# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3306, Task ID: 732

Task ID: 732 Risk Level: 10

Date Processed: 2016-05-18 10:31:27 (UTC)

Processing Time: 62.14 seconds Virtual Environment: IntelliVM

**Execution Arguments:** "c:\windows\temp\35644f3d0029f81c3d478d3c2407fac3.exe"

Sample ID: Type: basic Owner: admin

35644f3d0029f81c3d478d3c2407fac3 Label:

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

PE32:win32:gui File Type: File Size: 597504 bytes

35644f3d0029f81c3d478d3c2407fac3 MD5:

05093ba493e460b909f4922656c72a340517b31d8d6ff569dd73a2c1c9fc04dd SHA256:

Description: None

### Pattern Matching Results

Writes to system32 folder

2 PE: Nonstandard section

10 Creates malicious mutex: Expiro [Fileinfector]

6 Suspicious packer: VMProtect

5 Creates process in suspicious location

5 Validates shell extensions

3 Long sleep detected

Terminates process under Windows subfolder

#### Static Events

Anomaly: PE: Contains one or more non-standard sections

#### Process/Thread Events

C:\WINDOWS\Temp\35644f3d0029f81c3d478d3c2407fac3.exe Creates process:

["c:\windows\temp\35644f3d0029f81c3d478d3c2407fac3.exe" ]

C:\WINDOWS\system32\cisvc.exe [C:\WINDOWS\system32\cisvc.exe] Creates process: C:\WINDOWS\system32\cidaemon.exe ["cidaemon.exe" DownLevelDaemon Creates process:

"c:\system volume information\catalog.wci" 1966721 16561]

C:\WINDOWS\system32\verclsid.exe [/S /C {E4B29F9D-D390-480B-92FD-Creates process:

7DDB47101D71} /I {0000010B-0000-0000-C000-000000000046} /X 0x401]

C:\WINDOWS\system32\verclsid.exe [/S /C {EB9B1153-3B57-4E68-959A-Creates process:

A3266BC3D7FE} /I {0000010B-0000-0000-C000-000000000046} /X 0x401]

C:\WINDOWS\system32\verclsid.exe [/S /C {875CB1A1-0F29-45DE-A1AE-Creates process: CFB4950D0B78} /I {0000010B-0000-0000-C000-000000000046} /X 0x401]

C:\WINDOWS\system32\verclsid.exe [/S /C {FBF23B40-E3F0-101B-8488-Creates process: 00AA003E56F8} /I {0000010B-0000-0000-C000-000000000046} /X 0x401]

CiSvc [C:\WINDOWS\system32\cisvc.exe] Loads service:

Terminates process: C:\WINDOWS\Temp\35644f3d0029f81c3d478d3c2407fac3.exe

Terminates process: C:\WINDOWS\system32\verclsid.exe

## Named Object Events

Creates mutex:	\BaseNamedObjects\PDH_PLA_MUTEX
Creates mutex:	\BaseNamedObjects\kkq-vx_mtx1

\BaseNamedObjects\kkq-vx\_mtx28 Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-Creates mutex:

1957994488-1003

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

1957994488-1003

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

1957994488-1003

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

1957994488-1003

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

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

\BaseNamedObjects\SHIMLIB\_LOG\_MUTEX Creates mutex: \BaseNamedObjects\gazavat-svc Creates mutex:

Creates mutex: \BaseNamedObjects\gazavat-svc\_28 Creates mutex:  $\BaseNamedObjects\CiPerfMonMutex$ 

\BaseNamedObjects\c::system volume information:catalog.wci\_\_cimutexsem Creates mutex:

Creates event: \BaseNamedObjects\DINPUTWINMM

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

\BaseNamedObjects\crypt32LogoffEvent Creates event:

Creates event: \BaseNamedObjects\c::system volume information\_\_cievent3

Creates event: \BaseNamedObjects\c::system volume information:catalog.wci\_\_cievent1 Creates event:

\BaseNamedObjects\c::system volume information:catalog.wci\_\_cievent2 \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57} Creates semaphore: Creates semaphore:

\BaseNamedObjects\OleDfRoot00002550B Creates semaphore:

Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

## File System Events

File System Events	
Creates:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.vir
Creates:	<pre>C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe</pre>
Creates:	C:\WINDOWS\system32\cisvc.vir
Creates:	C:\WINDOWS\system32\cisvc.exe
Creates:	<pre>C:\WINDOWS\system32\clipsrv.vir C:\WINDOWS\system32\clipsrv.exe</pre>
Creates:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.vir
Creates:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
Creates:	C:\System Volume Information
Creates:	C:\System Volume Information\catalog.wci
Creates:	C:\WINDOWS\system32\dmadmin.vir
Creates:	<pre>C:\System Volume Information\catalog.wci\CiSP0000.000 C:\System Volume Information\catalog.wci\CiSP0000.001</pre>
Creates: Creates:	C:\System Volume Information\catalog.wci\CiSP0000.001 C:\System Volume Information\catalog.wci\CiSP0000.002
Creates:	C:\WINDOWS\system32\dmadmin.exe
Creates:	C:\System Volume Information\catalog.wci\INDEX.000
Creates:	<pre>C:\System Volume Information\catalog.wci\INDEX.001</pre>
Creates:	C:\System Volume Information\catalog.wci\INDEX.002
Creates:	C:\System Volume Information\catalog.wci\CiFLfffd.000
Creates: Foundation\infocard.vir	C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication
Creates:	C:\System Volume Information\catalog.wci\CiFLfffd.001
Creates:	C:\System Volume Information\catalog.wci\CiFLfffd.002
Creates:	C:\System Volume Information\catalog.wci\CiCL0001.000
Creates:	C:\System Volume Information\catalog.wci\CiCL0001.001
Creates:	<pre>C:\System Volume Information\catalog.wci\CiCL0001.002</pre>
Creates:	C:\System Volume Information\catalog.wci\CiSL0001.000
Creates:	<pre>C:\System Volume Information\catalog.wci\CiSL0001.001 C:\System Volume Information\catalog.wci\CiSL0001.002</pre>
Creates: Creates:	C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication
Foundation\infocard.exe	C. WINDOWS WILL OSOT C. NET WIT MINEWOY KVS. O WITHOWS COMMUNICATION
Creates:	C:\System Volume Information\catalog.wci\CiP10000.000
Creates:	<pre>C:\System Volume Information\catalog.wci\CiP10000.001</pre>
Creates:	C:\System Volume Information\catalog.wci\CiP10000.002
Creates:	C:\System Volume Information\catalog.wci\CiP20000.000
Creates: Creates:	<pre>C:\System Volume Information\catalog.wci\CiP20000.001 C:\System Volume Information\catalog.wci\CiP20000.002</pre>
Creates:	C:\System Volume Information\catalog.wci\CiPT0000.002
Creates:	C:\System Volume Information\catalog.wci\CiPT0000.001
Creates:	C:\System Volume Information\catalog.wci\CiPT0000.002
Creates:	<pre>C:\System Volume Information\catalog.wci\CiST0000.000</pre>
Creates:	C:\System Volume Information\catalog.wci\CiST0000.001
Creates:	C:\System Volume Information\catalog.wci\CiST0000.002
Creates: Creates:	<pre>C:\System Volume Information\catalog.wci\00000001.ps1 C:\System Volume Information\catalog.wci\propstor.bk1</pre>
Creates:	C:\System Volume Information\catalog.wci\00000001.ps2
Creates:	C:\System Volume Information\catalog.wci\propstor.bk2
Creates:	<pre>C:\System Volume Information\catalog.wci\cicat.hsh</pre>
Creates:	C:\System Volume Information\catalog.wci\CiVP0000.000
Creates:	C:\System Volume Information\catalog.wci\CiVP0000.001
Creates: Creates:	<pre>C:\System Volume Information\catalog.wci\CiVP0000.002 C:\System Volume Information\catalog.wci\cicat.fid</pre>
Creates:	C:\WINDOWS\system32\imapi.vir
Creates:	C:\WINDOWS\system32\imapi.exe
Creates:	C:\System Volume Information\catalog.wci\00000002.ps1
Creates:	<pre>C:\System Volume Information\catalog.wci\00000002.ps2</pre>
Creates:	C:\WINDOWS\system32\mnmsrvc.vir
Creates:	C:\WINDOWS\system32\mnmsrvc.exe
Creates:	C:\WINDOWS\system32\msiexec.vir C:\WINDOWS\system32\msiexec.exe
Creates:	C:\WINDOWS\system32\netdde.vir
Creates:	C:\WINDOWS\system32\netdde.exe
Creates:	<pre>C:\Program Files\Common Files\Microsoft Shared\Source Engine\ose.vir</pre>
Creates:	C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE
Creates:	C:\WINDOWS\system32\sessmgr.vir
Creates:	C:\WINDOWS\system32\sessmgr.exe
Creates:	C:\WINDOWS\system32\locator.vir C:\WINDOWS\system32\locator.exe
Creates:	C:\WINDOWS\system32\scardsvr.vir
Creates:	C:\WINDOWS\system32\scardsvr.exe
Creates:	C:\WINDOWS\system32\smlogsvc.vir
Creates:	C:\windows\system32\smlogsvc.exe
Creates:	C:\WINDOWS\system32\vssvc.vir
Creates:	C:\WINDOWS\system32\vssvc.exe C:\WINDOWS\system32\wbem\wmiapsrv.vir
creates.	C. MITINDONO (SYSTEMIOZ MIDEII (MILITAPO) V. VII

```
Creates:
                         C:\WINDOWS\system32\wbem\wmiapsrv.exe
                         C:\Program Files\Internet Explorer\iexplore.vir
 Creates:
 Creates:
                         C:\Program Files\Internet Explorer\iexplore.exe
 Creates:
                         C:\System Volume Information\catalog.wci\00010001.ci
 Creates:
                         C:\System Volume Information\catalog.wci\00010001.dir
 Creates:
                         C:\System Volume Information\catalog.wci\CiFLfffc.000
                         C:\System Volume Information\catalog.wci\CiFLfffc.001
 Creates:
                         C:\System Volume Information\catalog.wci\CiFLfffc.002
 Creates:
                         {\tt C:\WINDOWS\Prefetch\35644F3D0029F81C3D478D3C2407F-06C959F7.pf}\\
 Opens:
                         C:\Documents and Settings\Admin
 Opens:
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\pdh.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
                         C:\WINDOWS\system32\msasn1.dll
 Opens:
                         C:\WINDOWS\system32\odbc32.dll
                         C:\WINDOWS\system32\odbcbcp.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\imm32.dll
 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\shell32.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
 Opens:
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\WINDOWS\system32\odbcint.dll
 Opens:
                         C:\WINDOWS\system32\sfc_os.dll
 Opens:
                         C:\WINDOWS\system32\wintrust.dll
 Opens:
                         C:\WINDOWS\system32\pstorec.dll
 Opens:
                         C:\WINDOWS\system32\atl.dll
 Opens:
                         C:\WINDOWS\system32\crtdll.dll
 Opens:
                         C:\WINDOWS\system32\sfc.dll
 Opens:
                         C:\WINDOWS\system32\MSCTF.dll
 Opens:
                         C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
                         C:\windows\SysWOW64\svchost.exe
 Opens:
                         C:\windows\system32\svchost.exe
                         C:\WINDOWS\system32\svchost.exe
 Opens:
 Opens:
                         C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe
 Opens:
                         C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
                         C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.vir
 Opens:
 Opens:
                         C:\WINDOWS\Temp\27db9baa-dc60-425c-8aca-ef0ca60d7b54
 Opens:
                         C:\windows\SysWOW64\cisvc.exe
                         C:\WINDOWS\system32\cisvc.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\WINDOWS\system32\cisvc.vir
                         C:\WINDOWS\Prefetch\CISVC.EXE-21F69875.pf
 Opens:
 Opens:
                         C:\WINDOWS\system32\query.dll
 Opens:
                         C:\WINDOWS\system32\shimeng.dll
                         C:\WINDOWS\AppPatch\sysmain.sdb
 Opens:
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
                         C:\WINDOWS\AppPatch\AcGenral.dll
                         C:\WINDOWS\system32\winmm.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\msacm32.dll
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rpcss.dll
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
                         C:\WINDOWS\system32\ciadmin.dll
                         C:\WINDOWS\system32\ciadmin.dll.2.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\ciadmin.dll.2.Config
 Opens:
                         C:\WINDOWS\system32\ixsso.dll
                         C:\WINDOWS\system32\nlhtml.dll
 Opens:
 Opens:
                         C:\windows\SysWOW64\clipsrv.exe
 Opens:
                         C:\WINDOWS\system32\clipsrv.exe
 Opens:
                         C:\WINDOWS\system32\offfilt.dll
 Opens:
                         C:\WINDOWS\system32\clipsrv.vir
 Opens:
                         C:\WINDOWS\system32\ciodm.dll
 Opens:
                         C:\WINDOWS\system32\infosoft.dll
 Opens:
                         C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
 Opens:
                         C:\WINDOWS\system32\mimefilt.dll
 Opens:
                         C:\WINDOWS\system32\langwrbk.dll
 Opens:
                         C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.vir
                         C:\windows\SysWOW64\dllhost.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32\dllhost.exe
```

```
Opens:
                         C:\System Volume Information\catalog.wci
 Opens:
                         C:\
                         C:\windows\SysWOW64\dmadmin.exe
 Opens:
                         C:\WINDOWS\system32\dmadmin.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32\dmadmin.vir
 Opens:
                         C:\WINDOWS\system32\ntmarta.dll
 Opens:
                         C:\WINDOWS\system32\samlib.dll
                         C:\WINDOWS\Microsoft.NET\Framework\v3.0\WPF\PresentationFontCache.exe
 Opens:
 Opens:
                         C:\System Volume Information\catalog.wci\INDEX.001
                         C:\System Volume Information\catalog.wci\INDEX.002
 Opens:
 Opens:
                         C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication
Foundation\infocard.exe
 Opens:
                         C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication Foundation
                         C:\System Volume Information\catalog.wci\CiCL0001.000
 Opens:
 Opens:
                         C:\System Volume Information\catalog.wci\CiCL0001.001
                         C:\System Volume Information\catalog.wci\CiCL0001.002
 Opens:
                         C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication
 Opens:
Foundation\infocard.vir
 Opens:
                         C:\System Volume Information\catalog.wci\CiFLfffd.000
 Opens:
                         C:\System Volume Information\catalog.wci\CiFLfffd.001
 Opens:
                         C:\System Volume Information\catalog.wci\CiFLfffd.002
 Opens:
                         C:\System Volume Information\catalog.wci\CiSL0001.001
 Opens:
                         C:\System Volume Information\catalog.wci\CiSL0001.002
 Opens:
                         C:\System Volume Information\catalog.wci\CiSP0000.002
 Opens:
                         C:\System Volume Information\catalog.wci\CiSP0000.001
 Opens:
                         C:\System Volume Information\catalog.wci\CiP10000.001
 Opens:
                         C:\System Volume Information\catalog.wci\CiP20000.001
 Opens:
                         C:\System Volume Information\catalog.wci\CiPT0000.001
 Opens:
                         C:\System Volume Information\catalog.wci\CiST0000.001
 Opens:
                         C:\System Volume Information\catalog.wci\CiP10000.002
 Opens:
                         C:\system volume information\catalog.wci\00000001.ci
 Opens:
                         C:\system volume information\catalog.wci\0000001.hsh
 Opens:
                         C:\system volume information\catalog.wci\00000001.ps1
 Opens:
                         C:\system volume information\catalog.wci\0000001.ps2
 Opens:
                         C:\System Volume Information\catalog.wci\CiP20000.002
 Opens:
                         C:\System Volume Information\catalog.wci\CiVP0000.001
 Opens:
                         C:\windows\SysWOW64\imapi.exe
 Opens:
                         C:\WINDOWS\system32\imapi.exe
 Opens:
                         C:\WINDOWS\system32\imapi.vir
 Opens:
                         C:\System Volume Information\catalog.wci\00000001.ps1
 Opens:
                         C:\System Volume Information\catalog.wci\CiPT0000.002
 Opens:
                         C:\system volume information\catalog.wci\00000002.ci
 Opens:
                         C:\system volume information\catalog.wci\00000002.hsh
 Opens:
                         C:\system volume information\catalog.wci\00000002.ps1
 Opens:
                         C:\system volume information\catalog.wci\00000002.ps2
 Opens:
                         C:\System Volume Information\catalog.wci\00000001.ps2
                         C:\WINDOWS\system32\drprov.dll
 Opens:
 Opens:
                         C:\windows\SysWOW64\mnmsrvc.exe
                         C:\WINDOWS\system32\mnmsrvc.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32\ntlanman.dll
 Opens:
                         C:\WINDOWS\system32\netui0.dll
 Opens:
                         C:\WINDOWS\system32\netui1.dll
 Opens:
                         C:\WINDOWS\system32\netrap.dll
 Opens:
                         C:\WINDOWS\system32\davclnt.dll
 Opens:
                         C:\WINDOWS\system32\mnmsrvc.vir
 Opens:
                         C:\WINDOWS\system32\cidaemon.exe
 Opens:
                         C:\windows\SysWOW64\msdtc.exe
                         C:\WINDOWS\system32\msdtc.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
                         C:\windows\SysWOW64\msiexec.exe
 Opens:
                         C:\WINDOWS\system32\msiexec.exe
 Opens:
                         C:\WINDOWS\system32\cidaemon.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\CIDAEMON.EXE-27AE97A4.pf
 Opens:
                         C:\WINDOWS\system32\msiexec.vir
 Opens:
                         C:\windows\SysWOW64\netdde.exe
 Opens:
                         C:\WINDOWS\system32\netdde.exe
 Opens:
                         C:\Documents and Settings
 Opens:
                         C:\WINDOWS\system32\netdde.vir
 Opens:
                         C:\windows\SysWOW64\lsass.exe
 Opens:
                         C:\windows\system32\lsass.exe
 Opens:
                         C:\WINDOWS\system32\lsass.exe
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\Source Engine
 Opens:
                         C:\Program Files\Common Files\Microsoft Shared\Source Engine\ose.vir
 Opens:
                         C:\windows\SysWOW64\sessmgr.exe
                         C:\WINDOWS\system32\sessmgr.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32\sessmgr.vir
 Opens:
                         C:\Documents and Settings\Administrator
 Opens:
                         C:\Documents and Settings\All Users
 Opens:
                         C:\Documents and Settings\Default User
                         C:\Documents and Settings\LocalService
```

C:\windows\SvsWOW64\locator.exe

C:\WINDOWS\system32\locator.exe

Opens:

Opens: Opens:

```
Opens:
                         C:\WINDOWS\system32\locator.vir
                         C:\Documents and Settings\NetworkService\Application Data
 Opens:
 Opens:
                         C:\Documents and Settings\NetworkService\Cookies
 Opens:
                         C:\Documents and Settings\NetworkService\Local Settings
 Opens:
                         C:\Documents and Settings\NetworkService\NTUSER.DAT
 Opens:
                         C:\Documents and Settings\NetworkService\ntuser.dat.LOG
                         C:\Documents and Settings\NetworkService\ntuser.ini
 Opens:
                         {\tt C:\Documents\ and\ Settings\NetworkService\Local\ Settings\Application\ Data}
 Opens:
 Opens:
                         C:\Documents and Settings\NetworkService\Local Settings\desktop.ini
 Opens:
                         C:\Documents and Settings\NetworkService\Local Settings\History
 Opens:
                         C:\Documents and Settings\NetworkService\Local Settings\Temp
 Opens:
                         C:\Documents and Settings\NetworkService\Local Settings\Temporary
Internet Files
 Opens:
                         C:\Documents and Settings\NetworkService\Application Data\Microsoft
                         C:\Documents and Settings\LocalService\Application Data
 Opens:
                         C:\Documents and Settings\LocalService\Cookies
 Opens:
 Opens:
                         C:\Documents and Settings\LocalService\Local Settings
 Opens:
                         C:\Documents and Settings\LocalService\NTUSER.DAT
                         C:\Documents and Settings\LocalService\ntuser.dat.LOG
 Opens:
 Opens:
                         C:\Documents and Settings\LocalService\ntuser.ini
                         C:\Documents and Settings\LocalService\Local Settings\Application Data
 Opens:
 Opens:
                         C:\Documents and Settings\LocalService\Local Settings\desktop.ini
 Opens:
                         C:\Documents and Settings\LocalService\Local Settings\History
 Opens:
                         C:\Documents and Settings\LocalService\Local Settings\Temp
                         {\tt C:\Documents\ and\ Settings\backslash LocalService\backslash Local\ Settings\backslash Temporary\ Internet}
 Opens:
Files
 Opens:
                         C:\Documents and Settings\LocalService\Cookies\index.dat
                         C:\windows\SysWOW64\scardsvr.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32\scardsvr.exe
 Opens:
                         C:\Documents and Settings\LocalService\Application Data\Microsoft
 Opens:
                         C:\WINDOWS\system32\scardsvr.vir
 Opens:
                         C:\windows\SysWOW64\smlogsvc.exe
 Opens:
                         C:\WINDOWS\system32\smlogsvc.exe
 Opens:
                         C:\WINDOWS\system32\smlogsvc.vir
 Opens:
                         C:\windows\SysWOW64\ups.exe
 Opens:
                         C:\WINDOWS\system32\ups.exe
 Opens:
                         C:\windows\SysWOW64\vssvc.exe
 Opens:
                         C:\WINDOWS\system32\vssvc.exe
 Opens:
                         C:\Documents and Settings\Default User\Application Data
 Opens:
                         C:\Documents and Settings\Default User\Cookies
                         C:\documents and settings
 Opens:
 Opens:
                         C:\Documents and Settings\Default User\Desktop
 Opens:
                         C:\WINDOWS\system32\vssvc.vir
 Opens:
                         C:\Documents and Settings\Default User\Favorites
 Opens:
                         C:\Documents and Settings\Default User\Local Settings
                         C:\Documents and Settings\Default User\My Documents
 Opens:
 Opens:
                         C:\Documents and Settings\Default User\NetHood
 Opens:
                         C:\Documents and Settings\Default User\NTUSER.DAT
                         C:\Documents and Settings\Default User\NTUSER.DAT.LOG
 Opens:
 Opens:
                         C:\windows\SysWOW64\wbem\wmiapsrv.exe
 Opens:
                         C:\WINDOWS\system32\wbem\wmiapsrv.exe
 Opens:
                         C:\Documents and Settings\Default User\PrintHood
 Opens:
                         C:\WINDOWS\system32\wbem
 Opens:
                         C:\Documents and Settings\Default User\Recent
 Opens:
                         C:\WINDOWS\system32\wbem\wmiapsrv.vir
 Opens:
                         C:\Documents and Settings\Default User\SendTo
 Opens:
                         C:\Documents and Settings\Default User\Start Menu
 Opens:
                         C:\Documents and Settings\Default User\Templates
 Opens:
                         C:\System Volume Information\catalog.wci\CiST0000.002
 Opens:
                         C:\Documents and Settings\Default User\Templates\amipro.sam
 Opens:
                         C:\Documents and Settings\Default User\Templates\excel.xls
 Opens:
                         C:\Documents and Settings\Default User\Templates\excel4.xls
 Opens:
                         C:\Documents and Settings\Default User\Templates\lotus.wk4
 Opens:
                         C:\Documents and Settings\Default User\Templates\powerpnt.ppt
 Opens:
                         C:\Documents and Settings\Default User\Templates\presenta.shw
 Opens:
                         C:\Documents and Settings\Default User\Templates\quattro.wb2
                         C:\Documents and Settings\Default User\Templates\sndrec.wav
 Opens:
 Opens:
                         C:\AUTOEXEC.BAT\
 Opens:
                         C:\boot.ini\
                         C:\CONFIG.SYS\
 Opens:
 Opens:
                         C:\Documents and Settings\Default User\Templates\winword.doc
 Opens:
                         C:\documents and settings\admin
                         C:\Documents and Settings\Admin\Application Data
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Acrobat\9.0\AdobeCMapFnt09.1st\
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\AdobeSysFnt09.1st\
                         C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0\Forms
 Opens:
 Opens:
                         C:\Documents and Settings\Default User\Templates\winword2.doc
```

