136-2b3e1f5ab6e2}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-4027-b136-2b3e1f5ab6e2}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-36ca-84d3-9f4dcf5c5bd9}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-36ca-84d3-9f4dcf5c5bd9}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-36ca-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]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[chkacdebuglevel]
Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[personal]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local settings]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsopdebuglevel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileimagepath]
Queries value: HKLM\software[debuglogpath]
Queries value: HKLM\software[debugloglevel]
Queries value: HKLM\software[enableddebuglog]
Queries value: HKLM\software\mozilla\firefox[pathtoexe]
Queries value: HKLM\software\mozilla\firefox\extensions[pathtoexe]
Queries value: HKLM\software\mozilla[pathtoexe]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\addressbook[addressbook]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\branding[branding]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\connection manager[connection manager]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\directanimation[directanimation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\directdrawex[directdrawex]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\dxm_runtime[dxm_runtime]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\fontcore[fontcore]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\icw[icw]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\idnmitigationapis[idnmitigationapis]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\ie40[ie40]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\ie4data[ie4data]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\ie5bakex[ie5bakex]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\ie7[ie7]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\iedata[iedata]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\mobileoptionpack[mobileoptionpack]
Queries value:

HKLM\software\microsoft\windows\currentversion\uninstall\mplayer2[mplayer2]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\netmeeting[netmeeting]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\nlsdownlevelmapping[nlsdownlevelmapping]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\outlookexpress[outlookexpress]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\schedulingagent[schedulingagent]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\wic[wic]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{350c97b0-3d7c-4ee8-baa9-00bc3d54227}\{350c97b0-3d7c-4ee8-baa9-00bc3d54227}
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{4a03706f-666a-4037-7777-5f2748764d10}\{4a03706f-666a-4037-7777-5f2748764d10}
Queries value: HKCU\software\classes\{clsid\{11c1d741-a95b-11d2-8a80-0080adb32ff4}\inprocserver32]
Queries value: HKLM\software\classes\{clsid\{11c1d741-a95b-11d2-8a80-0080adb32ff4}\inprocserver32]
Queries value: HKCU\software\classes\{ftp++.link\shell\open\command]
Queries value: HKLM\software\classes\{ftp++.link\shell\open\command]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[shownotifysize]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[recordsavedactive]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[widthlocalizeduse]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[pagecompressedinvalid]
Sets/Creates value: HKCU\software\microsoft\internet explorer\main[textcompletedmin]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\run[sonyagent]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[local appdata]
Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common appdata]
Value changes: HKCU\software\microsoft\internet explorer\main[textcompletedmin]