C:\Documents and Settings\NetworkService

```
C:\Documents and Settings\Default User\Templates\wordpfct.wpd
 Opens:
                         C:\Documents and Settings\Default User\Templates\wordpfct.wpg
 Opens:
                         C:\Documents and Settings\Default User\Start Menu\desktop.ini
 Opens:
                         C:\Documents and Settings\Default User\Start Menu\Programs
 Opens:
 Opens:
                         C:\documents and settings\administrator
 Opens:
                         C:\Documents and Settings\Default User\Start Menu\Programs\Accessories
                         C:\Documents and Settings\Default User\Start Menu\Programs\desktop.ini
 Opens:
                         C:\Documents and Settings\Default User\Start Menu\Programs\Remote
 Opens:
Assistance.lnk
                         C:\Documents and Settings\Default User\Start Menu\Programs\Startup
 Opens:
 Opens:
                         C:\Documents and Settings\Default User\Start Menu\Programs\Windows Media
Player.lnk
 Opens:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Startup\desktop.ini
 Opens:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Command Prompt.lnk
 Opens:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\desktop.ini
 Opens:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Entertainment
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Notepad.lnk
 Opens:
                         C:\documents and settings\all users
                         C:\documents and settings\default user
 Opens:
 Opens:
                         C:\documents and settings\localservice
 Opens:
                         C:\documents and settings\networkservice
 Opens:
                         C:\documents and settings\networkservice\application data
 Opens:
                         C:\documents and settings\networkservice\cookies
 Opens:
                         C:\documents and settings\networkservice\local settings
 Opens:
                         C:\WINDOWS\system32\noise.dat
 Opens:
                         C:\Documents and
Settings\NetworkService\ntuser.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C::{4c8cc155-6c1e-11d1-8e41-00c04fb9386d}:$DATA
 Opens:
 Opens:
                         C:: DocumentSummaryInformation:$DATA
 Opens:
                         C::Docf_ DocumentSummaryInformation:$DATA
                         C:\documents and settings\localservice\application data
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Acrobat\9.0\JavaScripts\glob.js\
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts\glob.settings.js\
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Program Compatibility Wizard.lnk
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Synchronize.lnk
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Tour Windows XP.lnk
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Windows Explorer.lnk
                         C:\documents and settings\localservice\local settings
 Opens:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
 Opens:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Accessibility\desktop.ini
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
 Opens:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
 Opens:
                         C:\Documents and
Settings\LocalService\ntuser.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Default User\SendTo\Compressed (zipped)
 Opens:
Folder.ZFSendToTarget
 Opens:
                         C:\documents and settings\localservice\cookies\index.dat
 Opens:
                         C:\Documents and Settings\Default User\SendTo\Desktop (create
shortcut).DeskLink
 Opens:
                         C:\Documents and Settings\Default User\SendTo\desktop.ini
                         C:\Documents and Settings\Default User\SendTo\Mail Recipient.MAPIMail
 Opens:
 Opens:
                         C:\documents and settings\default user\application data
                         C:\Documents and Settings\Default User\Local Settings\Application Data
 Opens:
 Opens:
                         C:\Documents and Settings\Default User\Local Settings\desktop.ini
 Opens:
                         C:\Documents and Settings\Default User\Local Settings\History
 Opens:
                         C:\Documents and Settings\Default User\Local Settings\Temp
                         C:\Documents and Settings\Default User\Local Settings\Temporary Internet
 Opens:
Files
```

```
C:\Documents and Settings\Default User\Application Data\desktop.ini
 Opens:
                         C:\Documents and Settings\Default User\Application Data\Microsoft
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application Data
 Opens:
                         C:\documents and settings\default user\cookies
 Opens:
                         C:\documents and settings\default user\desktop
                         C:\documents and settings\default user\favorites
 Opens:
                         C:\documents and settings\default user\local settings
 Opens:
 Opens:
                         C:\documents and settings\default user\my documents
                         C:\documents and settings\default user\nethood
 Opens:
 Opens:
                         C:\documents and settings\default user\printhood
 Opens:
                         C:\documents and settings\default user\recent
 Opens:
                         C:\documents and settings\default user\sendto
                         C:\documents and settings\default user\start menu
 Opens:
 Opens:
                         C:\documents and settings\default user\templates
                         C:\Documents and Settings\Default
 Opens:
User\Templates\amipro.sam: Raec25ph4sudbf0hAag5ehw3Nf:$DATA
 Opens:
                         C:\WINDOWS\system32\noise.enu
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\SharedDataEvents\
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\UserCache.bin\
 Opens:
                         C:\Documents and Settings\Default
User\Templates\excel4.xls: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Default
User\Templates\lotus.wk4: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Default
User\Templates\presenta.shw: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Default
User\Templates\quattro.wb2: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\WINDOWS\system32\verclsid.exe
                         C:\WINDOWS\system32\verclsid.exe.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\Prefetch\VERCLSID.EXE-3667BD89.pf
 Opens:
                         C:\WINDOWS
                         C:\WINDOWS\Registration
 Opens:
 Opens:
                         C:\WINDOWS\WinSxS
 Opens:
                         C:\WINDOWS\system32\ntdll.dll
 Opens:
                         C:\WINDOWS\system32\kernel32.dll
 Opens:
                         C:\WINDOWS\system32\unicode.nls
 Opens:
                         C:\WINDOWS\system32\locale.nls
                         C:\WINDOWS\system32\sorttbls.nls
 Opens:
 Opens:
                         C:\WINDOWS\system32\ole32.dll
 Opens:
                         C:\WINDOWS\system32\advapi32.dll
                         C:\WINDOWS\system32\rpcrt4.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\secur32.dll
 Opens:
                         C:\WINDOWS\system32\gdi32.dll
 Opens:
                         C:\WINDOWS\system32\user32.dll
 Opens:
                         C:\WINDOWS\system32\msvcrt.dll
 Opens:
                         C:\WINDOWS\system32\ctype.nls
 Opens:
                         C:\WINDOWS\system32\sortkey.nls
 Opens:
                         C:\WINDOWS\system32\oleaut32.dll
 Opens:
                         C:\WINDOWS\system32\version.dll
 Opens:
                         C:\WINDOWS\system32\shlwapi.dll
 Opens:
                         C:\WINDOWS\system32\shdocvw.dll
 Opens:
                         C:\WINDOWS\system32\cryptui.dll
 Opens:
                         C:\WINDOWS\system32\wininet.dll
 Opens:
                         C:\WINDOWS\system32\imagehlp.dll
 Opens:
                         C:\WINDOWS\system32\wldap32.dll
                         C:\WINDOWS\system32\riched20.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\userenv.dll
 Opens:
                         C:\Documents and Settings\All Users\Desktop
 Opens:
                         C:\Documents and Settings\All Users\Documents
 Opens:
                         C:\Documents and Settings\All Users\DRM
 Opens:
                         C:\Documents and Settings\All Users\Favorites
                         C:\Documents and Settings\All Users\ntuser.pol
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Start Menu
 Opens:
                         C:\Documents and Settings\All Users\Templates
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Set Program Access and
Defaults.lnk
                         C:\Documents and Settings\All Users\Start Menu\Windows Catalog.lnk
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Windows Update.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Accessories
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Adobe Reader
9.1nk
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office
Excel Viewer.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office
```

C:\Documents and Settings\Default User\Cookies\index.dat

```
Word Viewer 2003.1nk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft
 Opens:
PowerPoint Viewer .lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\MSN.lnk
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Startup
                         C:\Documents and Settings\All Users\Start Menu\Programs\Windows
 Opens:
Messenger.lnk
 Opens:
                         C:\WINDOWS\system32\shmedia.dll
                         C:\Documents and Settings\All Users\Start Menu\Programs\Windows Movie
 Opens:
Maker.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Startup\desktop.ini
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\IDLE
 Opens:
(Python GUI).lnk
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Module Docs.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python (command line).lnk
 Opens:
                         C:\WINDOWS\system32\msvfw32.dll
 Opens:
                         C:\WINDOWS\system32\avifil32.dll
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python for Windows Documentation.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python Manuals.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python
 Opens:
2.7\PythonWin.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python
 Opens:
2.7\Uninstall Python.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Games\desktop.ini
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Games\Freecell.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Hearts.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
 Opens:
Backgammon.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Checkers.lnk
 Opens:
                         C:\WINDOWS\system32\verclsid.exe.124.Manifest
 Opens:
                         C:\Documents and Settings\Default
User\Templates\winword2.doc: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Default
 Opens:
User\Templates\wordpfct.wpd: Raec25ph4sudbf0hAag5ehw3Nf:$DATA
                         C:\Documents and Settings\Default
 Opens:
User\Templates\wordpfct.wpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\documents and settings\default user\start menu\programs
                         C:\documents and settings\default user\start menu\programs\accessories
 Opens:
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\WINDOWS\system32\winlogon.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32\xpsp2res.dll
 Opens:
                         C:\WINDOWS\system32\linkinfo.dll
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Flash Player
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Flash
Player\AssetCache
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Adobe\Flash
Player\AssetCache\7PLTA3CP
 Opens:
                         C:\WINDOWS\system32\ntshrui.dll
 Opens:
                         C:\WINDOWS\system32\ntshrui.dll.123.Manifest
                         C:\WINDOWS\system32\ntshrui.dll.123.Config
 Opens:
 Opens:
                         C:\Documents and Settings\Default User\Start Menu\Programs\Remote
Assistance.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\documents and settings\default user\start menu\programs\startup
 Opens:
 Opens:
                         C:\Documents and Settings\Default User\Start Menu\Programs\Windows Media
Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Startup\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\documents and settings\default user\start
 Opens:
menu\programs\accessories\accessibility
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Command Prompt.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\documents and settings\default user\start
menu\programs\accessories\entertainment
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Notepad.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Config
```

```
C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Program Compatibility Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Hearts.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Reversi.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
 Opens:
Spades.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Minesweeper.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Pinball.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Solitaire.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Spider
 Opens:
Solitaire.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Component Services.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Opens:
Tools\Computer Management.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Opens:
Tools\Data Sources (ODBC).lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Opens:
Tools\desktop.ini
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Opens:
Tools\Event Viewer.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Opens:
Tools\Local Security Policy.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Opens:
Tools\Performance.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Opens:
Tools\Services.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Accessibility
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Calculator.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications
                         C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Synchronize.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\Paint.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Remote Desktop Connection.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\WordPad.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Svstem Tools\Activate Windows.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Backup.lnk
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\System Tools\Character Map.lnk
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Tour Windows XP.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\desktop.ini
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\System Tools\Disk Cleanup.lnk
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Disk Defragmenter.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Files and Settings Transfer Wizard.lnk
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\System Tools\Scheduled Tasks.lnk
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Security Center.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\System Information.lnk
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\System Tools\System Restore.lnk
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\Sound Recorder.lnk
                         C:\Documents and Settings\All Users\Start
 Opens:
```

Menu\Programs\Accessories\Entertainment\Volume Control.lnk

```
C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Windows Explorer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\Communications\desktop.ini
 Opens:
                        C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\HyperTerminal.lnk
                        C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Entertainment\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Entertainment\Windows Media
Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Accessibility\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Default User\Start
 Opens:
C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Accessibility\Narrator.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                        C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Default User\Start
 Opens:
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Default User\SendTo\Compressed (zipped)
 Opens:
Folder.ZFSendToTarget: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                        C:\Documents and Settings\All Users\Start Menu\Set Program Access and
Defaults.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\All Users\Start Menu\Windows
 Opens:
Catalog.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\All Users\Start Menu\Windows
 Opens:
Update.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                        C:\documents and settings\all users\start menu\programs\accessories
 Opens:
                        C:\documents and settings\all users\start menu\programs\administrative
tools
 Opens:
                        C:\WINDOWS\Installer
 Opens:
                        C:\WINDOWS\Installer\{AC76BA86-7AD7-1033-7B44-A93000000001}
                        C:\Documents and Settings\All Users\Documents\desktop.ini
 Opens:
 Opens:
                        C:\Documents and Settings\All Users\Start Menu\Programs\Adobe Reader
9.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                        C:\documents and settings\all users\start menu\programs\games
                        C:\WINDOWS\Installer\{95120000-003F-0409-0000-0000000FF1CE}
 Opens:
 Opens:
                        C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office
Excel Viewer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\WINDOWS\Installer\{90850409-6000-11D3-8CFE-0150048383C9}
 Opens:
                        C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office
 Opens:
Word Viewer 2003.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\WINDOWS\Installer\{95140000-00AF-0409-0000-0000000FF1CE}
 Opens:
 Opens:
                        C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft
PowerPoint Viewer .lnk: Raec25ph4sudbf0hAag5ehw3Nf:$DATA
                        C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\MSN.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                        C:\documents and settings\all users\start menu\programs\python 2.7
                        C:\documents and settings\all users\start menu\programs\startup
 Opens:
 Opens:
                        C:\Documents and Settings\All Users\Start Menu\Programs\Windows
Messenger.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\All Users\Start Menu\Programs\Windows Movie
 Opens:
Maker.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Startup\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                        C:\WINDOWS\Installer\{C3CC4DF5-39A5-4027-B136-2B3E1F5AB6E2}
 Opens:
                        C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\IDLE
(Python GUI).lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Module Docs.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python (command line).lnk: Raec25ph4sudbf0hAag5ehw3Nf:$DATA
 Opens:
                        C:\Documents and Settings\Admin\Application Data\Adobe\Linguistics
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Linguistics\Dictionaries
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\all
                        C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\Communications\Network Connections.lnk
                        C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\Communications\Network Setup Wizard.lnk
                        C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\New Connection Wizard.lnk
 Opens:
                        C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Wireless Network Setup Wizard.lnk
                        C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\Accessibility\Accessibility Wizard.lnk
```

```
Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\DRM\drmv2.lic
                         C:\Documents and Settings\All Users\DRM\drmv2.sst
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Pictures
                         C:\Documents and Settings\All Users\Documents\My Videos
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Videos\Desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Pictures\Desktop.ini
                         C:\Documents and Settings\All Users\Documents\My Pictures\Sample
 Opens:
Pictures
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python for Windows Documentation.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python
 Opens:
2.7\Python Manuals.lnk:
                        Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Blue hills.jpg
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\desktop.ini
                         {\tt C:\Documents\ and\ Settings\All\ Users\Documents\My\ Pictures\Sample}
 Opens:
Pictures\Sunset.jpg
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Water lilies.jpg
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Winter.jpg
                         C:\Documents and Settings\All Users\Documents\My Music\Desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\My Playlists
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample Music
                         C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst1.wpl
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst10.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst11.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst12.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst13.wpl
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\PythonWin.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python
 Opens:
2.7\Uninstall Python.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Games\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Freecell.lnk: Raec25ph4sudbf0hAag5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Hearts.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Backgammon.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Checkers.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Hearts.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
 Opens:
Reversi.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Spades.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         {\tt C:\Documents\ and\ Settings\All\ Users\Start}
 Opens:
Menu\Programs\Games\Minesweeper.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Games\Pinball.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\brt
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Solitaire.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Spider
 Opens:
Solitaire.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Component Services.lnk: Raec25ph4sudbf0hAag5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Computer Management.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Opens:
Tools\Data Sources (ODBC).lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Opens:
Tools\Event Viewer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Opens:
Tools\Local Security Policy.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
```

```
C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Opens:
Tools\Performance.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Services.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\documents and settings\all users\start
 Opens:
menu\programs\accessories\accessibility
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Calculator.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\documents and settings\all users\start
menu\programs\accessories\communications
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\documents and settings\all users\start
menu\programs\accessories\entertainment
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Paint.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Remote Desktop Connection.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\documents and settings\all users\start
menu\programs\accessories\system tools
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\WordPad.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst14.wpl
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst15.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst2.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst3.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst4.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst5.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst6.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst7.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst8.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst9.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Music\Beethoven's Symphony No. 9 (Scherzo).wma
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Music\desktop.ini
                         C:\Documents and Settings\All Users\Documents\My Music\Sample Music\New
 Opens:
Stories (Highway Blues).wma
                         C:\Documents and Settings\All Users\Desktop\Adobe Reader 9.lnk
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Adobe
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application Data\desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Microsoft
 Opens:
                         C:\Documents and Settings\All Users\Application Data\Sun
                         C:\Documents and Settings\Administrator\Application Data
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Cookies
 Opens:
                         C:\Documents and Settings\Administrator\Desktop
                         C:\Documents and Settings\Administrator\Favorites
 Opens:
                         C:\Documents and Settings\Administrator\Local Settings
 Opens:
 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
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\System Tools\Activate Windows.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Administrator\SendTo
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu
                         C:\Documents and Settings\Administrator\Templates
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\can
 Opens:
                         {\tt C:\Documents\ and\ Settings\Administrator\Templates\amipro.sam}
 Opens:
                         C:\Documents and Settings\Administrator\Templates\excel.xls
 Opens:
                         C:\Documents and Settings\Administrator\Templates\excel4.xls
                         {\tt C:\Documents\ and\ Settings\Administrator\Templates\lotus.wk4}
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Templates\powerpnt.ppt
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\System Tools\Backup.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Character Map.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\System Tools\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
```

```
C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\System Tools\Disk Cleanup.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Disk Defragmenter.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                        C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Files and Settings Transfer
Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\All Users\Start
 Opens:
C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\System Tools\Security Center.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\System Information.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\System Tools\System Restore.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Default User\SendTo\Desktop (create
 Opens:
shortcut).DeskLink: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Default
User\SendTo\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Default User\SendTo\Mail
 Opens:
Recipient.MAPIMail: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Default
 Opens:
User\Cookies\index.dat: Raec25ph4sudbf0hAag5ehw3Nf:$DATA
 Opens:
                         C:\documents and settings\all users\application data
 Opens:
                         C:\documents and settings\all users\desktop
 Opens:
                         C:\documents and settings\all users\documents
 Opens:
                         C:\documents and settings\all users\drm
 Opens:
                         C:\documents and settings\all users\favorites
                         C:\Documents and Settings\All
 Opens:
Users\ntuser.pol: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\documents and settings\all users\start menu
 Opens:
                         C:\documents and settings\all users\templates
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\eng
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\Entertainment\Sound Recorder.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\documents and settings\all users\documents\my videos
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Templates\presenta.shw
 Opens:
                         C:\Documents and Settings\Administrator\Templates\quattro.wb2
                         C:\Documents and Settings\Administrator\Templates\sndrec.wav
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Templates\winword.doc
 Opens:
                         C:\Documents and Settings\Administrator\Templates\winword2.doc
                         {\tt C:\Documents\ and\ Settings\Administrator\Templates\wordpfct.wpd}
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Templates\wordpfct.wpg
                         C:\Documents and Settings\Administrator\Start Menu\desktop.ini
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu\Programs
 Opens:
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu\Programs\Remote
Assistance.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start Menu\Programs\Startup
                         C:\Documents and Settings\Administrator\Start Menu\Programs\Windows
 Opens:
Media Player.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Startup\desktop.ini
                         C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Accessibility
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Command Prompt.lnk
                         C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\desktop.ini
                         C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Entertainment
                         C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Notepad.lnk
                         C:\Documents and Settings\All Users\Documents\My
 Opens:
Videos\Desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Program Compatibility Wizard.lnk
                         C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Synchronize.lnk
                         C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Tour Windows XP.lnk
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Windows Explorer.lnk
 Opens:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
                         C:\Documents and Settings\Administrator\Start
 Opens:
```

Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk

```
Opens:
                                    C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
                                    C:\Documents and Settings\Administrator\Start
  Opens:
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
                                    C:\Documents and Settings\Administrator\Start
  Opens:
Menu\Programs\Accessories\Accessibility\Narrator.lnk
  Opens:
                                    C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
  Opens:
                                    C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
                                    C:\Documents and Settings\Administrator\SendTo\Compressed (zipped)
  Opens:
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
                                    C:\Documents and Settings\All Users\Documents\My
  Opens:
Pictures\Desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                   C:\documents and settings\all users\documents\my pictures\sample
pictures
  Opens:
                                    C:\WINDOWS\system32\shimgvw.dll
  Opens:
C: \verb|WINDOWS| \verb|WinSxS| x86_Microsoft. \verb|Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c| and the second s
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-
ww_dfb54e0c\GdiPlus.dll
  Opens:
                                    C:\Documents and Settings\Administrator\Local Settings\Application Data
  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\Temp
  Opens:
                                    C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files
  Opens:
                                    C:\Documents and Settings\Administrator\Cookies\index.dat
  Opens:
                                    C:\Documents and Settings\Administrator\Application Data\desktop.ini
                                    C:\Documents and Settings\Administrator\Application Data\Microsoft
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\Cookies
  Opens:
                                    C:\Documents and Settings\Admin\Desktop
  Opens:
                                    C:\Documents and Settings\Admin\Favorites
  Opens:
                                    C:\Documents and Settings\Admin\IECompatCache
  Opens:
                                    C:\Documents and Settings\Admin\IETldCache
                                    C:\Documents and Settings\Admin\Local Settings
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\My Documents
  Opens:
                                    C:\Documents and Settings\Admin\NetHood
                                    C:\Documents and Settings\Admin\NTUSER.DAT
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\NTUSER.DAT.LOG
  Opens:
                                    C:\Documents and Settings\Admin\ntuser.ini
                                    C:\Documents and Settings\Admin\PrintHood
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\PrivacIE
                                    C:\Documents and Settings\Admin\Recent
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\SendTo
                                    C:\Documents and Settings\All Users\Documents\My Pictures\Sample
  Opens:
Pictures\Blue hills.jpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                    C:\Documents and Settings\Admin\Start Menu
                                    C:\Documents and Settings\Admin\Templates
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\Templates\amipro.sam
  Opens:
                                    C:\Documents and Settings\Admin\Templates\excel.xls
  Opens:
                                    C:\Documents and Settings\Admin\Templates\excel4.xls
  Opens:
                                    C:\Documents and Settings\Admin\Application Data\Adobe\LogTransport2
                                    C:\Documents and Settings\Admin\Application
  Opens:
Data\Adobe\LogTransport2\Logs
  Opens:
                                   C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                    C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Sunset.jpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                    C:\Documents and Settings\All Users\Documents\My Pictures\Sample
  Opens:
Pictures\Water lilies.jpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                    C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Winter.jpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                    C:\Documents and Settings\All Users\Documents\My
Music\Desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                    C:\documents and settings\all users\documents\my music\my playlists
  Opens:
  Opens:
                                    C:\documents and settings\all users\documents\my music\sample music
  Opens:
                                    C:\documents and settings\all users\documents\my music\sample playlists
  Opens:
                                    C:\documents and settings\all users\documents\my music\sample
playlists\000c5a7a
                                    C:\Documents and Settings\All Users\Documents\My Music\Sample
  Opens:
Playlists\000C5A7A\Plylst1.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                    C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst10.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                    C:\Documents and Settings\All Users\Documents\My Music\Sample
  Opens:
Playlists\000C5A7A\Plylst11.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                    C:\Documents and Settings\All Users\Documents\My Music\Sample
  Opens:
Playlists\000C5A7A\Plylst12.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
```

```
C:\Documents and Settings\Admin\Templates\lotus.wk4
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst13.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Templates\powerpnt.ppt
 Opens:
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Templates\presenta.shw}
 Opens:
                         C:\Documents and Settings\Admin\Templates\quattro.wb2
                         C:\Documents and Settings\Admin\Templates\sndrec.wav
 Opens:
                         C:\Documents and Settings\Admin\Templates\winword.doc
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Templates\winword2.doc
                         C:\Documents and Settings\Admin\Templates\wordpfct.wpd
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Templates\wordpfct.wpg
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
                         C:\Documents and Settings\Admin\Start Menu\Programs\Internet
 Opens:
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\Windows Media
Player.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Startup\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Address
Book.lnk
                         {\tt C:\Documents\ and\ Settings\Admin\Start\ Menu\Programs\Accessories\Command}
 Opens:
Prompt.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\desktop.ini
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment
 Opens:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Notepad.lnk
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Program
 Opens:
Compatibility Wizard.lnk
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Synchronize.lnk
                         {\tt C:\Documents\ and\ Settings\Admin\Start\ Menu\Programs\Accessories\System}
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst14.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Application Data\desktop.ini\
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Identities
 Opens:
                         Opens:
1E8B-4ECF-8560-0E560368800D}
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Playlists\000C5A7A\Plylst15.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Application Data\Macromedia
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst2.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
Player\macromedia.com\support
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
 Opens:
Player\macromedia.com\support\flashplayer\sys
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Opens:
Player\macromedia.com\support\flashplayer\sys\settings.sol\
 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\Accessories\System
Tools\Internet Explorer (No Add-ons).lnk
 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
                         C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\Accessibility\desktop.ini
                         C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
 Opens:
                         C:\Documents and Settings\Admin\Start
```

```
Menu\Programs\Accessories\Accessibility\Narrator.lnk
                                  C:\Documents and Settings\All Users\Documents\My Music\Sample
  Opens:
Playlists\000C5A7A\Plylst3.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                   C:\Documents and Settings\Admin\Application Data\Microsoft
  Opens:
  Opens:
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\AddIns
  Opens:
                                   C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst4.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                  C:\Documents and Settings\Admin\Application Data\Microsoft\Credentials
  Opens:
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-1003
  Opens:
                                   C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst5.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                   C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst6.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache
                                   C:\Documents and Settings\Admin\Application
  Opens:
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\
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004\
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\3130B1871A126520A8C47861EFE3ED4D\
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\60E31627FDA0A46932B0E5948949F2A5\
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\62B5AF9BE9ADC1085C3C56EC07A82BF6\
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D49D759AD\
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\7396C420A8E1BC1DA97F1AF0D10BAD21\
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE8E7EB5F575EC9\
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\8DFDF057024880D7A081AFBF6D26B92F\
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015\
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\Content\A44F4E7CB3133FF765C39A53AD8FCFDD\
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\F482C95F83F1B59228F1B1E720F2EDF1\
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\MetaData
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\0797C381B2F87EB5A1D5573BD15BA4F4\
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\135BD6A358680A7BF1CCEC7C0172393D\
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497DD56F57004\
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\3130B1871A126520A8C47861EFE3ED4D\
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\60E31627FDA0A46932B0E5948949F2A5\
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\62B5AF9BE9ADC1085C3C56EC07A82BF6\
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD\
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7396C420A8E1BC1DA97F1AF0D10BAD21\
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7B2238AACCEDC3F1FFE8E7EB5F575EC9\
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\CryptnetUrlCache\MetaData\8DFDF057024880D7A081AFBF6D26B92F\
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015\
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\A44F4E7CB3133FF765C39A53AD8FCFDD\
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\F482C95F83F1B59228F1B1E720F2EDF1\
  Opens:
                                   C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst7.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                   C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst8.wpl: Raec25ph4sudbf0hAag5ehw3Nf:$DATA
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto
  Opens:
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA
  Opens:
  Opens:
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
1-5-21-1757981266-507921405-1957994488-1003
  Opens:
                                   {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Crypto\RSA\S-lines C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Crypto\RSA\S-lines C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Crypto\RSA\S-lines C:\Documents\ Admin\Application\ Data\Microsoft\Crypto\Application\ Data\Microsoft\Application\ Data\Microsoft\Application\Application\ Data\Microsoft\Application\Application\ Data\Microsoft\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application\Application
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\
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst9.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
 Opens:
Explorer\brndlog.bak\
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\brndlog.txt\
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Desktop.htt\
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Internet}
 Opens:
Explorer\Quick Launch
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\desktop.ini\
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Opens:
Music\Beethoven's Symphony No. 9 (Scherzo).wma: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Program Files\Internet Explorer
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
Music\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample Music\New
Stories (Highway Blues).wma: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.vir
 Opens:
                         C:\Documents and Settings\All Users\Desktop\Adobe Reader
9.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\documents and settings\administrator\application data
 Opens:
                         C:\documents and settings\administrator\cookies
                         C:\documents and settings\administrator\desktop
 Opens:
 Opens:
                         C:\documents and settings\administrator\favorites
 Opens:
                         C:\documents and settings\administrator\local settings
                         C:\documents and settings\administrator\my documents
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk\
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
 Opens:
Explorer\Quick Launch\Show Desktop.scf\
                         C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
                         {\tt C:\Documents\ and\ Settings\Admin\SendTo\Compressed\ (zipped)}\\
 Opens:
Folder.ZFSendToTarget
 Opens:
                         C:\Documents and Settings\Admin\SendTo\Desktop (create
shortcut).DeskLink
 Opens:
                         C:\Documents and Settings\Admin\SendTo\desktop.ini
                         C:\Documents and Settings\Admin\SendTo\Mail Recipient.MAPIMail
 Opens:
                         C:\Documents and Settings\Admin\SendTo\My Documents.mydocs
 Opens:
 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\PrivacIE\index.dat
 Opens:
                         C:\Documents and Settings\Admin\My Documents\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\My Documents\My Music
                         C:\Documents and Settings\Admin\My Documents\My Pictures
 Opens:
 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\My Documents\My Music\Desktop.ini
                         C:\Documents and Settings\Admin\My Documents\My Music\Sample Music.lnk
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application\ Data}
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History
                         C:\Documents and Settings\Admin\Local Settings\Temp
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
                         C:\Documents and Settings\Admin\IETldCache\index.dat
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\IECompatCache\index.dat}\\
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Links
 Opens:
                         C:\documents and settings\administrator\nethood
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Media Player
 Opens:
                         C:\Documents and
Settings\Administrator\ntuser.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\MMC
                         C:\documents and settings\administrator\printhood
 Opens:
 Opens:
                         C:\documents and settings\administrator\recent
 Opens:
                         C:\documents and settings\administrator\sendto
 Opens:
                         C:\documents and settings\administrator\start menu
 Opens:
                         C:\documents and settings\administrator\templates
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Office
                         C:\Documents and Settings\Admin\Application
 Opens:
```

Data\Microsoft\Office\Excel12.pip\

```
C:\Documents and Settings\Admin\Application Data\Microsoft\Office\Recent
  Opens:
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\Office\Recent\Desktop.ini\
                                   C:\Documents and
Settings\Administrator\Templates\amipro.sam: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Protect
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\Protect\CREDHIST\
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
  Opens:
5-21-1757981266-507921405-1957994488-1003
  Opens:
                                   {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Protect\S-1-Barbarana Constraints}. \\
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\
                                   {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\ Data\Microsoft\Protect\S-1-Relation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\Barrelation\
  Opens:
5-21-1757981266-507921405-1957994488-1003\Preferred\
  Opens:
                                   C:\documents and settings\administrator\start menu\programs\startup
  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\
                                   C:\Documents and Settings\Administrator\Start Menu\Programs\Windows
  Opens:
Media Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                   C:\Documents and Settings\Administrator\Start
  Opens:
Menu\Programs\Startup\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                   C:\documents and settings\administrator\start
menu\programs\accessories\accessibility
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\SystemCertificates
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My
                                   C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\Certificates
                                   C:\Documents and Settings\Administrator\Start
  Opens:
Menu\Programs\Accessories\Command Prompt.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\SystemCertificates\My\CRLs
                                   C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                   {\tt C:\documents\ and\ settings\administrator\start}
  Opens:
menu\programs\accessories\entertainment
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\SystemCertificates\My\CTLs
                                   C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Notepad.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                   C:\Documents and Settings\Administrator\Start
  Opens:
Menu\Programs\Accessories\Program Compatibility Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Templates
  Opens:
                                   {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Windows}
  Opens:
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\Windows\Themes
                                   C:\Documents and Settings\Admin\Application
  Opens:
Data\Microsoft\Windows\Themes\Custom.theme\
                                   C:\Documents and Settings\Administrator\Start
  Opens:
Menu\Programs\Accessories\Synchronize.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                   C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Tour Windows XP.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                   C:\Documents and Settings\Admin\Application Data\Oracle
  Opens:
                                   C:\Documents and Settings\Admin\Application Data\Oracle\Java
  Opens:
                                   C:\Documents and Settings\Admin\Application Data\Oracle\Java\Uninstall
                                   C:\Documents and Settings\Admin\Application Data\Sun
  Opens:
  Opens:
                                   C:\Documents and Settings\Admin\Application Data\Sun\Java
  Opens:
                                   C:\Documents and Settings\Admin\Application Data\Sun\Java\AU
                                   Opens:
  Opens:
                                   C:\Documents and Settings\Admin\Application Data\Sun\Java\AU\au.msi\
                                   C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment
  Opens:
  Opens:
                                   C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Windows Explorer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                   C:\Documents and Settings\Admin\Favorites\Microsoft Websites
  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\Application
Data\Sun\Java\Deployment\cache
                                   C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0
  Opens:
                                   C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\0
  Opens:
                                   C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE Add-on
```

site.url

```
Opens:
                        C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE site on
Microsoft.com.url
 Opens:
                        C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Home.url
                        C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
 Opens:
At Work.url
 Opens:
                        C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
Store.url
 Opens:
                        C:\Documents and Settings\Admin\Favorites\Links\desktop.ini
 Opens:
                        C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\1
 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\Cookies\admin@c1.microsoft[2].txt
 Opens:
                        C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt
 Opens:
                        C:\Documents and Settings\Admin\Cookies\admin@rto.microsoft[11.txt
 Opens:
                        C: \verb|\Documents| and Settings\\| Admin\\| Cookies\\| admin\\| @search.microsoft[1].txt
 Opens:
                        C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt
                        C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[3].txt
 Opens:
                        C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Entertainment\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        {\tt C:\Documents\ and\ Settings\Admin\Application}
 Opens:
Data\Sun\Java\Deployment\cache\6.0\10
                        C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
 Opens:
                        C:\Documents and Settings\Admin\Application Data\desktop.ini
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\11
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\12
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171\
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\12\eef218c-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
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\17
 Opens:
                        C:\Documents and Settings\Admin\Application
Opens:
                        C:\Documents and Settings\Admin\Application
C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\17\49a00451-6.0.lap\
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\18
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1\
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1.idx\
 Opens:
                        C:\Documents and Settings\Admin\Application
Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\2
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\20
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\21
                        C:\Documents and Settings\Administrator\Start
 Opens:
Menu\Programs\Accessories\Entertainment\Windows Media
Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\22
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\23
 Opens:
                        C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\24
                        C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\25
 Opens:
                        C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Magnifier.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Admin\Application
 Opens:
```

Data\Sun\Java\Deployment\cache\6.0\26

```
Opens:
                                     C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\27
  Opens:
                                     C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                     C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\28
  Opens:
                                     C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\29
  Opens:
                                     C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\3
                                     C:\Documents and Settings\Administrator\Start
  Opens:
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                     C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\30
  Opens:
                                     C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\31
                                     C:\Documents and Settings\Administrator\Start
  Opens:
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                     C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\32
                                     C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\33
                                     C:\Documents and Settings\Administrator\SendTo\Compressed (zipped)
  Opens:
Folder.ZFSendToTarget: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                     C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\34
                                     C:\Documents and Settings\Administrator\SendTo\Desktop (create
  Opens:
shortcut).DeskLink: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                     C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\35
                                     C:\Documents and
  Opens:
Settings\Administrator\SendTo\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                     C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\36
                                     C:\Documents and Settings\Administrator\SendTo\Mail
  Opens:
Recipient.MAPIMail: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                     C:\Documents and Settings\Admin\Application
  Opens:
C:\Documents and
Settings\Administrator\Cookies\index.dat: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                     C:\documents and settings\admin\application data
                                     C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\38
                                     C:\documents and settings\admin\desktop
  Opens:
  Opens:
                                     C:\documents and settings\admin\favorites
  Opens:
                                     C:\documents and settings\admin\local settings
  Opens:
                                     C:\documents and settings\admin\my documents
  Opens:
                                     C:\documents and settings\admin\nethood
  Opens:
                                     C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\39
                                     C:\Documents and
Settings\Admin\ntuser.ini: Raec25ph4sudbf0hAag5ehw3Nf:$DATA
  Opens:
                                     C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\4
  Opens:
                                     C:\documents and settings\admin\printhood
  Opens:
                                     C:\documents and settings\admin\recent
                                     C:\documents and settings\admin\sendto
  Opens:
                                     C:\documents and settings\admin\start menu
  Opens:
  Opens:
                                     C:\documents and settings\admin\templates
                                     C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\40
  Opens:
                                     C:\Documents and
Settings\Admin\Templates\amipro.sam: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                     C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\41
                                     C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\42
                                     C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\43
                                     C:\Documents and Settings\Admin\Application
  Opens:
C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d.idx\
  Opens:
                                     C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\44
  Opens:
                                     C:\Documents and
Settings \verb| Admin \verb| Templates \verb| excel4.xls: Raec25ph4sudbf0hAaq5ehw3Nf: $DATA | Admin \verb| Templates \verb| excel4.xls: Raec25ph4sudbf0hAaq5ehw3Nf: $DATA | Admin $ATA$ | Admin $
                                     C:\Documents and Settings\Admin\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\45
  Opens:
                                     C:\Documents and
Settings\Admin\Templates\lotus.wk4: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                     C:\Documents and Settings\Admin\Application
  Opens:
```

Data\Sun\Java\Deployment\cache\6.0\46

```
Opens:
                                            C:\boot.ini
                                            C:\CONFIG.SYS
   Opens:
   Opens:
                                            C:\dump.pcap
   Opens:
                                            C:\exception.log
   Opens:
                                            C:\IO.SYS
                                            C:\MSDOS.SYS
   Opens:
                                            C:\NTDETECT.COM
   Opens:
   Opens:
                                            C:\ntldr
   Opens:
                                            C:\pagefile.sys
   Opens:
                                            C:\Program Files
   Opens:
                                            C:\static_events.gpb
   Opens:
                                            C:\System Volume Information
                                            C:\WINDOWS\0.log
   Opens:
   Opens:
                                            C:\WINDOWS\addins
                                            C:\WINDOWS\AppPatch
   Opens:
                                            C:\WINDOWS\assembly
   Opens:
   Opens:
                                            C:\WINDOWS\Blue Lace 16.bmp
   Opens:
                                            C:\WINDOWS\bootstat.dat
   Opens:
                                            C:\WINDOWS\clock.avi
   Opens:
                                            C:\WINDOWS\cmsetacl.log
   Opens:
                                            C:\WINDOWS\Coffee Bean.bmp
   Opens:
                                            C:\WINDOWS\comsetup.log
   Opens:
                                            C:\WINDOWS\Config
   Opens:
                                            C:\WINDOWS\Connection Wizard
   Opens:
                                            C:\WINDOWS\control.ini
   Opens:
                                            C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\47
                                            C:\WINDOWS\CSC
   Opens:
   Opens:
                                            C:\WINDOWS\Cursors
   Opens:
                                            C:\WINDOWS\Debug
   Opens:
                                            C:\WINDOWS\desktop.ini
   Opens:
                                            C:\WINDOWS\Downloaded Program Files
   Opens:
                                            C:\WINDOWS\Driver Cache
                                            C:\WINDOWS\DtcInstall.log
   Opens:
   Opens:
                                            C:\WINDOWS\ehome
   Opens:
                                            C:\WINDOWS\explorer.exe
   Opens:
                                            C:\WINDOWS\explorer.scf
   Opens:
                                            C:\WINDOWS\FaxSetup.log
   Opens:
                                            C:\WINDOWS\FeatherTexture.bmp
                                            {\tt C:\Documents\ and\ Settings\Admin\Application}
   Opens:
Data\Sun\Java\Deployment\cache\6.0\48
                                            C:\WINDOWS\Fonts
   Opens:
                                            C:\WINDOWS\Gone Fishing.bmp
   Opens:
   Opens:
                                            C:\WINDOWS\Greenstone.bmp
   Opens:
                                            C:\WINDOWS\Help
   Opens:
                                            C:\WINDOWS\hh.exe
   Opens:
                                            C:\WINDOWS\ie8
                                            C:\WINDOWS\ie8.log
   Opens:
   Opens:
                                            C:\Documents and
Settings\Admin\Templates\presenta.shw: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                            C:\Documents and Settings\Admin\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\49
                                            C:\Documents and
Settings \verb| Admin \verb| Templates \verb| quattro.wb2: Raec25ph4sudbf0hAaq5ehw3Nf: \$DATA| \\
  Opens:
                                            C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\5
   Opens:
                                            C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\50
                                            C:\Documents and Settings\Admin\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\51
  Opens:
                                            C:\Documents and
Settings\Admin\Templates\winword2.doc: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
   Opens:
                                            C:\Documents and
Settings \land Admin \land Templates \land wordpfct.wpd: Raec 25 ph 4 sudb f 0 h Aaq 5 ehw 3 Nf: \$DATA Aap 5 ehw 3 Nf: \$
                                            C:\Documents and Settings\Admin\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\52
   Opens:
                                            C:\Documents and
Settings\Admin\Templates\wordpfct.wpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                            C:\Documents and Settings\Admin\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\53
                                            C:\Documents and Settings\Admin\Start
Menu\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
   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\Application
Data\Sun\Java\Deployment\cache\6.0\54
                                            C:\Documents and Settings\Admin\Start
Menu\Programs\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
   Opens:
                                            C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\55
                                            C:\Documents and Settings\Admin\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\56
```

C:\AUTOEXEC.BAT

```
Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Internet
Explorer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\57
                         C:\Documents and Settings\Admin\Start Menu\Programs\Outlook
 Opens:
Express.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\58
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\59
                         C:\Documents and Settings\Admin\Start Menu\Programs\Remote
 Opens:
Assistance.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\documents and settings\admin\start menu\programs\startup
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\6
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Windows Media
Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\60
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\61
                         C:\Documents and Settings\Admin\Application
 Opens:
C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Startup\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\documents and settings\admin\start
menu\programs\accessories\accessibility
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\63
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\7
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Address
 Opens:
Book.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\8
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\9
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Command
 Opens:
Prompt.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Admin\Application
 Opens:
{\tt Data\Sun\Java\Deployment\cache\6.0\host}
                         C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Admin\Application
C:\documents and settings\admin\start
 Opens:
menu\programs\accessories\entertainment
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache\6.0\muffin
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\tmp
                         C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\Notepad.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Program
Compatibility Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\deployment.properties\
                         C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\ext
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\log
                         C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\Synchronize.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\security
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\security\trusted.certs\
                         C:\documents and settings\admin\start menu\programs\accessories\system
 Opens:
tools
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Sun\Java\Deployment\tmp}
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\tmp\si
                         C:\WINDOWS\ie8_main.log
 Opens:
                         C:\WINDOWS\iis6.log
 Opens:
 Opens:
                         C:\WINDOWS\ime
 Opens:
                         C:\WINDOWS\imsins.BAK
 Opens:
                         C:\WINDOWS\imsins.log
 Opens:
                         C:\WINDOWS\inf
 Opens:
                         C:\WINDOWS\java
 Opens:
                         C:\WINDOWS\L2Schemas
                         C:\WINDOWS\MedCtrOC.log
 Opens:
 Opens:
                         C:\WINDOWS\Media
 Opens:
                         C:\WINDOWS\Microsoft.NET
```

C:\WINDOWS\msagent

C:\WINDOWS\msapps

```
C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Tour
  Opens:
Windows XP.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                      C:\WINDOWS\msgsocm.log
  Opens:
  Opens:
                                      C:\WINDOWS\msmqinst.log
  Opens:
                                      C:\WINDOWS\mui
                                      C:\WINDOWS\netfxocm.log
  Opens:
                                      C:\WINDOWS\Network Diagnostic
  Opens:
  Opens:
                                      C:\WINDOWS\NOTEPAD.EXE
  Opens:
                                      C:\WINDOWS\ntbtlog.txt
  Opens:
                                      C:\WINDOWS\ntdtcsetup.log
  Opens:
                                      C:\WINDOWS\ocgen.log
  Opens:
                                      C:\WINDOWS\ocmsn.log
                                      C:\WINDOWS\ODBCINST.INI
  Opens:
  Opens:
                                      C:\WINDOWS\OEWABLog.txt
  Opens:
                                      C:\WINDOWS\Offline Web Pages
                                      C:\WINDOWS\pchealth
  Opens:
  Opens:
                                      C:\WINDOWS\PeerNet
  Opens:
                                      C:\WINDOWS\Prairie Wind.bmp
  Opens:
                                      C:\WINDOWS\Prefetch
  Opens:
                                      C:\WINDOWS\Provisioning
  Opens:
                                      C:\WINDOWS\regedit.exe
                                      C:\WINDOWS\REGLOCS.OLD
  Opens:
  Opens:
                                      C:\WINDOWS\regopt.log
  Opens:
                                      C:\WINDOWS\repair
  Opens:
                                      C:\WINDOWS\Resources
  Opens:
                                      C:\WINDOWS\Rhododendron.bmp
  Opens:
                                      C:\WINDOWS\River Sumida.bmp
  Opens:
                                      C:\WINDOWS\Santa Fe Stucco.bmp
  Opens:
                                      C:\WINDOWS\SchedLgU.Txt
  Opens:
                                      C:\WINDOWS\security
  Opens:
                                      C:\WINDOWS\sessmgr.setup.log
  Opens:
                                      C:\WINDOWS\SET3.tmp
  Opens:
                                      C:\WINDOWS\SET4.tmp
                                      C:\WINDOWS\SET8.tmp
  Opens:
                                      C:\WINDOWS\setupact.log
  Opens:
  Opens:
                                      C:\WINDOWS\setupapi.log
                                      C:\Documents and Settings\Admin\Application Data\Sun\Java\jre1.7.0_02
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Application
Data\Sun\Java\jre1.7.0_02\Data1.cab\
                                      {\tt C:\Documents\ and\ Settings\Admin\Application}
  Opens:
Data\Sun\Java\jre1.7.0_02\jre1.7.0_02.msi\
                                      C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Windows
  Opens:
Explorer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                      C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\System
Tools\Internet Explorer (No Add-ons).lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                      \label{lem:cokies-admin} C:\Documents\ and\ Settings\Admin\Cookies\admin@c1.microsoft[2].txt\\
  Opens:
                                      C:\Documents\ and\ Settings\Admin\Cookies\admin@microsoft[1].txt\\
  Opens:
                                      C:\Documents and Settings\Admin\Cookies\admin@rto.microsoft[1].txt\
  Opens:
                                      C:\Documents and Settings\Admin\Cookies\admin@search.microsoft[1].txt\
  Opens:
                                      C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt\
  Opens:
                                      \label{lem:cokies} C: \Documents \ and \ Settings \Admin \Cookies \admin@www.microsoft[3].txt \Cookies \Admin \Cookies \Admi
  Opens:
                                      C:\Documents and Settings\Admin\Cookies\index.dat\
                                      C:\Documents and Settings\Admin\Favorites\Desktop.ini\
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Links\desktop.ini\
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url\
                                      C:\Documents and Settings\Admin\Favorites\Links\Suggested Sites.url\
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Links\Web Slice Gallery.url\
  Opens:
                                      C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE Add-on
site.url\
                                      C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE site on
  Opens:
Microsoft.com.url\
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Home.url\
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Work.url\
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
Store.url\
  Opens:
                                      C:\Documents and Settings\Admin\Favorites\MSN.com.url\
                                      C:\Documents and Settings\Admin\Favorites\Radio Station Guide.url\
  Opens:
                                      C:\Documents and Settings\Admin\Start
  Opens:
Menu\Programs\Accessories\Entertainment\Windows Media
Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                      C:\Documents and Settings\Admin\IECompatCache\index.dat\
  Opens:
                                      C:\Documents and Settings\Admin\IETldCache\index.dat\
                                      C:\Documents and Settings\Admin\Start
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
```

C:\WINDOWS\msdfmap.ini

```
Data\Adobe\Acrobat\9.0
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache\AcroFnt09.lst\
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache\Search
                        C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\Accessibility\Magnifier.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Acrobat\9.0\Updater
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Updater\updater.log\
 Opens:
                        C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Color
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Color\ACECache10.lst\
                        C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Updater6
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Updater6\aum.log\
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Updater6\aumLib.log\
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\Updater6\Install
                        C:\Documents and Settings\Admin\Start
 Opens:
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Admin\SendTo\Compressed (zipped)
 Opens:
Folder.ZFSendToTarget: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\GDIPFONTCACHEV1.DAT\
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\IconCache.db\
                        {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Microsoft
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\CD Burning
                        C:\Documents and Settings\Admin\SendTo\Desktop (create
 Opens:
shortcut).DeskLink: Raec25ph4sudbf0hAag5ehw3Nf:$DATA
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Credentials
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data \\ \ Microsoft \\ \ Credentials \\ \ S-1-5-21-1757981266-507921405-1957994488-1003
                        C:\Documents and
Settings\Admin\SendTo\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                        C:\documents and settings\all users\start menu\programs
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\FeedsStore.feedsdb-ms\
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds\Microsoft Feeds~
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms\
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms\
                        C:\Documents and Settings\All Users\Start
 Opens:
C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Suggested Sites~.feed-ms\
 Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
ms\
                        C:\Documents and Settings\All Users\Start
Opens:
                        C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\desktop.ini\
 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\FBANKAIW\desktop.ini\
                        {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
```

Data\Microsoft\Feeds Cache\FBANKAIW\fwlink[1]\

```
Opens:
                         C:\Documents and Settings\All Users\Start
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\G4DZ1I7H
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
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\
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\J3XY1QNV
 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]\
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\Communications\Network
Connections.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         \dot{\text{C:\Documents}} and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\TLMHA51J
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\TLMHA51J\desktop.ini\
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Feeds Cache\TLMHA51J\ieonline.microsoft[1]\
                         C:\WINDOWS\setuperr.log
 Opens:
 Opens:
                         C:\WINDOWS\setuplog.txt
 Opens:
                         C:\WINDOWS\Soap Bubbles.bmp
 Opens:
                         C:\WINDOWS\SoftwareDistribution
 Opens:
                         C:\WINDOWS\spupdsvc.log
 Opens:
                         C:\WINDOWS\srchasst
 Opens:
                         C:\WINDOWS\Sti_Trace.log
 Opens:
                         C:\WINDOWS\Sun
 Opens:
                         C:\WINDOWS\SxsCaPendDel
                         C:\WINDOWS\system
 Opens:
 Opens:
                         C:\WINDOWS\system.ini
 Opens:
                         C:\WINDOWS\tabletoc.log
                         C:\WINDOWS\TASKMAN.EXE
 Opens:
 Opens:
                         C:\WINDOWS\Tasks
 Opens:
                         C:\WINDOWS\Temp
 Opens:
                         C:\WINDOWS\tsoc.log
 Opens:
                         C:\WINDOWS\twain.dll
 Opens:
                         C:\WINDOWS\twain_32
 Opens:
                         C:\WINDOWS\twain 32.dll
 Opens:
                         C:\WINDOWS\twunk_16.exe
 Opens:
                         C:\WINDOWS\twunk_32.exe
 Opens:
                         C:\WINDOWS\unins000.dat
 Opens:
                         C:\WINDOWS\unins000.exe
                         C:\WINDOWS\unins001.dat
 Opens:
 Opens:
                         C:\WINDOWS\unins001.exe
 Opens:
                         C:\WINDOWS\updspapi.log
 Opens:
                         C:\WINDOWS\vb.ini
 Opens:
                         C:\WINDOWS\vbaddin.ini
 Opens:
                         C:\WINDOWS\vmmreg32.dll
 Opens:
                         C:\WINDOWS\WBEM
 Opens:
                         C:\WINDOWS\Web
                         C:\WINDOWS\wiadebug.log
 Opens:
                         C:\WINDOWS\wiaservc.log
 Opens:
 Opens:
                         C:\WINDOWS\win.ini
 Opens:
                         C:\WINDOWS\WindowsUpdate.log
 Opens:
                         C:\WINDOWS\winhelp.exe
 Opens:
                         C:\WINDOWS\winhlp32.exe
                         C:\WINDOWS\winnt.bmp
 Opens:
                         C:\WINDOWS\winnt256.bmp
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\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
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Custom Settings\Custom0
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Custom Settings\Custom0\install.ins\
 Opens:
                         C:\WINDOWS\wmsetup.log
                         C:\WINDOWS\WMSysPr9.prx
 Opens:
 Opens:
                         C:\WINDOWS\Zapotec.bmp
 Opens:
                         C:\WINDOWS\_default.pif
 Opens:
                         C:\WINDOWS\WinSxS\InstallTemp
                         C:\WINDOWS\WinSxS\Manifests
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Start
```

```
Menu\Programs\Accessories\Communications\Network Setup
Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\DOMStore
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\DOMStore\OWORJP5C
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK\www.microsoft[1].xml\
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\Communications\New Connection
Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T
 Opens:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Wireless Network Setup
Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                        C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\DOMStore\index.dat\
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\DOMStore\LQLIM8KB
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\Accessibility\Accessibility
Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Microsoft\Internet Explorer\frameiconcache.dat\
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT\
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Recovery
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Recovery\Active
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Last Active
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{80236AC0-AAD6-11E3-AE20-
08002733366F}.dat\
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Internet Explorer\Recovery\Last Active\{69EE14A0-C276-11E3-AE24-08002733366F}.dat\
                         C:\Documents and Settings\All Users\Start
 Opens:
Menu\Programs\Accessories\Accessibility\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\rsoplog.bak\
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Internet Explorer\rsoplog.txt\
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Services
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Media Player
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb\
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Office
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Office\12.0
                         C:\Documents and Settings\All
 Opens:
Users\Documents\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Office\14.0
                         C:\Documents and Settings\Admin\SendTo\Mail
 Opens:
Recipient.MAPIMail: Raec25ph4sudbf0hAag5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Silverlight
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Silverlight\mssl.lck\
 Opens:
                         C:\Documents and Settings\Admin\SendTo\My
Documents.mydocs: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Windows
 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\Recent\Desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Windows Media
```

C:\Documents and Settings\Admin\Local Settings\Application

```
Data\Microsoft\Windows Media\9.0
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD\
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML\
  Opens:
                                     C:\WINDOWS\system32\urlmon.dll.123.Manifest
  Opens:
                                     C:\WINDOWS\system32\urlmon.dll.123.Config
  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
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\0
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\1
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\10
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\11
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\12
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\14
                                     C:\WINDOWS\WinSxS\MSIL_IEExecRemote_b03f5f7f11d50a3a_2.0.0.0_x-
  Opens:
ww_6e57c34e
                                     C:\WINDOWS\WinSxS\Policies
  Opens:
                                     C:\WINDOWS\WinSxS\x86_Microsoft.Tools.VisualCPlusPlus.Runtime-
  Opens:
Libraries_6595b64144ccf1df_6.0.0.0_x-ww_ff9986d7
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700
  Opens:
C:\WINDOWS\WinSxS\x86 Microsoft.VC90.ATL 1fc8b3b9a1e18e3b 9.0.30729.4148 x-ww 353599c2
  Opens:
                                     C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.21022.8_x-
ww_d08d0375
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e
  Opens:
C:\WINDOWS\WinSxS\x86 Microsoft.VC90.MFCLOC 1fc8b3b9a1e18e3b 9.0.30729.4148 x-ww 15fc9313
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_a57c1f53
                                     C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
  Opens:
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.0.0_x-ww_2726e76a
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.2600.5512_x-
ww_3fd60d63
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.0.0_x-ww_8d353f13
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.Dxmrtp_6595b64144ccf1df_5.2.2.3_x-ww_468466a7
{\tt C:\WINDOWS\WinSxS\x86\_Microsoft.Windows.Networking.RtcDll\_6595b64144ccf1df\_5.2.2.3\_x-ww\_d6bd8b95}
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.RtcRes_6595b64144ccf1df_5.2.2.3_en_16a24bc0
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\15
C: \verb|WINDOWS| WinSxS| x86_System.EnterpriseServices_b03f5f7f11d50a3a_2.0.0.0_x-ww_7d5f3790| with the control of the control 
  Opens:
                                     {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Sun\Java\Deployment\cache\6.0\16
  Opens:
C:\WINDOWS\WinSxS\x86_System.EnterpriseServices_b03f5f7f11d50a3a_2.0.0.0_x-
ww_7d5f3790\System.EnterpriseServices.dll
  Opens:
C:\WINDOWS\WinSxS\x86_System.EnterpriseServices_b03f5f7f11d50a3a_2.0.0.0_x-
ww_7d5f3790\System.EnterpriseServices.Wrapper.dll
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.RtcRes_6595b64144ccf1df_5.2.2.3_en_16a24bc0\rtcres.dll
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.RtcDll_6595b64144ccf1df_5.2.2.3_x-
ww_d6bd8b95\rtcdll.dll
  Opens:
ww_468466a7\dxmrtp.dll
```

```
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.0.0_x-
ww_8d353f13\GdiPlus.dll
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.2600.5512_x-
ww_3fd60d63\msvcirt.dll
  Opens:
C:\WINDOWS\WinSxS\x86 Microsoft.Windows.CPlusPlusRuntime 6595b64144ccf1df 7.0.2600.5512 x-
ww_3fd60d63\msvcrt.dll
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.0.0_x-
ww_2726e76a\msvcirt.dll
  Opens:
C:\WINDOWS\WinSxS\x86 Microsoft.Windows.CPlusPlusRuntime 6595b64144ccf1df 7.0.0.0 x-
ww_2726e76a\msvcrt.dll
                                     C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE Add-on
  Opens:
site.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\17
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\18
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\19
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\2
  Opens:
                                     {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\21
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\22
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\23
                                     C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE site on
  Opens:
Microsoft.com.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\24
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\25
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\27
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\28
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
{\tt Data\Sun\Java\Deployment\cache\6.0\3}
  Opens:
                                     C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Home.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\30
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data \S un \S ava \S eployment \S ache \S 6.0 \S 31
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\32
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\33
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\34
  Opens:
                                     {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Sun\Java\Deployment\cache\6.0\35
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\36
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\37
  Opens:
                                     {\tt C:\Documents\ and\ Settings\Admin\Favorites\Microsoft\ Websites\Microsoft\ Websit
At Work.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\38
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\39
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\4
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\40
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\41
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\42
                                     C:\Documents and Settings\Admin\Local Settings\Application
  Opens:
Data\Sun\Java\Deployment\cache\6.0\43
```

```
Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\45
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc\
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
   Opens:
Store.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\46
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\47
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\47\15572e2f-21932044\
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Opens:
                                                    C:\Documents and
Settings \verb| Admin \verb| Favorites \verb| Links \verb| desktop.ini|: Raec25ph4sudbf0hAaq5ehw3Nf: \$DATA | Admin \verb| Favorites \verb| Links \verb| desktop.ini|: Raec25ph4sudbf0hAaq5ehw3Nf: \$DATA | Admin \verb| Favorites \verb| Links \verb| desktop.ini|: Raec25ph4sudbf0hAaq5ehw3Nf: \$DATA | Admin \verb| Admin \verb
                                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
   Opens:
Data\Sun\Java\Deployment\cache\6.0\48
   Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\49
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
{\tt Data\Sun\Java\Deployment\cache\6.0\5}
                                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
   Opens:
Data\Sun\Java\Deployment\cache\6.0\50
   Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\51
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\52
                                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
   Opens:
Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\54
                                                    C:\Documents and Settings\Admin\Favorites\Links\Free
   Opens:
Hotmail.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\55
   Opens:
                                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Sun\Java\Deployment\cache\6.0\56
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\57
   Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\58
   Opens:
                                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Sun\Java\Deployment\cache\6.0\59
   Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\6
   Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\60
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\61
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\62
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Sun\Java\Deployment\cache\6.0\63
   Opens:
                                                    C:\Documents and Settings\Admin\Favorites\Links\Suggested
Sites.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\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
\label{lem:decomposition} Data \S un \S ava \S eployment \cache \S 6.0 \S 
   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\lastAccessed\
   Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\muffin
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\tmp
   Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\desktop.ini\
   Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\History\desktop.ini\
   Opens:
                                                    C:\Documents and Settings\Admin\Local Settings\History\History.IE5
                                                    C:\Documents and Settings\Admin\Local
   Opens:
```

Settings\History\History.IE5\desktop.ini\

```
Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat\
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014031220140313
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\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\
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014041220140413
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings \verb|\History\History.IE5\MSHist012014041220140413\\ \verb|\Index.dat\\|
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Links\Web Slice
Gallery.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 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\
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ASPNETSetup_00000.log\
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ASPNETSetup_00001.log\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\AUCHECK_PARSER.txt\
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Compatibility\ Pack}
 Opens:
for the 2007 Office system (0).log\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_clwireg.txt\
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_depcheck_NETFX_EXP_35.txt\
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_dotnetfx35error.txt\
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_dotnetfx35install.txt\
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_NET_Framework20_Setup164F.txt\
                         C:\Documents and Settings\Admin\Local
 Opens:
{\tt Settings\Temp\dd\_NET\_Framework30\_Setup16AE.txt} \\
                         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\
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_RGB9RAST_x86.msi601E.txt\
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_wcf_retCA2A49.txt\
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\dd_wcf_retCA3565.txt\
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\dd_wcf_retCA35A0.txt\
                         C:\Documents and Settings\Admin\Local Settings\Temp\dd_XPS.txt\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\gen_py
 Opens:
                         \label{local Settings-Temp-gen_py-2.7} C: \verb|\Documents| and Settings-Admin-Local Settings-Temp-gen_py-2.7
 Opens:
                         C:\Documents and Settings\Admin\Local
 Opens:
{\tt 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\Cookies\admin@search.microsoft[1].txt: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\Documents and
Settings\Admin\Cookies\index.dat: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\JAUReg.log\
                         C:\Documents and Settings\Admin\Local Settings\Temp\java_install.log\
 Opens:
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\java_install_reg.log\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\jusched.log\
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\Microsoft\ PowerPoint}
 Opens:
Viewer (0).log\
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Opens:
2010 x86 Redistributable Setup_10.0.30319
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup 20131223 035827352-MSI vc red.msi.txt\
                         C:\AUTOEXEC.BAT: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20131223_035827352.html\
                         C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
 Opens:
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\
                                   C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
  Opens:
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\
                                   C:\Documents and Settings\Admin\Local Settings\Temp\setup.log\
  Opens:
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\SilverlightO.log\
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temp\SilverlightMSI.log\
                                   C:\Documents and Settings\Admin\Local Settings\Temp\uxeventlog.txt\
  Opens:
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\AntiPhishing
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\AntiPhishing\2CEDBFBC-DBA8-43AA-B1FD-CC8E6316E3E2.dat\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\180x150_WP_NokiaReinvented_EN_US[1].gif\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\300lo[1].json\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\300lo[2].json\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files \verb|\Content.IE5| CXCXW1MR \verb|\33975792-bade-4cf2-b676-3b0eee2cf2ed_16[1].jpg \verb|\Files| CXCXW1MR \verb|\A33975792-bade-4cf2-b676-3b0eee2cf2ed_16[1].jpg \verb|\Files| CXCXW1MR CXCXW
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\3ef01e72-0832-46f0-a6e1-23f9d5a07d86_5[1].png\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\871d9c8a-b403-40aa-aeb8-9ecd40181833_15[1].jpg\
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\88666cc6-d578-45c8-baf0-89d3837f41c3_89[1].css\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\93e33485-fea3-4687-a642-2c5dd233522f_12[1].eot\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\access-web-bg-grey[1].jpg\
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\access_dev_center_new[1].jpg\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\accordion_icon_sprites[1].png\
                                   {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\CXCXW1MR\ADSAdClient31[1].txt\
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[2].txt\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\ADSAdClient31[3].txt\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[4].txt\
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[5].txt\
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\adServer[1].htm\
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\auth016[1].js\
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\bimapping[2].js\
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\broker[1].js\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CA9ATUDW.css\
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CAMLW29Z.jsx\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\CATM568T.jsx\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\CAVLZJ9D.jsx\
  Opens:
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\click-to-install-right[1].png\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\Closed_btn_21x21[1].png\
  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\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
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\
                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\daf22230-6bbc-4982-87b3-6da3f5e6e8b4_28[1].jpg\
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\DataList[1].css\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\desktop.ini\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\dotnetfx35setup[1].exe
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\dotnetfx35setup[1].exe\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\e64030e7-ad8c-4be8-a45a-b69a2df3caef_13[1].eot\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\eb4f0171-7cb7-428a-afcc-d93a6b84525c_33[1].png\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\event[1].js\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\event[2].js\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\event[3].js\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\event[5].js\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\false[1].htm\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\favicon[1].ico\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\General[1].css\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\General[1].js\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\georedirect[1].htm\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\georedirect[2].htm\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\georedirect[3].htm\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\georedirect[4].htm\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\gl_social[1].png\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\icon_plus_hover[1].png\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\icon_to_right_arrow[1].png\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\info_tip_16x16[1].png\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\install[1].css\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\js[2].ashx\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\LoginStatus[1].css\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\microsoft-accessibility_2[1].jpg\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\microsoft_symbol_clr_56x56[1].png\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\microsoft_update_icon[1].png\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\ms-silverlight-logo-rev[1].png\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\Nebula[1].js\
                         C:\boot.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\omnibase[2].css\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\oneMscomBlade[2].css\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\onemscomfooter[2].css\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[2].js\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[3].js\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\page_bg_mid[1].png\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\page_top[1].png\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\script[1].js\
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\script[1].jsx\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\script[2].jsx\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files \verb|\CXCXW1MR\top-nav-right[1].jpg\\|
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\top-nav-seperator[1].gif\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\true[1].htm\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\true[2].htm\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\views[1]\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\WebResource[1].axd\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\wtid[1].js\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\CXCXW1MR\wt_capi[2].js\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\desktop.ini\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\index.dat\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\ONWV4FIP
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\ONWV4FIP\35a5f647-c96d-4bbf-b9f4-ca71e16add70_28[1].jpg\
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\5a7873a1-fd4e-4462-8ab2-32bd729117c6_7[1].png\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\ONWV4FIP\736e3781-6a19-4119-b717-e61f0d8982c0_12[1].eot\
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\accessibility_logo[1].jpg\
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\ADSAdClient31[1].txt\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\ONWV4FIP\ADSAdClient31[2].txt\
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\auth016[1].js\
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\auth016[2].js\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\ONWV4FIP\bgLineTile[1].jpg\
  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\bing_logo[1].png\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files \verb|\| Content.IE5 \verb|\| ONWV4FIP \verb|\| blind-low-vision-thumb[1].jpg \verb|\| blind-l
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\broker-config_s1[1].js\
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\broker-config_s1[2].js\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\ONWV4FIP\broker-config_s1[3].js\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\ONWV4FIP\CA39W670.isx\
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\CAANG12B.css\
                                    C:\CONFIG.SYS: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\CAU35S9Y.jsx\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\0NWV4FIP\cbc6f38d-b79c-4bff-8b67-b81eb9676ab3_5[1].png\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\ONWV4FIP\ChangePassword[1].css\
  Opens:
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\click-to-install-left[1].png\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
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\
                                    C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\ONWV4FIP\core114[1].js\
```

```
Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\counter017[1].js\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\counter017[2].js\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
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\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\desktop.ini\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\details[1].htm\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\details[2].htm\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\e9979a8b-c439-452a-a09f-d3b32df0e5b1_13[1].png\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\email[1].png\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\en-us[1].gif\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\event[1].js\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\event[3].js\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\event[6].js\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\facebook[1].gif\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\favicon[1].ico\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\favicon[2].ico\
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\ONWV4FIP\favicon[4].ico\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\favicon[5].ico\
                         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_site[1].png\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\ONWV4FIP\gl_social[1].svg\
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\hero_bg_index[1].png\
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\icon_minus_hover[1].png\
                         C:\system volume information\catalog.wci\00010001.dir
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\IE8-WindowsXP-x86-ENU[1].exe
                         C:\System Volume Information\catalog.wci\00010001.dir
 Opens:
 Opens:
                         C:\System Volume Information\catalog.wci\00010001.ci
 Opens:
                         C:\System Volume Information\catalog.wci\CiFLfffc.002
 Opens:
                         C:\System Volume Information\catalog.wci\CiFLfffc.001
 Opens:
                         C:\exception.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                         C:\IO.SYS: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\MSDOS.SYS: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
 Opens:
                         C:\NTDETECT.COM: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\ntldr: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\program files
                         C:\system volume information
 Opens:
 Opens:
                         C:\windows
 Opens:
                         C:\WINDOWS\0.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\windows\addins
 Opens:
                         C:\windows\apppatch
 Opens:
                         C:\windows\assembly
                         C:\WINDOWS\Blue Lace 16.bmp: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
 Opens:
                         C:\WINDOWS\bootstat.dat: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
                         C:\WINDOWS\svstem32\wsock32.dll
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\wbem\wbemprox.dll
 Opens:
                         C:\WINDOWS\system32\wbem\wbemcomn.dll
 Opens:
                         C:\WINDOWS\system32\wbem\wbemsvc.dll
                         C:\WINDOWS\explorer.exe: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
 Opens:
 Opens:
                         C:\WINDOWS\system32\wbem\fastprox.dll
 Opens:
                         C:\WINDOWS\system32\msvcp60.dll
                         C:\WINDOWS\system32\ntdsapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll
 Opens:
                         C:\WINDOWS\explorer.scf: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
```

Opens: C:\WINDOWS\WinSxS\x86 Microsoft.VC90.MFC 1fc8b3b9a1e18e3b 9.0.30729.4148 x-ww a57c1f53\mfc90.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_x-ww\_a57c1f53\mfc90u.dll Opens:  ${\tt C:WINDOWS\winSxS\x86\_Microsoft.VC90.MFC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_x-ww\_a57c1f53\mfcm90.dll}$ Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_a57c1f53\mfcm90u.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFCLOC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_15fc9313\mfc90chs.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFCLOC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_15fc9313\mfc90cht.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFCLOC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_15fc9313\mfc90deu.dll Opens:  $\textbf{C:.} \\ \textbf{WINDOWS} \\ \textbf{WinSxS} \\ \textbf{x86\_Microsoft.VC90.MFCLOC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_x-16.2000} \\ \textbf{x148\_x2000} \\ \textbf{x25000} \\ \textbf{x25000} \\ \textbf{x36000} \\ \textbf{x36000} \\ \textbf{x36000} \\ \textbf{x36000} \\ \textbf{x46000} \\ \textbf{x36000} \\ \textbf{x46000} \\ \textbf{x46000} \\ \textbf{x66000} \\ \textbf$ ww\_15fc9313\mfc90enu.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFCLOC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_15fc9313\mfc90esn.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFCLOC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_15fc9313\mfc90esp.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFCLOC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_15fc9313\mfc90fra.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFCLOC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_15fc9313\mfc90ita.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFCLOC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_15fc9313\mfc90jpn.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFCLOC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_15fc9313\mfc90kor.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.MFCLOC\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_15fc9313\mfc90rus.dll Opens: ww\_d495ac4e\msvcm90.dll Opens: ww\_d495ac4e\msvcp90.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.CRT\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_xww\_d495ac4e\msvcr90.dll Opens: C:\WINDOWS\WinSxS\x86 Microsoft.VC90.CRT 1fc8b3b9a1e18e3b 9.0.21022.8 xww\_d08d0375\msvcm90.dl1 Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.CRT\_1fc8b3b9a1e18e3b\_9.0.21022.8\_xww\_d08d0375\msvcp90.dll Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.CRT\_1fc8b3b9a1e18e3b\_9.0.21022.8\_xww\_d08d0375\msvcr90.dl1 Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC90.ATL\_1fc8b3b9a1e18e3b\_9.0.30729.4148\_x-ww\_353599c2\atl90.dl1 C:\WINDOWS\WinSxS\x86\_Microsoft.VC80.CRT\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_6b128700\msvcm80.dll Opens:  ${\tt C:\WINDOWS\WinSxS\x86\_Microsoft.VC80.CRT\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_6b128700\mbox{msvcp80.dll}}$ Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.VC80.CRT\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_6b128700\msvcr80.dll C:\WINDOWS\WinSxS\x86\_Microsoft.VC80.CRT\_1fc8b3b9a1e18e3b\_8.0.50727.3053\_xww\_b80fa8ca\msvcm80.dll C:\WINDOWS\WinSxS\x86\_Microsoft.VC80.CRT\_1fc8b3b9a1e18e3b\_8.0.50727.3053\_xww b80fa8ca\msvcp80.dll C:\WINDOWS\WinSxS\x86 Microsoft.VC80.CRT 1fc8b3b9a1e18e3b 8.0.50727.3053 xww\_b80fa8ca\msvcr80.dll Opens: C:\WINDOWS\FaxSetup.log: Raec25ph4sudbf0hAaq5ehw3Nf:\$DATA C:\WINDOWS\WinSxS\x86\_Microsoft.Tools.VisualCPlusPlus.Runtime-Opens: Libraries\_6595b64144ccf1df\_6.0.0.0\_x-ww\_ff9986d7\atl.dll C:\WINDOWS\WinSxS\x86\_Microsoft.Tools.VisualCPlusPlus.Runtime-

Opens: C:\WINDOWS\FeatherTexture.bmp: Raec25ph4sudbf0hAaq5ehw3Nf:\$DATA
Opens: C:\windows\fonts

C:\WINDOWS\WinSxS\x86\_Microsoft.Tools.VisualCPlusPlus.Runtime-

 $Libraries\_6595b64144ccf1df\_6.0.0.0\_x-ww\_ff9986d7 \verb|\mfc42.dll|$ 

Libraries\_6595b64144ccf1df\_6.0.0.0\_x-ww\_ff9986d7\mfc42u.dll

```
Opens:
                                                                   C:\WINDOWS\Gone Fishing.bmp: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
    Opens:
                                                                   C:\WINDOWS\Greenstone.bmp: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
    Opens:
                                                                   C:\windows\help
                                                                   C:\WINDOWS\hh.exe: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
    Opens:
    Opens:
                                                                   C:\windows\ie8
    Opens:
                                                                   C:\WINDOWS\ie8.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
    Opens:
                                                                   C:\WINDOWS\ie8_main.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                                                   C:\WINDOWS\iis6.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
    Opens:
    Opens:
                                                                   C:\windows\ime
                                                                   C:\WINDOWS\imsins.BAK: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
    Opens:
                                                                  C:\WINDOWS\imsins.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
    Opens:
    Opens:
                                                                   C:\windows\inf
    Opens:
                                                                   C:\windows\installer
                                                                   C:\windows\java
    Opens:
    Opens:
                                                                   C:\windows\l2schemas
    Opens:
                                                                   C:\WINDOWS\MedCtrOC.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
    Opens:
                                                                  C:\windows\media
    Opens:
                                                                   C:\windows\microsoft.net
    Opens:
                                                                   C:\windows\msagent
    Opens:
                                                                   C:\windows\msapps
    Opens:
                                                                   C:\WINDOWS\system32\mswsock.dll
    Opens:
                                                                   C:\WINDOWS\system32\hnetcfg.dll
                                                                   C:\WINDOWS\system32\wshtcpip.dll
    Opens:
                                                                   C:\WINDOWS\system32\iphlpapi.dll
    Opens:
    Opens:
                                                                   C:\WINDOWS\msdfmap.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                                                   C:\WINDOWS\msgsocm.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
    Opens:
    Opens:
                                                                   C:\WINDOWS\system32\winrnr.dll
    Opens:
                                                                   C:\WINDOWS\system32\drivers\etc\hosts
    Opens:
                                                                   C:\WINDOWS\system32\rsaenh.dll
    Opens:
                                                                   C:\WINDOWS\msmqinst.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
    Opens:
                                                                   C:\windows\mui
                                                                   C:\WINDOWS\netfxocm.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
    Opens:
    Opens:
                                                                   C:\windows\network diagnostic
    Opens:
                                                                   C:\WINDOWS\NOTEPAD.EXE: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
                                                                   {\tt C:\WINDOWS\WinSxS\x86\_Microsoft.Tools.VisualCPlusPlus.Runtime-line} \\
    Opens:
Libraries_6595b64144ccf1df_6.0.0.0_x-ww_ff9986d7\msvcp60.dll
    Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.1.0.Microsoft.Windows.GdiPlus_6595b64144ccf1df_x-
ww_4e8510ac
    Opens:
C: \verb|WINDOWS| \verb|WinSxS| Policies| x86_policy.5.1. \verb|Microsoft|. Windows.SystemCompatible_6595b64144ccf1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df
ww a0111510
    Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.5.2.Microsoft.Windows.Networking.Dxmrtp_6595b64144ccf1df_x-
ww 362e60dd
    Opens:
C: \verb|WINDOWS| WinSxS | Policies| x86_policy.5.2. Microsoft. Windows. Networking. Rtcdll_6595b64144ccf1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_x-f1df_
ww c7b7206f
                                                                   C:\WINDOWS\WinSxS\Policies\x86_policy.6.0.Microsoft.Windows.Common-
    Opens:
Controls_6595b64144ccf1df_x-ww_5ddad775
C:\WINDOWS\WinSxS\Policies\x86_policy.7.0.Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_x-
ww_a317e4b3
    Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-ww_77c24773
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.ATL_1fc8b3b9a1e18e3b_x-ww_9e7eb501
    Opens:
C: \verb|WINDOWS| winSxS| Policies| x86_policy.9.0. \verb|Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-ww_b7353f75| and the property of the
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_x-ww_b8438ace
    Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_x-ww_4ee8bb30
    Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_x-
ww_4ee8bb30\9.0.30729.4148.cat
    Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_x-
ww_4ee8bb30\9.0.30729.4148.policy
    Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_x-
ww_b8438ace\9.0.30729.4148.cat
    Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_x-
ww_b8438ace\9.0.30729.4148.policy
    Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-
ww_b7353f75\9.0.21022.8.cat
    Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-
ww_b7353f75\9.0.21022.8.policy
    Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-
```

```
ww_b7353f75\9.0.30729.4148.cat
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-
ww_b7353f75\9.0.30729.4148.policy
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.ATL_1fc8b3b9a1e18e3b_x-
ww_9e7eb501\9.0.30729.4148.cat
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.ATL_1fc8b3b9a1e18e3b_x-
ww_9e7eb501\9.0.30729.4148.policy
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-
ww_77c24773\8.0.50727.3053.cat
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-
ww_77c24773\8.0.50727.3053.policy
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-
ww_77c24773\8.0.50727.762.cat
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-
ww_77c24773\8.0.50727.762.policy
C:\WINDOWS\WinSxS\Policies\x86_policy.7.0.Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_x-
ww_a317e4b3\7.0.2600.5512.cat
  Opens:
C: \verb|WINDOWS| WinSxS| Policies| x86_policy. 7.0. \\ Microsoft. \\ Windows. CPlusPlusRuntime\_6595b64144ccf1 \\ df_x-f1 \\ df_x-f1 \\ df_x-f2 \\ df_x-f2 \\ df_x-f3 \\ df_x-f3
ww_a317e4b3\7.0.2600.5512.Policy
                                       Opens:
Controls_6595b64144ccf1df_x-ww_5ddad775\6.0.2600.5512.cat
                                       C:\WINDOWS\WinSxS\Policies\x86_policy.6.0.Microsoft.Windows.Common-
  Opens:
Controls_6595b64144ccf1df_x-ww_5ddad775\6.0.2600.5512.Policy
C:\WINDOWS\WinSxS\Policies\x86_policy.5.2.Microsoft.Windows.Networking.Rtcdll_6595b64144ccf1df_x-
ww_c7b7206f\5.2.2.3.cat
C:\WINDOWS\WinSxS\Policies\x86_policy.5.2.Microsoft.Windows.Networking.Rtcdll_6595b64144ccf1df_x-
ww_c7b7206f\5.2.2.3.Policy
                                       C:\WINDOWS\ntbtlog.txt: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:
  Writes to:
                                       C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.vir
  Writes to:
                                       \label{lem:c:windows} $$C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet\_state.exe$
  Writes to:
                                       C:\WINDOWS\system32\cisvc.vir
  Writes to:
                                       C:\WINDOWS\system32\cisvc.exe
  Writes to:
                                       C:\WINDOWS\system32\clipsrv.vir
                                       C:\WINDOWS\system32\clipsrv.exe
  Writes to:
                                       C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.vir
  Writes to:
  Writes to:
                                       \label{lem:c:windows} \textbf{C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mbox{\mbox{$m$corsvw.exe}$}} exe
  Writes to:
                                       C:\WINDOWS\system32\dmadmin.vir
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiSP0000.000
  Writes to:
                                       C:\WINDOWS\system32\dmadmin.exe
                                       C:\System Volume Information\catalog.wci\INDEX.000
  Writes to:
  Writes to:
                                       C:\System Volume Information\catalog.wci\INDEX.002
  Writes to:
                                       C:\System Volume Information\catalog.wci\INDEX.001
                                       C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication
  Writes to:
Foundation\infocard.vir
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiFLfffd.000
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiCL0001.000
  Writes to:
                                       C:\Svstem Volume Information\catalog.wci\CiSL0001.000
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiP10000.000
                                       C:\System Volume Information\catalog.wci\CiP20000.000
  Writes to:
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiPT0000.000
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiST0000.000
                                       C:\System Volume Information\catalog.wci\propstor.bk1
  Writes to:
                                       C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication
  Writes to:
Foundation\infocard.exe
                                       C:\System Volume Information\catalog.wci\CiP10000.002
  Writes to:
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiP10000.001
  Writes to:
                                       C:\System Volume Information\catalog.wci\propstor.bk2
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiP20000.002
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiP20000.001
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiVP0000.000
                                       C:\WINDOWS\system32\imapi.vir
  Writes to:
  Writes to:
                                       C:\WINDOWS\system32\imapi.exe
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiPT0000.002
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiPT0000.001
  Writes to:
                                       C:\System Volume Information\catalog.wci\cicat.hsh
  Writes to:
                                       C:\System Volume Information\catalog.wci\cicat.fid
  Writes to:
                                       C:\WINDOWS\system32\mnmsrvc.vir
  Writes to:
                                       C:\WINDOWS\system32\mnmsrvc.exe
  Writes to:
                                       C:\System Volume Information\catalog.wci\CiSP0000.001
  Writes to:
                                       C:\WINDOWS\system32\msiexec.vir
                                       C:\System Volume Information\catalog.wci\CiSP0000.002
  Writes to:
```

C:\WINDOWS\system32\msiexec.exe

Writes to:

```
Writes to:
                          C:\WINDOWS\system32\netdde.vir
 Writes to:
                          C:\WINDOWS\system32\netdde.exe
                          C:\System Volume Information\catalog.wci\00000002.ps1
 Writes to:
                          C:\System Volume Information\catalog.wci\00000002.ps2
 Writes to:
 Writes to:
                          C:\Program Files\Common Files\Microsoft Shared\Source Engine\ose.vir
 Writes to:
                          C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE
 Writes to:
                          C:\WINDOWS\system32\sessmgr.vir
 Writes to:
                          C:\WINDOWS\system32\sessmgr.exe
 Writes to:
                          C:\WINDOWS\system32\locator.vir
 Writes to:
                          C:\WINDOWS\system32\locator.exe
                          C:\WINDOWS\system32\scardsvr.vir
 Writes to:
 Writes to:
                          C:\WINDOWS\system32\scardsvr.exe
 Writes to:
                          C:\WINDOWS\system32\smlogsvc.vir
                          C:\WINDOWS\system32\vssvc.vir
 Writes to:
 Writes to:
                          C:\WINDOWS\system32\vssvc.exe
 Writes to:
                          C:\WINDOWS\system32\wbem\wmiapsrv.vir
                          C:\WINDOWS\system32\wbem\wmiapsrv.exe
 Writes to:
 Writes to:
                          C:\System Volume Information\catalog.wci\CiST0000.002
 Writes to:
                          C:\System Volume Information\catalog.wci\CiST0000.001
 Writes to:
                          C:\System Volume Information\catalog.wci\CiCL0001.002
 Writes to:
                          C:\System Volume Information\catalog.wci\CiCL0001.001
 Writes to:
                          C:\Program Files\Internet Explorer\iexplore.vir
                          C:\Program Files\Internet Explorer\iexplore.exe
 Writes to:
 Writes to:
                          C:\WINDOWS\Prefetch\VERCLSID.EXE-3667BD89.pf
 Writes to:
                          C:\System Volume Information\catalog.wci\00010001.dir
                          C:\System Volume Information\catalog.wci\00010001.ci
 Writes to:
 Writes to:
                          C:\System Volume Information\catalog.wci\CiFLfffc.000
 Writes to:
                          C:\System Volume Information\catalog.wci\CiFLfffc.002
                          {\tt C:\System\ Volume\ Information\catalog.wci\CiFLfffc.001}
 Writes to:
 Reads from:
                          C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe
 Reads from:
                          C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.vir
 Reads from:
                          C:\WINDOWS\system32\cisvc.exe
 Reads from:
                          C:\WINDOWS\system32\cisvc.vir
 Reads from:
                          C:\WINDOWS\Registration\R00000000007.clb
                          C:\WINDOWS\system32\ixsso.dll
 Reads from:
 Reads from:
                          C:\WINDOWS\system32\clipsrv.exe
 Reads from:
                          C:\WINDOWS\system32\clipsrv.vir
 Reads from:
                          C:\WINDOWS\system32\ciodm.dll
 Reads from:
                          C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
 Reads from:
                          C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.vir
 Reads from:
                          C:\WINDOWS\system32\langwrbk.dll
                          C:\WINDOWS\system32\dllhost.exe
 Reads from:
 Reads from:
                          C:\WINDOWS\system32\dmadmin.exe
 Reads from:
                          C:\WINDOWS\system32\dmadmin.vir
                          C:\WINDOWS\Microsoft.NET\Framework\v3.0\WPF\PresentationFontCache.exe
 Reads from:
 Reads from:
                          C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication
Foundation\infocard.exe
 Reads from:
                          C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication
Foundation\infocard.vir
 Reads from:
                          C:\WINDOWS\system32\imapi.exe
 Reads from:
                          C:\WINDOWS\system32\imapi.vir
 Reads from:
                          C:\WINDOWS\system32\mnmsrvc.exe
 Reads from:
                          C:\WINDOWS\system32\mnmsrvc.vir
                          C:\WINDOWS\system32\msdtc.exe
 Reads from:
 Reads from:
                          C:\WINDOWS\svstem32\msiexec.exe
 Reads from:
                          C:\WINDOWS\system32\msiexec.vir
                          C:\WINDOWS\system32\netdde.exe
 Reads from:
 Reads from:
                          C:\WINDOWS\system32\netdde.vir
 Reads from:
                          C:\System Volume Information\catalog.wci\propstor.bk1
 Reads from:
                          C:\System Volume Information\catalog.wci\propstor.bk2
 Reads from:
                          C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE
 Reads from:
                          C:\Program Files\Common Files\Microsoft Shared\Source Engine\ose.vir
                          C:\WINDOWS\system32\sessmgr.exe
 Reads from:
 Reads from:
                          C:\WINDOWS\system32\sessmgr.vir
 Reads from:
                          C:\WINDOWS\system32\locator.exe
 Reads from:
                          C:\WINDOWS\system32\locator.vir
 Reads from:
                          C:\WINDOWS\system32\scardsvr.exe
 Reads from:
                          C:\WINDOWS\system32\scardsvr.vir
 Reads from:
                          C:\WINDOWS\system32\smlogsvc.exe
                          C:\WINDOWS\system32\ups.exe
 Reads from:
 Reads from:
                          C:\WINDOWS\system32\vssvc.exe
                          C:\WINDOWS\system32\vssvc.vir
 Reads from:
 Reads from:
                          C:\WINDOWS\system32\wbem\wmiapsrv.exe
 Reads from:
                          C:\WINDOWS\system32\wbem\wmiapsrv.vir
 Reads from:
                          C:\WINDOWS\system32\noise.dat
 Reads from:
                          C:\Documents and Settings\NetworkService\ntuser.ini
 Reads from:
                          C:\Documents and Settings\LocalService\ntuser.ini
                          C:\Documents and Settings\Default User\Templates\amipro.sam
 Reads from:
 Reads from:
                          C:\WINDOWS\system32\noise.enu
 Reads from:
                          C:\Documents and Settings\Default User\Templates\excel.xls
 Reads from:
                          C:\Documents and Settings\Default User\Templates\excel4.xls
 Reads from:
                          C:\Documents and Settings\Default User\Templates\lotus.wk4
 Reads from:
                          C:\Documents and Settings\Default User\Templates\presenta.shw
```

```
C:\Documents and Settings\Default User\Templates\quattro.wb2
 Reads from:
 Reads from:
                          C:\WINDOWS\Prefetch\VERCLSID.EXE-3667BD89.pf
 Reads from:
                          C:\Documents and Settings\Default User\Templates\winword.doc
                          C:\Documents and Settings\Default User\Templates\winword2.doc
 Reads from:
 Reads from:
                          C:\Documents and Settings\Default User\Templates\wordpfct.wpd
 Reads from:
                          C:\Documents and Settings\Default User\Templates\wordpfct.wpg
                          C:\Documents and Settings\Default User\Start Menu\desktop.ini
 Reads from:
 Reads from:
                          C:\Documents and Settings\Default User\Start Menu\Programs\desktop.ini
 Reads from:
                          C:\Documents and Settings\Default User\Start Menu\Programs\Remote
Assistance.lnk
 Reads from:
                          C:\Documents and Settings\Default User\Start Menu\Programs\Windows Media
Player.lnk
 Reads from:
                          C:\Documents and Settings\Default User\Start
Menu\Programs\Startup\desktop.ini
 Reads from:
                          C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Command Prompt.lnk
                         C:\Documents and Settings\Default User\Start
 Reads from:
Menu\Programs\Accessories\desktop.ini
 Reads from:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Notepad.lnk
 Reads from:
                          C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Program Compatibility Wizard.lnk
 Reads from:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Synchronize.lnk
 Reads from:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Tour Windows XP.lnk
                          C:\Documents and Settings\Default User\Start
 Reads from:
Menu\Programs\Accessories\Windows Explorer.lnk
                         C:\Documents and Settings\Default User\Start
 Reads from:
Menu\Programs\Accessories\Entertainment\desktop.ini
                         C:\Documents and Settings\Default User\Start
 Reads from:
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
                          C:\Documents and Settings\Default User\Start
 Reads from:
Menu\Programs\Accessories\Accessibility\desktop.ini
                         {\tt C:\Documents\ and\ Settings\backslash Default\ User\backslash Start}
 Reads from:
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
                         C:\Documents and Settings\Default User\Start
 Reads from:
Menu\Programs\Accessories\Accessibility\Narrator.lnk
                          C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
 Reads from:
                         C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
                         C:\Documents and Settings\Default User\SendTo\desktop.ini
 Reads from:
 Reads from:
                          C:\Documents and Settings\Default User\SendTo\Compressed (zipped)
Folder.ZFSendToTarget
                         C:\Documents and Settings\All Users\Start Menu\Set Program Access and
 Reads from:
Defaults.lnk
 Reads from:
                          C:\Documents and Settings\All Users\Start Menu\desktop.ini
                          C:\Documents and Settings\All Users\Start Menu\Windows Catalog.lnk
 Reads from:
 Reads from:
                          C:\Documents and Settings\All Users\Start Menu\Windows Update.lnk
                          C:\Documents and Settings\All Users\Start Menu\Programs\Adobe Reader
 Reads from:
9.1nk
                          C:\Documents and Settings\All Users\Documents\desktop.ini
 Reads from:
                          C:\Documents and Settings\All Users\Start Menu\Programs\desktop.ini
 Reads from:
 Reads from:
                          C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office
Excel Viewer.lnk
                          C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office
 Reads from:
Word Viewer 2003.lnk
                          {\tt C:\Documents\ and\ Settings\All\ Users\Start\ Menu\Programs\Microsoft}
 Reads from:
PowerPoint Viewer .lnk
 Reads from:
                          C:\Documents and Settings\All Users\Start Menu\Programs\MSN.lnk
 Reads from:
                          C:\Documents and Settings\All Users\Start Menu\Programs\Windows
Messenger.lnk
 Reads from:
                          C:\Documents and Settings\All Users\Start Menu\Programs\Windows Movie
Maker.lnk
 Reads from:
                          C:\Documents and Settings\All Users\Start
Menu\Programs\Startup\desktop.ini
                          \label{lem:c:locuments} C:\Documents\ and\ Settings\All\ Users\Start\ Menu\Programs\Python\ 2.7\IDLE
 Reads from:
(Python GUI).lnk
 Reads from:
                          C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Module Docs.lnk
                          C:\Documents and Settings\All Users\Start Menu\Programs\Python
 Reads from:
2.7\Pvthon (command line).lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python for Windows Documentation.lnk
                          C:\Documents and Settings\All Users\Start Menu\Programs\Python
 Reads from:
2.7\Python Manuals.lnk
                          C:\Documents and Settings\All Users\Start Menu\Programs\Python
 Reads from:
2.7\PythonWin.lnk
                          C:\Documents and Settings\All Users\Start Menu\Programs\Python
 Reads from:
2.7\Uninstall Python.lnk
                          C:\Documents and Settings\All Users\Start
 Reads from:
Menu\Programs\Games\desktop.ini
```

```
Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Freecell.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Hearts.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Backgammon.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Checkers.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
 Reads from:
Hearts.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Reversi.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Spades.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Minesweeper.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Pinball.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Solitaire.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Games\Spider
 Reads from:
Solitaire.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Component Services.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\desktop.ini
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Reads from:
Tools\Computer Management.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Reads from:
Tools\Data Sources (ODBC).lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Reads from:
Tools\Event Viewer.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Reads from:
Tools\Local Security Policy.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Performance.lnk
                         C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
 Reads from:
Tools\Services.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Calculator.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\desktop.ini
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Paint.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Remote Desktop Connection.lnk
                         C:\Documents and Settings\All Users\Start
 Reads from:
Menu\Programs\Accessories\WordPad.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Svstem Tools\Activate Windows.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\desktop.ini
                         C:\Documents and Settings\All Users\Start
 Reads from:
Menu\Programs\Accessories\System Tools\Backup.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Character Map.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Disk Cleanup.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Disk Defragmenter.lnk
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Files and Settings Transfer Wizard.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Scheduled Tasks.lnk
                         C:\Documents and Settings\All Users\Start
 Reads from:
Menu\Programs\Accessories\System Tools\Security Center.lnk
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\System Information.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\System Restore.lnk
                         C:\Documents and Settings\Default User\SendTo\Desktop (create
 Reads from:
shortcut).DeskLink
                         C:\Documents and Settings\Default User\SendTo\Mail Recipient.MAPIMail
 Reads from:
 Reads from:
                         C:\Documents and Settings\Default User\Cookies\index.dat
 Reads from:
                         C:\Documents and Settings\All Users\ntuser.pol
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\Sound Recorder.lnk
                         C:\Documents and Settings\All Users\Documents\Mv Videos\Desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Pictures\Desktop.ini
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\desktop.ini
```

C:\Documents and Settings\All Users\Documents\My Pictures\Sample

Reads from:

```
Pictures\Blue hills.jpg
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Sunset.ipg
                         C:\Documents and Settings\All Users\Documents\My Pictures\Sample
 Reads from:
Pictures\Water lilies.jpg
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Winter.jpg
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Music\Desktop.ini
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst1.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Playlists\000C5A7A\Plylst10.wpl
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst11.wpl
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst12.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Playlists\000C5A7A\Plylst13.wpl
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst14.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Playlists\000C5A7A\Plylst15.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Playlists\000C5A7A\Plylst2.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Playlists\000C5A7A\Plylst3.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Playlists\000C5A7A\Plylst4.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Playlists\000C5A7A\Plylst5.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Playlists\000C5A7A\Plylst6.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Playlists\000C5A7A\Plylst7.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Playlists\000C5A7A\Plylst8.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Playlists\000C5A7A\Plylst9.wpl
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
 Reads from:
Music\desktop.ini
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\Internet}
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
                         C:\Program Files\Internet Explorer\iexplore.exe
 Reads from:
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Music\Sample
Music\Beethoven's Symphony No. 9 (Scherzo).wma
                         C:\Documents and Settings\All Users\Documents\My Music\Sample Music\New
 Reads from:
Stories (Highway Blues).wma
 Reads from:
                         C:\Documents and Settings\All Users\Desktop\Adobe Reader 9.lnk
                         C:\Program Files\Internet Explorer\iexplore.vir
 Reads from:
 Reads from:
                         C:\Documents and Settings\Administrator\ntuser.ini
                         C:\Documents and Settings\Administrator\Templates\amipro.sam
 Reads from:
                         C:\Documents and Settings\Administrator\Templates\excel.xls
 Reads from:
 Reads from:
                         C:\Documents and Settings\Administrator\Start Menu\Programs\Windows
Media Player.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start Menu\desktop.ini
 Reads from:
                         C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Startup\desktop.ini
 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
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Notepad.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Program Compatibility Wizard.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Synchronize.lnk
 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
                         C:\Documents and Settings\Administrator\Start
 Reads from:
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\Accessibility\desktop.ini
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk
 Reads from:
                         C:\Documents and Settings\Administrator\Start
```

```
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
                         C:\Documents and Settings\Administrator\Start
 Reads from:
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
                         C:\Documents and Settings\Administrator\SendTo\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Administrator\SendTo\Compressed (zipped)
Folder.ZFSendToTarget
 Reads from:
                         C:\Documents and Settings\Administrator\SendTo\Desktop (create
shortcut).DeskLink
                         C:\Documents and Settings\Administrator\SendTo\Mail Recipient.MAPIMail
 Reads from:
 Reads from:
                         C:\Documents and Settings\Administrator\Cookies\index.dat
 Reads from:
                         C:\Documents and Settings\Admin\ntuser.ini
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Templates\amipro.sam}
 Reads from:
                         C:\Documents and Settings\Admin\Templates\excel.xls
                         C:\Documents and Settings\Admin\Templates\excel4.xls
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Templates\lotus.wk4
                         C:\Documents and Settings\Admin\Templates\presenta.shw
 Reads from:
                         C:\Documents and Settings\Admin\Templates\quattro.wb2
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Templates\winword.doc
 Reads from:
                         C:\Documents and Settings\Admin\Templates\winword2.doc
                         {\tt C:\Documents\ and\ Settings\Admin\Templates\wordpfct.wpd}
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Templates\wordpfct.wpg
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\desktop.ini
                         C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Internet
Explorer.lnk
                         C:\Documents and Settings\Admin\Start Menu\Programs\Outlook Express.lnk
 Reads from:
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Start\ Menu\Programs\Remote}
Assistance.lnk
                         C:\Documents and Settings\Admin\Start Menu\Programs\Windows Media
 Reads from:
Player.lnk
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\Programs\Startup\desktop.ini
 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\desktop.ini
 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\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
                         C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Tour
 Reads from:
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\Accessories\System
Tools\Internet Explorer (No Add-ons).lnk
                         C:\Documents and Settings\Admin\Start
 Reads from:
Menu\Programs\Accessories\Entertainment\desktop.ini
                        C:\Documents and Settings\Admin\Start
 Reads from:
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
                        C:\Documents and Settings\Admin\Start
 Reads from:
Menu\Programs\Accessories\Accessibility\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
                         C:\Documents and Settings\Admin\Start
 Reads from:
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
                         C:\Documents and Settings\Admin\SendTo\desktop.ini
 Reads from:
 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\All Users\Start
Menu\Programs\Accessories\Entertainment\Volume Control.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\desktop.ini
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\HyperTerminal.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Network Connections.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Network Setup Wizard.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\New Connection Wizard.lnk
 Reads from:
                         C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Wireless Network Setup Wizard.lnk
```

C:\Documents and Settings\All Users\Start

Reads from:

```
Menu\Programs\Accessories\Accessibility\Accessibility Wizard.lnk
                         C:\Documents and Settings\All Users\Start
 Reads from:
Menu\Programs\Accessories\Accessibility\desktop.ini
                         C:\Documents and Settings\All Users\DRM\drmv2.lic
 Reads from:
 Reads from:
                         C:\Documents and Settings\All Users\DRM\drmv2.sst
 Reads from:
                         C:\Documents and Settings\Admin\SendTo\Mail Recipient.MAPIMail
 Reads from:
                          C:\Documents and Settings\Admin\SendTo\My Documents.mydocs
                          C:\Documents and Settings\Admin\Recent\Desktop.ini
 Reads from:
                         {\tt C:\Documents\ and\ Settings\Admin\Favorites\Microsoft\ Websites\IE\ Add-on}
 Reads from:
site.url
 Reads from:
                          C:\Documents and Settings\Admin\Favorites\Desktop.ini
 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\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:
                         {\tt C:\Documents\ and\ Settings\Admin\Favorites\Links\Web\ Slice\ Gallery.url}
 Reads from:
                          C: \verb|\Documents| and Settings\\| Admin\\| Cookies\\| admin\\| @search.microsoft[1].txt
 Reads from:
                          C:\Documents and Settings\Admin\Cookies\index.dat
 Reads from:
                          C:\AUTOEXEC.BAT
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\dotnetfx35setup[1].exe
 Reads from:
                         C:\boot.ini
 Reads from:
                          C:\CONFIG.SYS
 Reads from:
                         C:\System Volume Information\catalog.wci\00010001.ci
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\IE8-WindowsXP-x86-ENU[1].exe
 Reads from:
                         C:\exception.log
                         C:\10.SYS
 Reads from:
 Reads from:
                         C:\MSDOS.SYS
 Reads from:
                         C:\NTDETECT.COM
 Reads from:
                         C:\ntldr
 Reads from:
                         C:\WINDOWS\0.log
 Reads from:
                         C:\WINDOWS\Blue Lace 16.bmp
 Reads from:
                         C:\WINDOWS\bootstat.dat
 Reads from:
                          C:\WINDOWS\explorer.exe
 Reads from:
                         C:\WINDOWS\explorer.scf
                         C:\WINDOWS\FaxSetup.log
 Reads from:
 Reads from:
                          C:\WINDOWS\FeatherTexture.bmp
 Reads from:
                         C:\WINDOWS\Gone Fishing.bmp
                         C:\WINDOWS\Greenstone.bmp
 Reads from:
 Reads from:
                          C:\WINDOWS\hh.exe
 Reads from:
                         C:\WINDOWS\ie8.log
 Reads from:
                          C:\WINDOWS\ie8 main.log
                          C:\WINDOWS\iis6.log
 Reads from:
 Reads from:
                         C:\WINDOWS\imsins.BAK
 Reads from:
                         C:\WINDOWS\imsins.log
                          C:\WINDOWS\MedCtrOC.log
 Reads from:
 Reads from:
                         C:\WINDOWS\msdfmap.ini
 Reads from:
                          C:\WINDOWS\msgsocm.log
                          C:\WINDOWS\system32\drivers\etc\hosts
 Reads from:
 Reads from:
                          C:\WINDOWS\system32\rsaenh.dll
 Reads from:
                          C:\WINDOWS\msmqinst.log
 Reads from:
                          C:\WINDOWS\netfxocm.log
 Reads from:
                          C:\WINDOWS\NOTEPAD.EXE
                          C:\WINDOWS\ntbtlog.txt
 Reads from:
 Deletes:
                          C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.vir
 Deletes:
                          C:\WINDOWS\system32\cisvc.vir
 Deletes:
                          C:\WINDOWS\system32\clipsrv.vir
 Deletes:
                          C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.vir
 Deletes:
                          C:\WINDOWS\system32\dmadmin.vir
                          C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication
 Deletes:
Foundation\infocard.vir
                          C:\System Volume Information\catalog.wci\0000001.ps1
 Deletes:
 Deletes:
                          C:\WINDOWS\system32\imapi.vir
 Deletes:
                          C:\System Volume Information\catalog.wci\00000001.ps2
 Deletes:
                          C:\WINDOWS\system32\mnmsrvc.vir
 Deletes:
                          C:\WINDOWS\system32\msiexec.vir
 Deletes:
                          C:\WINDOWS\system32\netdde.vir
                          C:\Program Files\Common Files\Microsoft Shared\Source Engine\ose.vir
 Deletes:
 Deletes:
                          C:\WINDOWS\system32\sessmgr.vir
                          C:\WINDOWS\system32\locator.vir
 Deletes:
 Deletes:
                          C:\WINDOWS\system32\scardsvr.vir
```

C:\WINDOWS\system32\smlogsvc.vir

C:\Program Files\Internet Explorer\iexplore.vir

C:\WINDOWS\system32\vssvc.vir
C:\WINDOWS\system32\wbem\wmiapsrv.vir

Deletes:

Deletes:

Deletes: Deletes: Deletes: C:\System Volume Information\catalog.wci\CiFLfffd.000
Deletes: C:\System Volume Information\catalog.wci\CiFLfffd.001
Deletes: C:\System Volume Information\catalog.wci\CiFLfffd.002

## Windows Registry Events

Creates key: HKU\.default\software\microsoft\multimedia\audio

Creates key: HKU\.default\software\microsoft\multimedia\audio compression manager\

Creates key: HKU\.default\software\microsoft\multimedia\audio compression

manager\msacm

Creates key: HKU\.default\software\microsoft\multimedia\audio compression

manager\priority v4.00

Creates key: HKLM\software\classes
Creates key: HKCR\msidxs
Creates key: HKCR\msidxs\clsid

Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7\}
Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7\}\progid

Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-

00c04fd611d7}\versionindependentprogid

Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\inprocserver32 Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\ole db provider

Creates key: HKCR\msidxs errorlookup
Creates key: HKCR\msidxs errorlookup\clsid

Creates key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7} Creates key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\progid

Creates key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-

00c04fd611d7}\versionindependentprogid

Creates key:  $\label{eq:hkcrclsid} \mbox{HKCR\clsid\ff9ae8981-7e52-11d0-8964-00c04fd611d7}\nprocserver32 \\ \mbox{Creates key:} \mbox{HKCR\clsid\ff9ae8980-7e52-11d0-8964-00c04fd611d7}\extendederrors$ 

Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\extendederrors\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\
Creates key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\
Creates key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\progid

Creates key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-

00c04fc2f410}\versionindependentprogid

Creates key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\inprocserver32

Creates key: HKLM\system\currentcontrolset\contentindexcommon

Creates key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4\}
Creates key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4\}\inprocserver32

Creates key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}

Creates key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprocserver32

Creates key: HKCR\clsid\{098f2470-bae0-11cd-b579-08002b30bfeb}

Creates key: HKCR\clsid\{098f2470-bae0-11cd-b579-

08002b30bfeb}\persistentaddinsregistered

Creates key: HKCR\clsid\{098f2470-bae0-11cd-b579-

08002b30bfeb}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af} Creates key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}

Creates key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprocserver32

Creates key: HKCR\.386

Creates key: HKCR\.386\persistenthandler

Creates key: HKCR\.audiocd

Creates key: HKCR\.audiocd\persistenthandler

Creates key: HKCR\.desklink

Creates key: HKCR\.desklink\persistenthandler

Creates key: HKCR\.folder

Creates key: HKCR\.folder\persistenthandler

Creates key: HKCR\.mapimail

Creates key: HKCR\.mapimail\persistenthandler

Creates key: HKCR\.zfsendtotarget

Creates key: HKCR\.zfsendtotarget\persistenthandler

Creates key: HKCR\.aif

Creates key: HKCR\.aif\persistenthandler

Creates key: HKCR\.aifc

Creates key: HKCR\.aifc\persistenthandler

Creates key: HKCR\.aiff

Creates key: HKCR\.aiff\persistenthandler

Creates key: HKCR\.aps

Creates key: HKCR\.aps\persistenthandler

Creates key: HKCR\.asf

Creates key: HKCR\.asf\persistenthandler
Creates key: HKCR\.asx

Creates key: HKCR\.asx\persistenthandler
Creates key: HKCR\.au

Creates key: HKCR\.au\persistenthandler

Creates key: HKCR\.avi

Creates key: HKCR\.avi\persistenthandler

Creates key: HKCR\clsid\{00022602-0000-0000-c000-00000000046}\persistenthandler

Creates key: HKCR\.bin

Creates key: HKCR\.bin\persistenthandler

Creates key: HKCR\.bkf

Creates key: HKCR\.bkf\persistenthandler

Creates key: HKCR\.bmp

Creates key: HKCR\.bmp\persistenthandler

```
HKCR \ clsid \ \{d3e34b21-9d75-101a-8c3d-00aa001a1652\} \ \ persistent handler
Creates key:
Creates key:
                                              HKCR\.bsc
Creates key:
                                              HKCR\.bsc\persistenthandler
                                              HKCR\.cab
Creates key:
Creates key:
                                              HKCR\.cab\persistenthandler
Creates key:
                                              HKCR \verb|\clsid| \{0cd7a5c0-9f37-11ce-ae65-08002b2e1262\} \verb|\clsid| \{0cd7a5c0-9f37-11ce-ae65-08002b2e12622\} \verb|\clsid| \{0cd7a5c0-9f37-11ce-ae65-08002b2e12622\} \verb|\clsid| \{0cd7a5c0-9f37-11c
Creates key:
                                              HKCR\.cda
                                              HKCR\.cda\persistenthandler
Creates key:
Creates key:
                                              HKCR\.cgm
Creates key:
                                              HKCR\.cgm\persistenthandler
Creates key:
                                              HKCR\.com
Creates key:
                                              HKCR\.com\persistenthandler
Creates key:
                                              HKCR\.cpl
Creates key:
                                              HKCR\.cpl\persistenthandler
Creates key:
                                              HKCR\.cur
Creates key:
                                              HKCR\.cur\persistenthandler
Creates key:
                                              HKCR\.dbg
Creates key:
                                              HKCR\.dbg\persistenthandler
Creates key:
                                              HKCR\.dct
                                              HKCR\.dct\persistenthandler
Creates key:
Creates key:
                                              HKCR\.dib
Creates key:
                                              HKCR\.dib\persistenthandler
Creates kev:
                                              HKCR\.dl
Creates key:
                                              HKCR\.dl_\persistenthandler
Creates key:
                                              HKCR\.dll
                                              HKCR\.dll\persistenthandler
Creates key:
Creates key:
                                              HKCR\.drv
Creates key:
                                              HKCR\.drv\persistenthandler
                                              HKCR\.dvd
Creates key:
Creates key:
                                              HKCR\.dvd\persistenthandler
Creates key:
                                              HKCR\.emf
                                              HKCR\.emf\persistenthandler
Creates key:
Creates key:
                                              HKCR\.eps
Creates key:
                                              HKCR\.eps\persistenthandler
Creates key:
                                              HKCR\.ex_
Creates key:
                                              HKCR\.ex_\persistenthandler
Creates key:
                                              HKCR\.exe
Creates key:
                                              HKCR\.exe\persistenthandler
Creates key:
                                              HKCR\.exp
                                              HKCR\.exp\persistenthandler
Creates key:
Creates key:
                                              HKCR\.eyb
Creates key:
                                              HKCR\.eyb\persistenthandler
Creates kev:
                                              HKCR\.fnd
Creates key:
                                              HKCR\.fnd\persistenthandler
Creates key:
                                              HKCR\.fnt
                                              HKCR\.fnt\persistenthandler
Creates key:
Creates key:
                                              HKCR\.fon
Creates key:
                                              HKCR\.fon\persistenthandler
Creates key:
                                              HKCR\.ghi
Creates key:
                                              HKCR\.ghi\persistenthandler
Creates key:
                                              HKCR\.gif
                                              HKCR\.gif\persistenthandler
Creates key:
                                              Creates key:
Creates key:
                                              HKCR\.gz\persistenthandler
Creates key:
Creates key:
                                              HKCR\.hqx
Creates key:
                                              HKCR\.hqx\persistenthandler
Creates key:
                                              HKCR\.icm
Creates key:
                                              HKCR\.icm\persistenthandler
Creates key:
                                              HKCR\.ico
Creates key:
                                              HKCR\.ico\persistenthandler
Creates key:
                                              HKCR\.idb
Creates key:
                                              HKCR\.idb\persistenthandler
                                              HKCR\.ilk
Creates kev:
Creates key:
                                              HKCR\.ilk\persistenthandler
Creates key:
                                              HKCR\.imc
Creates key:
                                              HKCR\.imc\persistenthandler
Creates key:
                                              HKCR\.in_
Creates key:
                                              HKCR\.in_\persistenthandler
Creates kev:
                                              HKCR\.inv
Creates key:
                                              HKCR\.inv\persistenthandler
                                              HKCR\.ivf
Creates key:
Creates key:
                                              HKCR\.ivf\persistenthandler
Creates key:
                                              HKCR\.jbf
Creates key:
                                              HKCR\.jbf\persistenthandler
Creates key:
                                              HKCR\.jfif
Creates key:
                                              HKCR\.jfif\persistenthandler
Creates key:
                                              HKCR\.jpe
Creates key:
                                              HKCR\.jpe\persistenthandler
Creates key:
                                              HKCR\.jpeg
Creates key:
                                              HKCR\.jpeg\persistenthandler
Creates key:
                                              HKCR\.jpg
```

HKCR\.jpg\persistenthandler

Creates key:

```
HKCR\.latex
Creates key:
Creates key:
                         HKCR\.latex\persistenthandler
Creates key:
                         HKCR\.lib
Creates key:
                         HKCR\.lib\persistenthandler
Creates key:
                         HKCR\.m14
Creates key:
                         HKCR\.m14\persistenthandler
Creates key:
                         HKCR\.m1v
                         HKCR\.m1v\persistenthandler
Creates key:
Creates key:
                         HKCR\.m3u
Creates key:
                         HKCR\.m3u\persistenthandler
Creates key:
                         HKCR\.mdb
Creates key:
                         HKCR\.mdb\persistenthandler
Creates key:
                         HKCR\.mid
                         HKCR\.mid\persistenthandler
Creates key:
                         Creates key:
Creates key:
                         HKCR\.midi
Creates key:
                         HKCR\.midi\persistenthandler
Creates key:
                         HKCR\.mmf
Creates key:
                         HKCR\.mmf\persistenthandler
Creates key:
                         HKCR\.mov
Creates key:
                         HKCR\.mov\persistenthandler
Creates key:
                         HKCR\.movie
Creates kev:
                         HKCR\.movie\persistenthandler
Creates key:
                         HKCR\.mp2
Creates key:
                         HKCR\.mp2\persistenthandler
                         HKCR\.mp2v
Creates key:
Creates key:
                         HKCR\.mp2v\persistenthandler
Creates key:
                         HKCR\.mp3
                         HKCR\.mp3\persistenthandler
Creates key:
Creates key:
                         HKCR\.mpa
Creates key:
                         HKCR\.mpa\persistenthandler
Creates key:
                         HKCR\.mpe
Creates key:
                         HKCR\.mpe\persistenthandler
Creates key:
                         HKCR\.mpeg
                         HKCR\.mpeg\persistenthandler
Creates key:
                         HKCR\.mpg
Creates key:
Creates key:
                         HKCR\.mpg\persistenthandler
Creates key:
                         HKCR\.mpv2
Creates key:
                         HKCR\.mpv2\persistenthandler
Creates key:
                         HKCR\.msg
                         {\tt HKCR} \verb|\|.msg\persistenthandler|
Creates key:
Creates key:
                         HKCR\.mv
                         HKCR\.mv\persistenthandler
Creates kev:
Creates key:
                         HKCR\.mydocs
Creates key:
                         HKCR\.mydocs\persistenthandler
                         HKCR\.ncb
Creates key:
Creates key:
                         HKCR\.ncb\persistenthandler
                         HKCR\.obj
Creates key:
Creates key:
                         HKCR\.obj\persistenthandler
Creates key:
                         HKCR\.oc_
Creates key:
                         HKCR\.oc_\persistenthandler
Creates key:
                         HKCR\.ocx
Creates key:
                         HKCR\.ocx\persistenthandler
Creates key:
                         HKCR\.pch
Creates key:
                         HKCR\.pch\persistenthandler
Creates key:
                         HKCR\.pdb
Creates key:
                         HKCR\.pdb\persistenthandler
Creates key:
                         HKCR\.pds
Creates key:
                         HKCR\.pds\persistenthandler
Creates key:
                         HKCR\.pic
Creates key:
                         HKCR\.pic\persistenthandler
Creates key:
                         HKCR\.pma
Creates key:
                         HKCR\.pma\persistenthandler
Creates key:
                         HKCR\.pmc
                         HKCR\.pmc\persistenthandler
Creates key:
Creates key:
                         HKCR\.pml
Creates key:
                         HKCR\.pml\persistenthandler
Creates key:
                         HKCR\.pmr
Creates key:
                         HKCR\.pmr\persistenthandler
                         HKCR\.png
Creates kev:
Creates key:
                         HKCR\.png\persistenthandler
Creates key:
                         HKCR\.psd
Creates key:
                         HKCR\.psd\persistenthandler
Creates key:
                         HKCR\.res
Creates key:
                         HKCR\.res\persistenthandler
Creates kev:
                         HKCR\.rle
Creates key:
                         HKCR\.rle\persistenthandler
Creates key:
                         HKCR\.rmi
Creates key:
                         HKCR\.rmi\persistenthandler
Creates key:
                         HKCR\.rpc
Creates key:
                         HKCR\.rpc\persistenthandler
Creates key:
                         HKCR\.rsp
```

HKCR\.rsp\persistenthandler

Creates key:

```
HKCR\.sbr
 Creates key:
 Creates key:
                         HKCR\.sbr\persistenthandler
 Creates key:
                         HKCR\.sc2
 Creates key:
                         HKCR\.sc2\persistenthandler
 Creates key:
                         HKCR\.sit
 Creates key:
                         HKCR\.sit\persistenthandler
 Creates key:
                         HKCR\.snd
                         HKCR\.snd\persistenthandler
 Creates key:
 Creates key:
                         HKCR\.sr_
 Creates key:
                         HKCR\.sr_\persistenthandler
 Creates key:
                         HKCR\.sy_
 Creates key:
                         HKCR\.sy_\persistenthandler
 Creates key:
                         HKCR\.sym
 Creates key:
                         HKCR\.sym\persistenthandler
 Creates key:
                         HKCR\.sys
 Creates key:
                         HKCR\.sys\persistenthandler
 Creates key:
                         HKCR\.tar
 Creates key:
                         HKCR\.tar\persistenthandler
 Creates key:
                         HKCR\.tgz
                         HKCR\.tgz\persistenthandler
 Creates key:
 Creates key:
                         HKCR\.tif
 Creates key:
                         HKCR\.tif\persistenthandler
 Creates key:
                         HKCR\.tiff
 Creates key:
                         HKCR\.tiff\persistenthandler
 Creates key:
                         HKCR\.tlb
 Creates key:
                         HKCR\.tlb\persistenthandler
 Creates key:
                         HKCR\.tsp
 Creates key:
                         HKCR\.tsp\persistenthandler
 Creates key:
                         HKCR\.ttc
 Creates key:
                         HKCR\.ttc\persistenthandler
 Creates key:
                         HKCR\.ttf
                         HKCR\.ttf\persistenthandler
 Creates key:
 Creates key:
                         HKCR\.vbx
 Creates key:
                         HKCR\.vbx\persistenthandler
 Creates key:
                         HKCR\.vxd
 Creates key:
                         HKCR\.vxd\persistenthandler
 Creates key:
                         HKCR\.wav
 Creates key:
                         HKCR\.wav\persistenthandler
 Creates key:
                         HKCR\.wax
 Creates key:
                         HKCR\.wax\persistenthandler
 Creates key:
 Creates key:
                         HKCR\.wll
                         HKCR\.wll\persistenthandler
 Creates kev:
 Creates key:
                         HKCR\.wlt
 Creates key:
                         HKCR\.wlt\persistenthandler
                         HKCR\.wm
 Creates key:
 Creates key:
                         HKCR\.wm\persistenthandler
 Creates key:
                         HKCR\.wma
 Creates key:
                         HKCR\.wma\persistenthandler
 Creates key:
                         HKCR\.wmf
                         HKCR\.wmf\persistenthandler
 Creates key:
 Creates key:
                         HKCR\.wmp
 Creates key:
                         HKCR\.wmp\persistenthandler
                         HKCR\.wmv
 Creates key:
                         HKCR\.wmv\persistenthandler
 Creates key:
 Creates key:
                         HKCR\.wmx
 Creates key:
                         HKCR\.wmx\persistenthandler
 Creates key:
                         HKCR\.wmz
                         HKCR\.wmz\persistenthandler
 Creates key:
 Creates key:
                         HKCR\.wsz
 Creates key:
                         HKCR\.wsz\persistenthandler
 Creates key:
                         HKCR\.wvx
 Creates key:
                         HKCR\.wvx\persistenthandler
                         HKCR\.xbm
 Creates kev:
 Creates key:
                         HKCR\.xbm\persistenthandler
                         HKCR\.xix
 Creates key:
 Creates key:
                         HKCR\.xix\persistenthandler
 Creates key:
                         HKCR\.z
 Creates key:
                         HKCR\.z\persistenthandler
 Creates kev:
                         HKCR\.z96
 Creates key:
                         HKCR\.z96\persistenthandler
 Creates key:
                         HKCR\.zip
 Creates key:
                         HKCR\.zip\persistenthandler
 Creates key:
                         HKCR\clsid\{e88dcce0-b7b3-11d1-a9f0-00aa0060fa31}\persistenthandler
 Creates key:
                         HKCR\clsid\{5e941d80-bf96-11cd-b579-08002b30bfeb}
                         HKCR\clsid\{5e941d80-bf96-11cd-b579-
 Creates kev:
08002b30bfeb}\persistentaddinsregistered
                         HKCR\clsid\{5e941d80-bf96-11cd-b579-
 Creates key:
08002b30bfeb}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
 Creates key:
                         HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}
 Creates key:
                         HKCR\clsid\{73fddc80-aea9-101a-98a7-00aa00374959}\ \ persistent handler
 Creates key:
 Creates key:
```

```
HKCR\.dic
    Creates key:
    Creates key:
                                                                           HKCR\.dic\persistenthandler
    Creates key:
                                                                           HKCR\.txt
    Creates key:
                                                                           HKCR\.txt\persistenthandler
    Creates key:
                                                                           HKCR\.wtx
    Creates key:
                                                                           HKCR\.wtx\persistenthandler
    Creates key:
                                                                           HKCR\.bat
                                                                           HKCR\.bat\persistenthandler
    Creates key:
    Creates key:
                                                                           HKCR\.cmd
    Creates key:
                                                                           HKCR\.cmd\persistenthandler
    Creates key:
                                                                           HKCR\.ida
    Creates key:
                                                                           HKCR\.idq\persistenthandler
    Creates key:
                                                                           HKCR\.ini
    Creates key:
                                                                           HKCR\.ini\persistenthandler
    Creates key:
                                                                           HKCR\.inx
    Creates key:
                                                                           HKCR\.inx\persistenthandler
    Creates key:
                                                                           HKCR\.reg
    Creates key:
                                                                           HKCR\.reg\persistenthandler
    Creates key:
                                                                           HKCR\.inf
    Creates key:
                                                                           HKCR\.inf\persistenthandler
    Creates key:
                                                                           HKCR\.vbs
    Creates key:
                                                                           HKCR\.vbs\persistenthandler
    Creates key:
                                                                           HKCR\.asm
    Creates key:
                                                                           HKCR\.asm\persistenthandler
    Creates key:
                                                                           HKCR\.c
                                                                           HKCR\.c\persistenthandler
    Creates key:
    Creates key:
                                                                           HKCR\.cpp
    Creates key:
                                                                           HKCR\.cpp\persistenthandler
                                                                           HKCR\.cxx
    Creates kev:
    Creates key:
                                                                           HKCR\.cxx\persistenthandler
    Creates key:
                                                                           HKCR\.def
                                                                           HKCR\.def\persistenthandler
    Creates key:
    Creates key:
                                                                           HKCR\.h
    Creates key:
                                                                           HKCR\.h\persistenthandler
                                                                           HKCR\.hpp
    Creates key:
    Creates key:
                                                                           HKCR\.hpp\persistenthandler
    Creates key:
                                                                           HKCR\.hxx
                                                                           HKCR\.hxx\persistenthandler
    Creates key:
    Creates key:
                                                                           HKCR\.idl
                                                                           HKCR\.idl\persistenthandler
    Creates key:
    Creates key:
                                                                           HKCR\.inc
    Creates key:
                                                                           HKCR\.inc\persistenthandler
    Creates kev:
                                                                           HKCR\.is
    Creates key:
                                                                           HKCR\.js\persistenthandler
    Creates key:
                                                                           HKCR\.log
                                                                           HKCR\.log\persistenthandler
    Creates key:
    Creates key:
                                                                           HKCR\.pl
    Creates key:
                                                                           HKCR\.pl\persistenthandler
    Creates kev:
                                                                           HKCR\.rc
    Creates key:
                                                                           HKCR\.rc\persistenthandler
    Creates key:
                                                                           HKCR\.rtf
                                                                           HKCR\.rtf\persistenthandler
    Creates key:
    Creates key:
                                                                           HKCR\.url
    Creates key:
                                                                           HKCR\.url\persistenthandler
                                                                           HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\persistenthandler
    Creates key:
    Creates key:
                                                                           HKCR\.xml
    Creates key:
                                                                           HKCR\.xml\persistenthandler
    Creates key:
                                                                           HKCR\.xsl
                                                                           HKCR\.xsl\persistenthandler
    Creates key:
                                                                           HKLM\system\currentcontrolset\control\contentindex\language\neutral
    Creates key:
    Creates key:
                                                                           HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}
                                                                           Creates key:
    Creates key:
                                                                           HKCR\clsid\{78fe669a-186e-4108-96e9-77b586c1332f}
    Creates key:
                                                                           HKCR\clsid\{78fe669a-186e-4108-96e9-77b586c1332f}\inprocserver32
                                                                           HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}
    Creates key:
                                                                           HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\inprocserver32
    Creates kev:
    Creates key:
                                                                           HKCR\clsid\{1f247dc0-902e-11d0-a80c-00a0c906241a}
    Creates key:
                                                                           HKCR \ clsid \ \{1f247dc0-902e-11d0-a80c-00a0c906241a\} \ \ inprocserver 32
    Creates key:
                                                                           HKCR\clsid\{c04efa90-e221-11d2-985e-00c04f575153}
    Creates kev:
    Creates key:
                                                                           HKCR\clsid\{c04efa90-e221-11d2-985e-00c04f575153}\inprocserver32
    Creates kev:
                                                                           HKCR\interface
    Creates key:
                                                                           HKCR\interface\{f4eb8260-8dda-11d1-b3aa-00a0c9063796}
                                                                           HKCR\ interface \ \{f4eb8260-8dda-11d1-b3aa-00a0c9063796\} \ proxystubclsid32
    Creates key:
    Creates key:
                                                                           HKCR\ interface \ \{f4eb8260-8dda-11d1-b3aa-00a0c9063796\} \ \ nummethods
                                                                           HKCR\clsid\{95ad72f0-44ce-11d0-ae29-00aa004b9986}
    Creates kev:
    Creates key:
                                                                           HKCR\clsid\{95ad72f0-44ce-11d0-ae29-00aa004b9986}\inprocserver32
                                                                           HKLM \setminus software \setminus microsoft \setminus mmc \setminus snapins \setminus \{95ad72f0-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29
    Creates key:
00aa004b99863
    Creates key:
                                                                           HKLM \setminus software \setminus microsoft \setminus mmc \setminus snapins \setminus \{95ad72f0-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d
00aa004b9986}\extension
                                                                           HKLM \setminus software \setminus microsoft \setminus mmc \setminus snapins \setminus \{95ad72f0-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d
    Creates kev:
```

00aa004b9986}\standalone

```
Creates key:
00aa004b9986}\nodetypes
      Creates key:
                                                                                                HKLM \setminus software \setminus microsoft \setminus mmc \setminus snapins \setminus \{95ad72f0-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d
00aa004b9986}\nodetypes\{5401e3e9-f5f6-11d1-b4f7-00c04fc2db8d}
      Creates kev:
                                                                                                HKLM \setminus software \setminus microsoft \setminus mmc \setminus nodetypes \setminus \{5401e3e9-f5f6-11d1-b4f7-mmc \setminus nodetypes \setminus \{5401e3e9-mmc \setminus nodetypes \setminus \{5401e3e9-mmc \setminus nodetypes \setminus \{5401e3e-mmc \setminus nodetypes \setminus nodetypes \setminus \{5401e3e-mmc \setminus nodetypes \setminus nodetypes \setminus \{5401e3e-mmc \setminus nodetypes \setminus \{5401e3e-mmc \setminus nodetypes \setminus nodetypes \setminus \{5401e3e-mmc \setminus nodetypes \setminus nodetypes \setminus \{5401e3e-mmc \setminus nodetypes \setminus nodetypes \setminus nodetypes \setminus \{5401e3e-mmc \setminus nodetypes \setminus nodetypes \setminus nodetypes \setminus \{5401e3e-mmc \setminus nodetypes 
00c04fc2db8d}
      Creates key:
                                                                                                HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-
00c04fd8d5b0}
      Creates key:
                                                                                                HKLM \setminus software \setminus microsoft \setminus mmc \setminus detypes \setminus \{476e6449 - aaff-11d0 - b944 - aaaff-11d0 - b944 - aaff-11d0 - b944 - aaff-11d0 - b944 - aaff-11d0
00c04fd8d5b0}\extensions
                                                                                                HKLM \setminus software \setminus microsoft \setminus mmc \setminus detypes \setminus \{476e6449 - aaff-11d0 - b944 - aaaff-11d0 - b944 - aaff-11d0 - b944 - aaff-11d0 - b944 - aaff-11d0
     Creates kev:
00c04fd8d5b0}\extensions\namespace
     Creates key:
                                                                                                HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-
00c04fd8d5b0}\dynamic extensions
      Creates key:
                                                                                                HKLM\system\currentcontrolset\control\server applications
      Creates key:
                                                                                                HKCR\ixsso.query
      Creates key:
                                                                                                HKCR\ixsso.query\clsid
      Creates key:
                                                                                                HKCR\ixsso.query\curver
      Creates key:
                                                                                                HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}
                                                                                                Creates key:
      Creates key:
                                                                                                HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}\progid
      Creates key:
                                                                                                HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}\implemented categories
                                                                                               \label{local-equation} \begin{tabular}{ll} HKCR\clsid\\ eafdf8b3-3be5-4e05-bf86-1e486b2fef9d\\ \label{local-equation} \end{tabular} \begin{tabular}{ll} HKCR\clsid\\ \end{tabular} \begin{tabular}{ll} eafdf8b3-3be5-4e05-bf86-1e486b2fef9d\\ \end{tabular} \begin{tabular}{ll} HKCR\clsid\\ \end{tabular} \begin{tabular}{ll} eafdf8b3-3be5-4e05-bf86-1e486b2fef9d\\ \end{tabular} \begin{tabular}{ll} HKCR\clsid\\ \end{tabular} \begin{tabular}{ll} HKCR\clsid\\ \end{tabular} \begin{tabular}{ll} eafdf8b3-3be5-4e05-bf86-1e486b2fef9d\\ \end{tabular} \begin{tabular}{ll} HKCR\clsid\\ \end{tabul
      Creates key:
categories\{7dd95801-9882-11cf-9fa9-00aa006c42c4}
      Creates key:
                                                                                               HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}\implemented
categories\{7dd95802-9882-11cf-9fa9-00aa006c42c4}
      Creates key:
                                                                                                HKCR\ixsso.query.3
      Creates key:
                                                                                                HKCR\ixsso.query.3\clsid
                                                                                                HKCR\ixsso.query.2
      Creates kev:
      Creates key:
                                                                                                HKCR\ixsso.query.2\clsid
      Creates key:
                                                                                                HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}
                                                                                                HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\inprocserver32
      Creates key:
      Creates key:
                                                                                                HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\progid
      Creates key:
                                                                                                HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\implemented categories
                                                                                               HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024\}\implemented
      Creates kev:
categories\{7dd95801-9882-11cf-9fa9-00aa006c42c4}
      Creates key:
                                                                                               HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\implemented
categories\{7dd95802-9882-11cf-9fa9-00aa006c42c4}
      Creates key:
                                                                                                HKCR\ixsso.util
      Creates key:
                                                                                                HKCR\ixsso.util\clsid
                                                                                                HKCR\ixsso.util\curver
      Creates key:
      Creates key:
                                                                                                HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}
      Creates key:
                                                                                                HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\inprocserver32
                                                                                                HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\progid
      Creates key:
      Creates key:
                                                                                                HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\implemented categories
      Creates key:
                                                                                                HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\implemented
categories\{7dd95801-9882-11cf-9fa9-00aa006c42c4}
      Creates key:
                                                                                                categories\{7dd95802-9882-11cf-9fa9-00aa006c42c4}
      Creates key:
                                                                                               HKCR\ixsso.util.2
      Creates key:
                                                                                                HKCR\ixsso.util.2\clsid
      Creates key:
                                                                                                HKCR\clsid\{eec97550-47a9-11cf-b952-00aa0051fe20}
                                                                                               HKCR\clsid\{eec97550-47a9-11cf-b952-
      Creates key:
00aa0051fe20}\persistentaddinsregistered
     Creates kev:
                                                                                               HKCR\clsid\{eec97550-47a9-11cf-b952-
00aa0051fe20}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
      Creates key:
                                                                                                HKCR\clsid\{e0ca5340-4534-11cf-b952-00aa0051fe20}
      Creates key:
                                                                                                HKCR\clsid\{e0ca5340-4534-11cf-b952-00aa0051fe20}\inprocserver32
      Creates key:
                                                                                                HKCR\clsid\{3050f4d8-98b5-11cf-bb82-00aa00bdce0b}\persistenthandler
      Creates key:
                                                                                                HKCR\.odc
      Creates key:
                                                                                                HKCR\.odc\persistenthandler
      Creates key:
                                                                                                HKCR\.hhc
      Creates key:
                                                                                                HKCR\.hhc\persistenthandler
      Creates key:
                                                                                                HKCR\.htm
                                                                                                HKCR\.htm\persistenthandler
      Creates key:
      Creates key:
                                                                                                HKCR\.html
      Creates key:
                                                                                                HKCR\.html\persistenthandler
      Creates key:
                                                                                                HKCR\.htx
      Creates key:
                                                                                                HKCR\.htx\persistenthandler
      Creates key:
                                                                                                HKCR\.stm
      Creates key:
                                                                                                HKCR\.stm\persistenthandler
      Creates key:
                                                                                                HKCR\.htw
      Creates key:
                                                                                                HKCR\.htw\persistenthandler
      Creates key:
                                                                                                HKCR\.asp
      Creates key:
                                                                                                HKCR\.asp\persistenthandler
      Creates kev:
                                                                                                HKCR\.aspx
      Creates key:
                                                                                                HKCR\.aspx\persistenthandler
                                                                                                HKCR\.ascx
      Creates key:
      Creates key:
                                                                                                HKCR\.ascx\persistenthandler
      Creates key:
                                                                                                HKCR\.css
      Creates key:
                                                                                                HKCR\.css\persistenthandler
                                                                                                HKCR\.hta
      Creates kev:
```

HKCR\.hta\persistenthandler

Creates key:

```
HKCR\.htt
    Creates key:
                                                               HKCR\.htt\persistenthandler
    Creates key:
                                                               HKCR\clsid\{98de59a0-d175-11cd-a7bd-00006b827d94}
    Creates key:
                                                               HKCR\clsid\{98de59a0-d175-11cd-a7bd-
    Creates key:
00006b827d94}\persistentaddinsregistered
    Creates key:
                                                              HKCR\clsid\{98de59a0-d175-11cd-a7bd-
00006b827d94}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
                                                              HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}
    Creates key:
                                                               HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\ inprocserver32
    Creates key:
                                                               HKCR\clsid\{00020906-0000-0000-c000-00000000046}
    Creates key:
                                                               \label{localization} \begin{tabular}{ll} HKCR\clsid\{00020906-0000-0000-c000-00000000046}\persistenthandler \\ \end{tabular}
    Creates key:
    Creates key:
                                                               HKCR\clsid\{64818d11-4f9b-11cf-86ea-00aa00b929e8}
    Creates key:
                                                               HKCR \verb|\clsid|{64818d11-4f9b-11cf-86ea-00aa00b929e8} \verb|\clsid|{64818d11-4f9b
                                                               HKCR\clsid\{64818d10-4f9b-11cf-86ea-00aa00b929e8}
    Creates key:
    Creates key:
                                                               HKCR \clsid \end{64818d} 10-4f9b-11cf-86ea-00aa00b929e8 \end{64818d} versistent \end{64818d} here is the substitution of the
    Creates key:
                                                               HKCR\clsid\{00020820-0000-0000-c000-00000000046}
    Creates key:
                                                               HKCR\clsid\{00020820-0000-0000-c000-00000000046}\persistenthandler
    Creates key:
                                                               HKCR\clsid\{00020821-0000-0000-c000-00000000046}
    Creates key:
                                                               Creates key:
                                                               HKCR\clsid\{00020900-0000-0000-c000-00000000046}
    Creates key:
                                                               Creates key:
                                                               HKCR\clsid\{ea7bae70-fb3b-11cd-a903-00aa00510ea3}
    Creates key:
                                                               HKCR\clsid\{ea7bae70-fb3b-11cd-a903-00aa00510ea3}\persistenthandler
    Creates key:
                                                               HKCR\clsid\{ea7bae71-fb3b-11cd-a903-00aa00510ea3}
    Creates key:
                                                               HKCR\clsid\\{ea7bae71-fb3b-11cd-a903-00aa00510ea3}\\{persistenthandler}
    Creates key:
                                                               HKCR\clsid\{00020811-0000-0000-c000-00000000046}
    Creates key:
                                                               Creates key:
                                                               HKCR\clsid\{00020810-0000-0000-c000-00000000046}
                                                               \label{local-bound} \mbox{HKCR\clsid\{00020810-0000-0000-c000-000000000046\}\columnwidth}} \mbox{$\downarrow$ persistenthandler and $\downarrow$ and $\downarrow$ are supported by $\downarrow$ and $\downarrow$ are supported by $\downarrow$ and $\downarrow$ are supported by $\downarrow$ are supported by $\downarrow$ are supported by $\downarrow$ and $\downarrow$ are supported by 
    Creates kev:
    Creates key:
                                                               HKCR\.doc
    Creates key:
                                                               HKCR\.doc\persistenthandler
                                                               HKCR\.dot
    Creates key:
    Creates key:
                                                               HKCR\.dot\persistenthandler
    Creates key:
                                                               HKCR\.pot
    Creates key:
                                                               HKCR\.pot\persistenthandler
    Creates key:
                                                               HKCR\.ppt
    Creates key:
                                                               HKCR\.ppt\persistenthandler
    Creates key:
                                                               HKCR\.pps
    Creates key:
                                                               HKCR\.pps\persistenthandler
    Creates key:
                                                               HKCR\.xlb
    Creates key:
                                                               HKCR\.xlb\persistenthandler
    Creates key:
                                                               HKCR\.xlc
    Creates key:
                                                               HKCR\.xlc\persistenthandler
    Creates key:
                                                              HKCR\.xls
    Creates key:
                                                               HKCR\.xls\persistenthandler
                                                               HKCR\.xlt
    Creates key:
    Creates key:
                                                              HKCR\.xlt\persistenthandler
    Creates key:
                                                               HKCR \c1sid \{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d\}
                                                               HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\progid
    Creates kev:
    Creates key:
                                                              HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-
00c04fc2db8d}\versionindependentprogid
                                                               HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\programmable
    Creates kev:
    Creates key:
                                                               HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
    Creates key:
                                                               HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}
    Creates kev:
                                                               HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\progid
    Creates key:
                                                              HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-
00c04fc2db8d}\versionindependentprogid
                                                              HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\programmable
    Creates key:
    Creates kev:
                                                               HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
    Creates key:
                                                               HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}
    Creates key:
                                                               HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\progid
    Creates key:
                                                              HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-
00c04fc2db8d}\versionindependentprogid
                                                               HKCR\clsid{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\programmable
    Creates kev:
                                                               HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
    Creates key:
    Creates key:
                                                               HKLM\system\currentcontrolset\control\contentindex\language\english_us
    Creates key:
                                                               HKCR\clsid\{eeed4c20-7f1b-11ce-be57-00aa0051fe20}
                                                               HKCR\clsid\\{eeed4c20-7f1b-11ce-be57-00aa0051fe20}\\{inprocserver32}
    Creates key:
    Creates key:
                                                               Creates key:
                                                               HKCR\clsid\{d99f7670-7f1a-11ce-be57-00aa0051fe20}
    Creates key:
                                                              HKCR \c1sid \d99f7670-7f1a-11ce-be57-00aa0051fe20 \nprocserver 32
HKLM\system\currentcontrolset\control\contentindex\language\french french
    Creates key:
                                                              HKCR\clsid\{59e09848-8099-101b-8df3-00000b65c3b5}
    Creates key:
                                                               HKCR\clsid\{59e09848-8099-101b-8df3-00000b65c3b5}\) in procserver 32
                                                               HKCR\clsid\{2a6eb050-7f1c-11ce-be57-00aa0051fe20}
    Creates kev:
    Creates key:
                                                               HKCR\clsid\{2a6eb050-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
    Creates kev:
HKLM\system\currentcontrolset\control\contentindex\language\german_german
    Creates key:
                                                              HKCR\clsid\{9b08e210-e51b-11cd-bc7f-00aa003db18e}
    Creates key:
                                                               HKCR\clsid\{9b08e210-e51b-11cd-bc7f-00aa003db18e}\ \ inprocserver 32
                                                               HKCR\clsid\{510a4910-7f1c-11ce-be57-00aa0051fe20}
    Creates key:
    Creates key:
                                                              HKCR\clsid\{510a4910-7f1c-11ce-be57-00aa0051fe20}\ \ linprocserver 32
```

```
Creates key:
HKLM\system\currentcontrolset\control\contentindex\language\italian_italian
  Creates key:
                                    HKCR\clsid\{fd86b5d0-12c6-11ce-bd31-00aa004bbb1f}
  Creates key:
                                    HKCR\clsid\{fd86b5d0-12c6-11ce-bd31-00aa004bbb1f}\inprocserver32
  Creates kev:
                                    HKCR\clsid\{6d36ce10-7f1c-11ce-be57-00aa0051fe20}
  Creates key:
                                    HKCR \c1sid \end{6d36ce10-7f1c-11ce-be57-00aa0051fe20} \label{eq:hkcr} \\
  Creates key:
HKLM\system\currentcontrolset\control\contentindex\language\swedish_default
                                    HKCR\clsid\{01c6b350-12c7-11ce-bd31-00aa004bbb1f}
  Creates key:
  Creates key:
                                    HKCR\clsid\{01c6b350-12c7-11ce-bd31-00aa004bbb1f}\inprocserver32
  Creates key:
                                    HKCR\clsid\{9478f640-7f1c-11ce-be57-00aa0051fe20}
  Creates key:
                                    HKCR \c1sid \end{9478f640-7f1c-11ce-be57-00aa0051fe20} \label{eq:hkcr} \\
  Creates key:
Creates key:
                                    HKCR\clsid\{0285b5c0-12c7-11ce-bd31-00aa004bbb1f}
                                    HKCR\clsid\{0285b5c0-12c7-11ce-bd31-00aa004bbb1f}\inprocserver32
  Creates key:
  Creates key:
                                    HKCR\clsid\{b0516ff0-7f1c-11ce-be57-00aa0051fe20}
  Creates key:
                                    HKCR\clsid\{b0516ff0-7f1c-11ce-be57-00aa0051fe20}\
  Creates key:
                                    {\tt HKLM \ } .
                                    HKCR\clsid\{66b37110-8bf2-11ce-be59-00aa0051fe20}
  Creates key:
  Creates key:
                                    HKCR\clsid\{66b37110-8bf2-11ce-be59-00aa0051fe20}\inprocserver32
                                    HKCR\clsid\{860d28d0-8bf4-11ce-be59-00aa0051fe20}
  Creates key:
  Creates key:
                                    HKCR\clsid\{860d28d0-8bf4-11ce-be59-00aa0051fe20}\inprocserver32
  Creates key:
                                    HKCR\.nws
  Creates key:
                                    HKCR\microsoft internet news message
                                    HKCR\microsoft internet news message\clsid
  Creates key:
  Creates key:
                                    HKCR\clsid\{5645c8c0-e277-11cf-8fda-00aa00a14f93}
                                    HKCR\clsid\{5645c8c0-e277-11cf-8fda-00aa00a14f93}\persistenthandler
  Creates key:
                                    HKCR\clsid\{5645c8c1-e277-11cf-8fda-
  Creates kev:
00aa00a14f93\} \\ persistent add in sregistered \\ \{89bcb740-6119-101a-bcb7-00dd010655af\} \\
  Creates key:
                                    HKCR\clsid\{5645c8c2-e277-11cf-8fda-00aa00a14f93}\inprocserver32
  Creates key:
                                    HKCR\.eml
  Creates key:
                                    HKCR\microsoft internet mail message
  Creates key:
                                    HKCR\microsoft internet mail message\clsid
  Creates key:
                                    HKCR\clsid\{5645c8c3-e277-11cf-8fda-00aa00a14f93}
  Creates key:
                                    HKCR\clsid\{5645c8c3-e277-11cf-8fda-00aa00a14f93}\persistenthandler
  Creates key:
                                    HKCR\clsid\{5645c8c4-e277-11cf-8fda-
00aa00a14f93\} \\ persistent add in sregistered \\ \{89bcb740-6119-101a-bcb7-00dd010655af\} \\
  Creates key:
                                    HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}
  Creates key:
                                    HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\progid
  Creates kev:
                                    HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-
0090272fa362}\versionindependentprogid
  Creates key:
                                    HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserver32
                                    HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}
  Creates key:
  Creates key:
                                    HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}\progid
  Creates key:
                                    HKCR\clsid\{363f1015-fd5f-4ba8-ac58-
29634f378a42}\versionindependentprogid
  Creates key:
                                    HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}
  Creates kev:
                                    HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\progid
  Creates key:
  Creates key:
                                    HKCR\clsid\{f14e6b48-fbca-4d32-bd79-
7829d4f7e43b}\versionindependentprogid
                                    HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\inprocserver32
  Creates key:
  Creates key:
                                    HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}
  Creates key:
                                    HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\progid
                                    HKCR\clsid\{91870674-de84-4313-b07d-
  Creates key:
a387415bb4f5}\versionindependentprogid
                                    HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\inprocserver32
  Creates kev:
                                    HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}
  Creates kev:
  Creates key:
                                    HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\progid
  Creates key:
                                    HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-
c4825abbe5cf}\versionindependentprogid
                                    HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\inprocserver32
  Creates key:
  Creates key:
HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| explorer \verb|\| mountpoints 2 \verb|\| mountpoints 2 \verb|\| current version and a current version a
  Creates key:
                                    HKLM\software\microsoft\windows\currentversion\shell extensions\blocked
  Creates key:
                                    HKU\.default\software\microsoft\windows\currentversion\shell
extensions\blocked
  Creates key:
                                    HKLM\software\microsoft\windows\currentversion\shell extensions\cached
  Creates key:
                                    HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached
  Creates key:
                                    HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
  Creates key:
                                    HKU\.default\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
  Creates kev:
                                    HKLM\software\microsoft\wbem\cimom
  Creates kev:
                                    HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\35644f3d0029f81c3d478d3c2407fac3.exe
  Opens key:
                                    HKLM\system\currentcontrolset\control\terminal server
```

```
HKLM\system\currentcontrolset\control\safeboot\option
 Opens key:
 Opens key:
                         HKLM\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
                         HKCU\software\policies\microsoft\windows\safer\codeidentifiers
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\secur32.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\advapi32.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\winlogon
                         HKLM\
 Opens key:
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\diagnostics
 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\user32.dll
 Opens key:
                         HKLM\system\currentcontrolset\control\session manager
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
                         \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
 Opens key:
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\msvcrt.dll
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\netapi32.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\comctl32.dll
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\shell32.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comdlg32.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\crypt32.dll
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\odbc32.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\odbcbcp.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\pdh.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:
                         HKCU\
 Opens key:
                         HKCU\software\policies\microsoft\control panel\desktop
 Opens key:
                         HKCU\control panel\desktop
 Opens key:
                         HKLM\system\setup
 Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
                         HKCU\software\microsoft\windows\currentversion\explorer\advanced
 Opens key:
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\languagepack
 Opens key:
                         HKLM\system\currentcontrolset\services\crypt32\performance
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\msasn1
 Opens key:
                         HKLM\software\microsoft\bidinterface\loader
 Opens key:
                         HKLM\software\microsoft\mdac
 Opens key:
                         HKLM\software
 Opens key:
                         HKCU\software\odbc\odbc.ini\odbc
 Opens key:
                         HKLM\software\odbc\odbc.ini\odbc
                         HKLM\software\microsoft\ole
 Opens key:
 Opens key:
                         HKCR\interface
                         HKCR\interface\{00020400-0000-0000-c000-00000000046}
 Opens kev:
 Opens key:
                         HKLM\software\microsoft\oleaut
 Opens key:
                         HKLM\software\microsoft\oleaut\userera
 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\35644f3d0029f81c3d478d3c2407fac3.exe\rpcthreadpoolthrottle
 Opens key:
                         HKLM\software\policies\microsoft\windows nt\rpc
```

Opens key: HKLM\software\microsoft\windows nt\currentversion\pdh Opens key: HKLM\system\currentcontrolset\control\computername

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\odbcint.dll

Opens key: HKLM\system\currentcontrolset\control\servicecurrent

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

options\imagehlp.dll

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

options\wintrust.dll

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

options\sfc\_os.dll

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

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

options\crtdll.dll

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

options\sfc.dll

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

options\msctf.dll

Opens kev:

HKLM\software\microsoft\ctf\compatibility\35644f3d0029f81c3d478d3c2407fac3.exe

HKLM\software\microsoft\ctf\systemshared\ Opens key:

HKCU\keyboard layout\toggle Opens key: Opens key: HKLM\software\microsoft\ctf\

Opens key: HKLM\software\microsoft\windows nt\currentversion\imm

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

options\msctfime.ime

HKCU\software\microsoft\ctf Opens key:

Opens key:  ${\it HKLM \backslash software \backslash microsoft \backslash ctf \backslash systems hared}$ 

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: HKLM\software\policies\microsoft\system\dnsclient

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

options\cisvc.exe

Opens key: HKLM\system\wpa\tabletpc Opens key: HKLM\system\wpa\mediacenter

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

options\acgenral.dll

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

Opens key:

 $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ options\shimeng.dll

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

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

Opens key:

options\winmm.dll

Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\msacm32.dll

Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\userenv.dll

Opens kev: options\uxtheme.dll

Opens key: HKU\.default\software\policies\microsoft\control panel\desktop

HKU\.default\control panel\desktop Opens key:

Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\advanced

HKLM\software\microsoft\windows nt\currentversion\drivers32 Opens key:

Opens key:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm HKLM\software\microsoft\audiocompressionmanager\drivercache Opens key:

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.im aadpcm$ 

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msadpc manager \setminus driver cache \setminus msadpc msadpc$ 

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711

Opens kev:

 $HKLM \ \ software \ \ \ microsoft \ \ \ audio compression manager \ \ \ \ \ msgsm610$ 

Opens key:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ audiocompression manager\+ driver cache\+ msacm.\ trspch$ Opens key:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. \ msg723$ 

Opens kev:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1

 $HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. sl\_anet$ 

Opens key:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.iac2$ Opens key:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. 13 acm$ 

Opens key: HKLM\svstem\currentcontrolset\control\mediaresources\acm Opens key: HKLM\system\currentcontrolset\control\productoptions

HKU\.default\software\microsoft\windows\currentversion\explorer\user Opens key:

shell folders

Opens key: HKLM\software\policies\microsoft\windows\system

Opens key: HKU\.default\software\microsoft\windows\currentversion\thememanager Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\cisvc.exe\rpcthreadpoolthrottle

Opens key: HKLM\system\currentcontrolset\control\contentindex Opens key: HKLM\system\currentcontrolset\control\contentindex\catalogs Opens kev: HKLM\system\currentcontrolset\control\contentindex\catalogs\system Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setupapi.dll Opens key: HKLM\system\currentcontrolset\control\minint Opens key: HKLM\system\wpa\pnp HKLM\software\microsoft\windows\currentversion\setup Opens key:  ${\it HKLM \backslash software \backslash microsoft \backslash windows \backslash current version}$ Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels Opens key: Opens kev: HKLM\system\currentcontrolset\control\contentindex\catalogs\system\scopes

Opens key: HKLM\software\microsoft\com3

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

options\comres.dll

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

options\clbcatq.dll

Opens key: HKLM\software\microsoft\com3\debug

Opens key: HKCU\software\classes\ HKLM\software\classes Opens key:

Opens key: HKU\ Opens key: HKCR\clsid

HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a} Opens kev: Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\treatas

Opens key:

HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprocserver32 Opens key: Opens key:  $\label{lem:hkcr} $$ HKCR\clsid{2a488070-6fd9-11d0-a808-00a0c906241a} \in \clsid{2a488070-6fd9-11d0-a808-00a0c906241a} $$ \clsid{2a488070-6fd9-11d0-a808-00a0c906241a} = \cline{2a488070-6fd9-11d0-a808-00a0c906241a} = \cline{2a488070-6fd9-11d0-a808-00a0c906241a}$ Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\localserver32 Opens key:  $HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\tinprochandler 32$ Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprochandlerx86 Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\localserver

Opens key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\extendederrors\{f9ae8981-7e52-11d0-8964-00c04fd611d7}

Opens key:  $HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\$ \extendederrors Opens key:  $HKCR \ clsid \ \{f9ae 8981-7e52-11d0-8964-00c04fd611d7\} \ \ in procserver 32$ 

Opens key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-

00c04fd611d7}\versionindependentprogid

HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\progid Opens key:

Opens key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}

Opens key: HKCR\msidxs errorlookup\clsid HKCR\msidxs errorlookup Opens key:

Opens key:  $HKCR\clsid\f9ae8980-7e52-11d0-8964-00c04fd611d7\clsid\f9ae8980-7e52-11d0-8964-00c04fd611d7\clsid\cls$ Opens key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\inprocserver32

HKCR\clsid\{f9ae8980-7e52-11d0-8964-Opens key:

00c04fd611d7}\versionindependentprogid

Opens key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\progid

HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7} Opens key:

Opens key: HKCR\msidxs\clsid

HKCR\msidxs Opens kev:

 $HKCR \ c1sid \ \{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410\} \ \ inprocserver 32$ Opens key:

Opens key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-

00c04fc2f410}\versionindependentprogid

 $HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\progid$ Opens key: Opens key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}

Opens kev: HKLM\system\currentcontrolset\control

 $HKCR\clsid\\ \{aa205a4d-681f-11d0-a243-08002b36fca4\}\\ \cline{Absolution}$ Opens key: Opens key:  $HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\ \ inprocserver 32$ 

Opens key: HKCR\clsid\{08c524e0-89b0-11cf-88a1-00aa004b9986}

HKCR\binarvfile Opens kev: Opens key: HKCR\vxdfile Opens key: HKCR\vxdfile\clsid

HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce} Opens key: Opens key: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}\clsid Opens key: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce} HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}\clsid Opens key: Opens key: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062} Opens key: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}\clsid

HKCR\aifffile Opens key: Opens key: HKCR\aifffile\clsid Opens key: HKCR\asffile HKCR\asffile\clsid Opens key: Opens key: HKCR\asxfile Opens key: HKCR\asxfile\clsid HKCR\aufile Opens key: Opens key: HKCR\aufile\clsid HKCR\avifile Opens kev: HKCR\avifile\clsid Opens key:

Opens key: HKCR\clsid\{00022602-0000-0000-c000-00000000046}

Opens key: HKCR\msbackupfile Opens key: HKCR\msbackupfile\clsid Opens key: HKCR\paint.picture Opens kev: HKCR\paint.picture\clsid

Opens key: HKCR\clsid\{d3e34b21-9d75-101a-8c3d-00aa001a1652}

HKCR\clsid\{0cd7a5c0-9f37-11ce-ae65-08002b2e1262} Opens key: Opens key: HKCR\clsid\{0cd7a5c0-9f37-11ce-ae65-08002b2e1262}\clsid HKCR\cdafile Opens key: HKCR\cdafile\clsid Opens key: Opens key: HKCR\comfile Opens key: HKCR\comfile\clsid HKCR\cplfile Opens key: HKCR\cplfile\clsid Opens key: Opens key: HKCR\curfile HKCR\curfile\clsid Opens key: HKCR\dllfile Opens key: Opens key: HKCR\dllfile\clsid Opens key: HKCR\drvfile HKCR\drvfile\clsid Opens key: Opens key: HKCR\emffile HKCR\emffile\clsid Opens key: HKCR\exefile Opens kev: Opens key: HKCR\exefile\clsid Opens key: HKCR\fndfile HKCR\fndfile\clsid Opens key: Opens key: HKCR\fonfile Opens key: HKCR\fonfile\clsid HKCR\giffile Opens kev: Opens key: HKCR\giffile\clsid Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13} Opens key: HKCR\icmfile Opens key: HKCR\icmfile\clsid Opens key: HKCR\icofile Opens key: HKCR\icofile\clsid Opens key: HKCR\ivffile Opens key: HKCR\ivffile\clsid HKCR\pjpegfile Opens key: Opens key: HKCR\pjpegfile\clsid Opens key: HKCR\jpegfile HKCR\jpegfile\clsid Opens key: Opens key: HKCR\mpegfile Opens key: HKCR\mpegfile\clsid HKCR\m3ufile Opens key: Opens key: HKCR\m3ufile\clsid Opens key: HKCR\midfile HKCR\midfile\clsid Opens key: Opens key: HKCR\clsid\{00022603-0000-0000-c000-00000000046} Opens key: HKCR\mp3file HKCR\mp3file\clsid Opens key: Opens key: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367} Opens key: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}\clsid Opens key: HKCR\ocxfile Opens key: HKCR\ocxfile\clsid HKCR\perffile Opens kev: HKCR\perffile\clsid Opens key: Opens key: HKCR\pngfile Opens key: HKCR\pngfile\clsid HKCR\sysfile Opens key: Opens key: HKCR\sysfile\clsid Opens kev: HKCR\tifimage.document Opens key: HKCR\tifimage.document\clsid Opens key: HKCR\ttcfile HKCR\ttcfile\clsid Opens key: HKCR\ttffile Opens key: Opens key: HKCR\ttffile\clsid Opens key: HKCR\soundrec Opens key: HKCR\soundrec\clsid Opens key: HKCR\clsid\{00020c01-0000-0000-c000-00000000046} Opens key: HKCR\waxfile HKCR\waxfile\clsid Opens key: Opens key: HKCR\wmafile Opens key: HKCR\wmafile\clsid HKCR\wmffile Opens key: Opens key: HKCR\wmffile\clsid Opens key: HKCR\wmvfile HKCR\wmvfile\clsid Opens key: Opens key: HKCR\wmzfile Opens key: HKCR\wmzfile\clsid HKCR\wvxfile Opens key: Opens key: HKCR\wvxfile\clsid HKCR\.xbm Opens kev: Opens key: HKCR\.xbm\clsid Opens key: HKCR\compressedfolder Opens key: HKCR\compressedfolder\clsid HKCR\clsid\{e88dcce0-b7b3-11d1-a9f0-00aa0060fa31} Opens key:

 Opens key:
 HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprocserver32

 Opens key:
 HKCR\clsid\{89bcb7a4-6119-101a-bcb7-00dd010655af}

 Opens key:
 HKCR\clsid\{89bcb7a5-6119-101a-bcb7-00dd010655af}

```
HKCR\clsid\{89bcb7a6-6119-101a-bcb7-00dd010655af}
      Opens key:
      Opens key:
                                                                                                  HKCR\clsid\{961c1130-89ad-11cf-88a1-00aa004b9986}
      Opens key:
                                                                                                  HKCR\clsid\{8c9e8e1c-90f0-11d1-ba0f-00a0c906b239}
                                                                                                  HKCR\clsid\{95876eb0-90f0-11d1-ba0f-00a0c906b239}
      Opens key:
      Opens key:
                                                                                                  HKCR\clsid\{9e704f44-90f0-11d1-ba0f-00a0c906b239}
      Opens key:
                                                                                                  HKCR\clsid\{9ed4692c-90f0-11d1-ba0f-00a0c906b239}
                                                                                                  HKCR\clsid\{87db1ada-aa39-11d1-829f-00a0c906b239}
      Opens key:
      Opens key:
                                                                                                  HKCR\plaintext
      Opens key:
                                                                                                  HKCR\batfile
                                                                                                  HKCR\batfile\clsid
      Opens key:
                                                                                                  HKCR\cmdfile
      Opens key:
      Opens key:
                                                                                                  HKCR\cmdfile\clsid
      Opens key:
                                                                                                  HKCR\idqfile
                                                                                                  HKCR\inifile
      Opens key:
      Opens key:
                                                                                                  HKCR\inifile\clsid
                                                                                                  HKCR\inxfile
      Opens key:
                                                                                                  HKCR\regfile
      Opens kev:
      Opens key:
                                                                                                  HKCR\regfile\clsid
      Opens key:
                                                                                                  HKCR\inffile
                                                                                                  HKCR\inffile\clsid
      Opens key:
      Opens key:
                                                                                                  HKCR\vbsfile
      Opens key:
                                                                                                  HKCR\vbsfile\clsid
                                                                                                  HKCR\asmfile
      Opens kev:
      Opens key:
                                                                                                  HKCR\cfile
      Opens key:
                                                                                                  HKCR\cppfile
      Opens key:
                                                                                                  HKCR\cxxfile
      Opens key:
                                                                                                  HKCR\deffile
      Opens key:
                                                                                                  HKCR\hfile
                                                                                                  HKCR\hppfile
      Opens key:
      Opens key:
                                                                                                  HKCR\hxxfile
      Opens key:
                                                                                                  HKCR\idlfile
                                                                                                  HKCR\incfile
      Opens key:
      Opens key:
                                                                                                  HKCR\jsfile
      Opens key:
                                                                                                  HKCR\jsfile\clsid
                                                                                                  HKCR\logfile
      Opens key:
      Opens key:
                                                                                                  HKCR\plfile
      Opens key:
                                                                                                  HKCR\rcfile
                                                                                                  HKCR\rtffile
      Opens key:
      Opens key:
                                                                                                  HKCR\rtffile\clsid
      Opens key:
                                                                                                  HKCR\clsid\{73fddc80-aea9-101a-98a7-00aa00374959}
                                                                                                  HKCR\urlfile
      Opens key:
      Opens key:
                                                                                                  HKCR\xmlfile
      Opens key:
                                                                                                  HKCR\xmlfile\clsid
                                                                                                  HKCR \ clsid \ \{48123bc4-99d9-11d1-a6b3-00c04fd91555\}
      Opens key:
      Opens key:
                                                                                                  HKCR\xlsfile
      Opens key:
                                                                                                  HKCR\txtfile
                                                                                                  HKCR\txtfile\clsid
      Opens key:
      Opens key:
                                                                                                  HKCR\wordview.rtf.8
                                                                                                  HKCR\wordview.rtf.8\clsid
      Opens kev:
      Opens key:
                                                                                                  HKCR\internetshortcut
      Opens key:
                                                                                                  HKCR\internetshortcut\clsid
                                                                                                  HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}
      Opens key:
      Opens key:
                                                                                                  HKCR\xslfile
      Opens key:
                                                                                                  HKCR\xslfile\clsid
                                                                                                  HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprocserver32
      Opens kev:
                                                                                                  HKCR \verb|\clsid|{78fe669a-186e-4108-96e9-77b586c1332f} \verb|\inprocserver32|
      Opens key:
      Opens key:
                                                                                                  HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\ \ in procserver 32
                                                                                                  HKCR\clsid\{1f247dc0-902e-11d0-a80c-00a0c906241a}\inprocserver32
      Opens key:
      Opens key:
                                                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ciadmin.dll
      Opens key:
                                                                                                  HKLM\software\microsoft\mmc\snapins
      Opens key:
                                                                                                  HKLM \ software \ microsoft \ mmc \ snapins \ \{95ad72f0-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46
00aa004b9986}
      Opens key:
                                                                                                  HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-
00aa004b9986}\nodetypes
      Opens key:
                                                                                                  HKLM\software\microsoft\mmc\nodetypes
      Opens key:
                                                                                                  HKLM \setminus software \setminus microsoft \setminus mmc \setminus nodetypes \setminus \{5401e3e9-f5f6-11d1-b4f7-mmc \setminus nodetypes \setminus nodetypes \setminus \{5401e3e9-f5f6-11d1-b4f7-mmc \setminus nodetypes \setminus nodetypes \setminus nodetypes \setminus \{5401e3e-f5f6-11d1-b4f7-mmc \setminus nodetypes \setminus nodetypes \setminus \{5401e3e-f5f6-11d1-b4f7-mmc \setminus nodetypes \setminus \{5401e3e-f5f6-11d1-b4f7-mmc \setminus nodetypes \setminus \{5401e3e-f5f6-11d1-b4f7-mmc \setminus nodetypes \setminus
00c04fc2db8d}
      Opens key:
                                                                                                  00c04fd8d5b0}
      Opens key:
                                                                                                  HKLM \setminus software \setminus microsoft \setminus mmc \setminus detypes \setminus \{476e6449 - aaff-11d0 - b944 - aaaff-11d0 - b944 - aaff-11d0 - b944 - aaff-11d0 - b944 - aaff-11d0
00c04fd8d5b0}\extensions
                                                                                                 HKLM \setminus software \setminus microsoft \setminus mmc \setminus nodetypes \setminus \{476e6449 - aaff-11d0 - b944 - aaff-11d
     Opens kev:
00c04fd8d5b0}\extensions\namespace
      Opens key:
                                                                                                 00c04fd8d5b0}\dynamic extensions
      Opens key:
                                                                                                  HKLM\system\currentcontrolset\control\
      Opens key:
                                                                                                  HKLM\system\currentcontrolset\control\server applications
      Opens key:
                                                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ixsso.dll
      Opens key:
                                                                                                  HKCR\typelib
                                                                                                  HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}
      Opens kev:
```

 $HKCR \ typelib \ \{4e469dd1-2b6f-11d0-bfbc-0020f8008024\} \ \ 1.0$ 

Opens key:

HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0\flags Opens key: HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0\409 Opens key: Opens kev: HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0\helpdir Opens key: Opens key: HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c} Opens key:  $HKCR \land f7456c32-6ff0-11d1-a260-0000f8753d7c \rbrace \land proxystubclsid$ Opens key: HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}\typelib Opens key: Opens key: HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}  $HKCR\ interface \ \{7d74218f-4858-42f9-99cc-ef2ba840425a\}\ proxystubclsid$ Opens key: Opens key: HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}\proxystubclsid32 Opens key:  $HKCR\interface {7d74218f-4858-42f9-99cc-ef2ba840425a} \typelib$ Opens key: HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}  $HKCR \setminus \{3b34e346-6cf1-11d1-a260-0000f8753d7c\} \setminus \{3b34e346-6cf1-11d1-a260-0000f87546-6cf1-11d1-a260-0000f8766$ Opens key: Opens key: HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}\typelib Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\nlhtml.dll Opens key: HKCR\clsid\{e0ca5340-4534-11cf-b952-00aa0051fe20}\inprocserver32 Opens key: HKCR\clsid\{7f73b8f6-c19c-11d0-aa66-00c04fc2eddc} Opens key: HKCR\clsid\{bd70c020-2d24-11d0-9110-00004c752752} Opens key: HKCR\clsid\{ffb10349-5267-4c96-8ad7-01b52a2de434} HKCR\clsid\{ea25106f-12f5-4460-a10a-19e48fff1da5} Opens kev: Opens key: HKCR\odcfile Opens key: HKCR\odcfile\clsid HKCR\hhcfile Opens key: Opens key: HKCR\htmlfile Opens key: HKCR\htmlfile\clsid Opens key: HKCR\asp\_auto\_file Opens key: HKCR\aspxfile Opens key: HKCR\ascxfile Opens key: HKCR\cssfile Opens key: HKCR\cssfile\clsid Opens key: HKCR\htafile HKCR\htafile\clsid Opens key: Opens key: HKCR\clsid\{3050f4d8-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCR\httfile HKCR\httfile\clsid Opens key: Opens key: HKCR\aspfile Opens key: HKCR\aspfile\clsid  $\label{lem:hklm} \mbox{HKLM\software\mbox{$\backslash$ microsoft\windows nt\currentversion\selection}} \ \ \mbox{nt} \ \ \mbox{$\backslash$ currentversion\selection} \ \ \mbox{$\backslash$ microsoft\selection} \ \mbox{$\backslash$ microsoft\selection} \ \mbox{$\backslash$ microsoft\selection} \ \ \mbox{$\backslash$ microsoft\selection} \ \mbox{$\backslash$$ Opens key: options\offfilt.dll Opens key: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprocserver32 HKCR\word.document.8 Opens key: Opens key: HKCR\word.document.8\clsid Opens key: HKCR\word.template.8 HKCR\powerpoint.template.8 Opens key: Opens key: HKCR\powerpoint.template.8\clsid HKCR\powerpoint.show.8 Opens kev:  ${\tt HKCR \backslash powerpoint.show.8 \backslash clsid}$ Opens key: Opens key: HKCR\powerpoint.slideshow.8 Opens key: HKCR\powerpoint.slideshow.8\clsid HKCR\excel.sheet.8 Opens key: Opens key: HKCR\excel.sheet.8\clsid Opens kev: HKCR\excel.chart.8 Opens key: HKCR\excel.template.8 Opens key: HKCR\word.document.6 Opens key: HKCR\word.template HKCR\powerpoint.show.7 Opens kev: Opens key: HKCR\powerpoint.template Opens key: HKCR\excel.chart.5 Opens key: HKCR\excel.sheet.5 Opens key: HKCR\wordview.document.8 Opens key: HKCR\wordview.document.8\clsid HKCR\wordview.template.8 Opens key: Opens key: HKCR\wordview.template.8\clsid Opens key: HKCR\powerpointviewer.template.11  $HKCR \verb|\powerpointviewer.template.11\clsid|$ Opens key: Opens key: HKCR\powerpointviewer.show.11 Opens key: HKCR\powerpointviewer.show.11\clsid HKCR\powerpointviewer.slideshow.11 Opens key: Opens key: HKCR\powerpointviewer.slideshow.11\clsid Opens key: HKCR\excelviewer.sheet.8 Opens key: HKCR\excelviewer.sheet.8\clsid Opens key: HKCR\excelviewer.template.8 HKCR\excelviewer.template.8\clsid Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ciodm.dll Opens key: HKCR\microsoft.isadm.1

Opens key:

HKCR\microsoft.isadm.1\clsid Opens key: HKCR\microsoft.isadm HKCR\microsoft.isadm\curver Opens key: Opens key: HKCR\microsoft.isadm\clsid

```
HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}
   Opens key:
                                             HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
   Opens key:
   Opens kev:
                                             HKCR \clsid \ \{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d\} \ \ progid
                                             HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\programmable
   Opens key:
   Opens kev:
                                             HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-
00c04fc2db8d}\versionindependentprogid
   Opens key:
                                             HKCR\microsoft.iscatadm.1
                                             HKCR\microsoft.iscatadm.1\clsid
   Opens key:
   Opens key:
                                             HKCR\microsoft.iscatadm
   Opens key:
                                             HKCR\microsoft.iscatadm\curver
   Opens key:
                                             HKCR\microsoft.iscatadm\clsid
                                             HKCR \c1sid \ \{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d\}
   Opens key:
   Opens key:
                                             HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
                                             \label{local-back} \begin{tabular}{ll} HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\progid \end{tabular}
   Opens key:
   Opens key:
                                             HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\programmable
   Opens key:
                                             HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-
00c04fc2db8d}\versionindependentprogid
   Opens key:
                                             HKCR\microsoft.isscopeadm.1
   Opens key:
                                             HKCR\microsoft.isscopeadm.1\clsid
   Opens key:
                                             HKCR\microsoft.isscopeadm
   Opens key:
                                             HKCR\microsoft.isscopeadm\curver
   Opens key:
                                             HKCR\microsoft.isscopeadm\clsid
                                             HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}
   Opens kev:
   Opens key:
                                             HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
   Opens key:
                                             HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\progid
                                             HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\programmable
   Opens key:
   Opens key:
                                             HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-
00c04fc2db8d}\versionindependentprogid
                                             HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}
   Opens kev:
   Opens key:
                                             HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0
   Opens key:
                                             HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\flags
                                             HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\0
   Opens key:
   Opens key:
                                             HKCR \ typelib \ \{3bc4f393-652a-11d1-b4d4-00c04fc2db8d\} \ 1.0 \ 0 \ win 32
   Opens key:
                                             HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\helpdir
   Opens key:
                                             HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}
   Opens key:
                                             HKCR\interface{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid
   Opens key:
                                             HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid32
                                             HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\typelib
   Opens key:
   Opens key:
                                             HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}
   Opens key:
                                             HKCR\ interface \ \{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d\}\ proxystubclsid
                                             Opens key:
   Opens key:
                                             Opens key:
                                             HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}
                                             HKCR \verb|\| interface \verb|\| \{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d\} \verb|\| proxystubclsid| 
   Opens key:
   Opens key:
                                             HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid32
   Opens key:
                                             HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}\typelib
   Opens key:
                                             \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\infosoft.dll
                                             HKCR\clsid\{eeed4c20-7f1b-11ce-be57-00aa0051fe20}\inprocserver32
   Opens kev:
                                             HKCR \verb|\clsid|{d99f7670-7f1a-11ce-be57-00aa0051fe20} \verb|\inprocserver32|
   Opens key:
   Opens key:
                                             HKCR\clsid\{59e09848-8099-101b-8df3-00000b65c3b5}\inprocserver32
   Opens key:
                                             HKCR\clsid\{2a6eb050-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
                                             HKCR\clsid\{9b08e210-e51b-11cd-bc7f-00aa003db18e}\inprocserver32
   Opens key:
   Opens key:
                                             HKCR\clsid\{510a4910-7f1c-11ce-be57-00aa0051fe20}\ \ inprocserver 32
   Opens kev:
                                             HKCR\clsid\fd86b5d0-12c6-11ce-bd31-00aa004bbb1f\\\label{line} Inproceserver 32
   Opens key:
                                             Opens key:
                                             HKCR\clsid\{01c6b350-12c7-11ce-bd31-00aa004bbb1f}\inprocserver32
   Opens key:
                                             HKCR\clsid\{9478f640-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
   Opens key:
                                             HKCR \verb|\clsid|{0285b5c0-12c7-11ce-bd31-00aa004bbb1f} \verb|\inprocserver32|
   Opens key:
                                             \label{local-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-one-best-o
   Opens key:
                                             HKCR\clsid\{66b37110-8bf2-11ce-be59-00aa0051fe20}\inprocserver32
   Opens key:
                                             HKCR\clsid\{860d28d0-8bf4-11ce-be59-00aa0051fe20}\inprocserver32
   Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mimefilt.dll
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\langwrbk.dll
   Opens key:
                                             HKCR\enguswrdbrk.enguswrdbrk.1
                                             HKCR \verb|\enguswrdbrk.enguswrdbrk.1\verb|\clsid|
   Opens key:
   Opens key:
                                             HKCR\enguswrdbrk.enguswrdbrk
   Opens key:
                                             HKCR\enguswrdbrk.enguswrdbrk\curver
                                             HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}
   Opens key:
   Opens key:
                                             HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserver32
                                             HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\progid
   Opens key:
                                             HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-
   Opens key:
0090272fa362}\versionindependentprogid
                                             HKCR\engukwrdbrk.engukwrdbrk.1
   Opens kev:
                                             HKCR\engukwrdbrk.engukwrdbrk.1\clsid
   Opens key:
   Opens key:
                                             HKCR\engukwrdbrk.engukwrdbrk
   Opens key:
                                             HKCR\engukwrdbrk.engukwrdbrk\curver
                                             HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}
   Opens key:
   Opens key:
                                             HKCR \c1sid \{363f1015-fd5f-4ba8-ac58-29634f378a42} \c) in procserver 32f3 \c) and the second of t
                                             HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}\progid
   Opens kev:
   Opens key:
                                             HKCR\clsid\{363f1015-fd5f-4ba8-ac58-
```

```
29634f378a42}\versionindependentprogid
                         HKCR\frnfrnwrdbrk.frnfrnwrdbrk.1
 Opens key:
                         HKCR\frnfrnwrdbrk.frnfrnwrdbrk.1\clsid
 Opens key:
 Opens key:
                         HKCR\frnfrnwrdbrk.frnfrnwrdbrk
 Opens key:
                         HKCR\frnfrnwrdbrk.frnfrnwrdbrk\curver
 Opens key:
                         HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}
 Opens key:
                         HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\tinprocserver32
                         HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\progid
 Opens key:
                         HKCR\clsid\{f14e6b48-fbca-4d32-bd79-
 Opens key:
7829d4f7e43b}\versionindependentprogid
 Opens kev:
                         HKCR\itlitlwrdbrk.itlitlwrdbrk.1
 Opens key:
                         HKCR\itlitlwrdbrk.itlitlwrdbrk.1\clsid
 Opens key:
                         HKCR\itlitlwrdbrk.itlitlwrdbrk
                         HKCR\itlitlwrdbrk.itlitlwrdbrk\curver
 Opens key:
                         HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}
 Opens key:
 Opens key:
                         HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\inprocserver32
                         HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\progid
 Opens key:
 Opens key:
                         HKCR\clsid\{91870674-de84-4313-b07d-
a387415bb4f5}\versionindependentprogid
 Opens key:
                         HKCR\spnmdrwrdbrk.spnmdrwrdbrk.1
 Opens key:
                         HKCR\spnmdrwrdbrk.spnmdrwrdbrk.1\clsid
                         HKCR\spnmdrwrdbrk.spnmdrwrdbrk
 Opens key:
 Opens key:
                         HKCR\spnmdrwrdbrk.spnmdrwrdbrk\curver
 Opens key:
                         HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}
 Opens key:
                         HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\inprocserver32
                         HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\progid
 Opens key:
 Opens key:
                         HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-
c4825abbe5cf}\versionindependentprogid
                         HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}
 Opens kev:
 Opens key:
                         HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0
 Opens key:
                         HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\flags
                         HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\0
 Opens key:
 Opens key:
                         HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\0\win32
 Opens key:
                         HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\helpdir
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\samlib.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll
 Opens key:
                         HKLM\system\currentcontrolset\services\ldap
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntmarta.dll
 Opens key:
                         HKLM\system\currentcontrolset\services\contentindex\performance
 Opens key:
                         HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}
                         HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410\}\treatas
 Opens key:
 Opens key:
                         HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\inprocserverx86
 Opens key:
                         HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\localserver32
                         HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\nprochandler32
 Opens key:
 Opens key:
                         HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\tinprochandlerx86
 Opens key:
                         HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\localserver
 Opens key:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system\properties
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\mpr.dll
 Opens key:
                         Opens kev:
                         HKLM\system\currentcontrolset
                         HKLM \verb|\system| current controlset \verb|\services| rdpnp \verb|\networkprovider| \\
 Opens key:
 Opens key:
                         HKLM \setminus system \setminus current control set \setminus services \setminus lanman work station \setminus network provider
 Opens key:
                         HKLM\system\currentcontrolset\services\webclient\networkprovider
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\drprov.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netui0.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\network\world full
access shared parameters
 Opens key:
                         HKU\.default\control panel\international
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netrap.dll
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\netui1.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntlanman.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\davclnt.dll
 Opens key:
                         HKLM\system\currentcontrolset\control\session manager\appcertdlls
 Opens key:
                         HKLM\system\currentcontrolset\control\session manager\appcompatibility
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
 Opens key:
                         HKU\.default\software\microsoft\windows
nt\currentversion\appcompatflags\layers
 Opens key:
                         HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cidaemon.exe
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\appcompatflags
```

```
Opens key:
                                                       HKCU\software\microsoft\windows nt\currentversion\appcompatflags
    Opens key:
                                                       HKU\.default\software\microsoft\windows nt\currentversion\appcompatflags
    Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cidaemon.exe
    Opens kev:
                                                       HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}
    Opens key:
                                                       HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\treatas
                                                       HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\inprocserverx86
    Opens key:
                                                       HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\localserver32
    Opens key:
                                                       HKCR \verb|\clsid|{aa205a4d-681f-11d0-a243-08002b36fca4} \verb|\inprochandler32| \\
    Opens key:
                                                       HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\inprochandlerx86
    Opens key:
                                                       HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\localserver
    Opens key:
    Opens key:
                                                       HKLM\system\currentcontrolset\control\contentindex\language
    Opens key:
                                                       HKLM\system\currentcontrolset\control\contentindex\language\dutch_dutch
    Opens key:
                                                       HKLM\system\currentcontrolset\control\contentindex\language\english uk
    Opens key:
                                                       HKLM\system\currentcontrolset\control\contentindex\language\english_us
    Opens key:
Opens key:
HKLM\system\currentcontrolset\control\contentindex\language\german_german
    Opens key:
HKLM\system\currentcontrolset\control\contentindex\language\italian_italian
    Opens key:
                                                       HKLM\system\currentcontrolset\control\contentindex\language\neutral
                                                       HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}
    Opens kev:
    Opens key:
                                                       HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\treatas
    Opens key:
                                                       \label{lem:hkcr} $$ HKCR\clsid{369647e0-17b0-11ce-9950-00aa004bbb1f} \in \clsid{369647e0-17b0-11ce-9950-00aa004bbb1f} in processing the second context of 
    Opens key:
                                                       HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\localserver32
    Opens key:
                                                       \label{lem:hkcr} $$HKCR\clsid{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprochandler 32 $$
    Opens key:
                                                       HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprochandlerx86
                                                       HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\localserver
    Opens key:
    Opens key:
                                                       HKLM\software\microsoft\security center\svc
    Opens key:
                                                       HKLM\software\microsoft\windows\currentversion\uninstall
                                                       HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-
    Opens key:
3d01-b289-befc77a11a1e}
    Opens key:
                                                       HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-
4ca4-87b4-2f83217002ff}
                                                       HKLM\software\microsoft\windows\currentversion\uninstall\{350c97b0-3d7c-
    Opens key:
4ee8-baa9-00bcb3d54227}
                                                       HKLM\software\microsoft\windows\currentversion\uninstall\{4a03706f-666a-
   Opens key:
4037-7777-5f2748764d10}
    Opens key:
                                                       HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-
0409-0000-0000000ff1ce}
                                                       HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-
    Opens key:
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:
                                                       1033-7b44-a93000000001}
    Opens key:
                                                       HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-
3f2d-899a-6a1d67f2073f}
    Opens key:
                                                       HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-
4027-b136-2b3e1f5ab6e2}
    Opens key:
                                                       36ca-84d3-9f4dcf5c5bd9}
    Opens key:
                                                       HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-
36ca-84d3-9f4dcf5c5bd9}.kb953595
    Opens key:
                                                       HKCR\.ini\persistenthandler
    Opens key:
                                                       HKCR\clsid\{5e941d80-bf96-11cd-b579-
08002b30bfeb \} \ persistent add in sregistered \\ \{89bcb740-6119-101a-bcb7-00dd010655af\} \\ \{89bcb740-6114-bcb7-00dd010655af\} \\ \{89bcb740-6144-bcb7-00dd010655af\} \\
                                                       HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}
    Opens key:
    Opens key:
                                                       HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\treatas
                                                       HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprocserverx86
    Opens key:
    Opens key:
                                                       HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\localserver32
    Opens key:
                                                       HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprochandler32
    Opens key:
                                                       HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprochandlerx86
    Opens key:
                                                       HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\localserver
                                                       HKLM\software\microsoft\windows\currentversion\policies\explorer
    Opens kev:
    Opens key:
                                                       HKU\.default\software\microsoft\windows\currentversion\policies\explorer
    Opens kev:
a2d8-08002b30309d}
    Opens key:
                                                       Opens kev:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cidaemon.exe\rpcthreadpoolthrottle
    Opens kev:
HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| explorer \verb|\| mountpoints 2 \verb|\| cpc \verb|\| volume | leading to the context of the context o
    Opens key:
                                                       HKCR\directory
    Opens key:
                                                       HKCR\directory\curver
    Opens key:
                                                       HKCR\directory\
    Opens key:
                                                       HKU\.default\software\microsoft\windows\currentversion\explorer
```

```
Opens key:
                                       HKU\.default\software\microsoft\windows\currentversion\explorer\
  Opens key:
                                       HKU\.default\software\microsoft\internet explorer\desktop\scheme
  Opens key:
                                       HKU\.default\software\microsoft\internet explorer\desktop\components
  Opens key:
HKU\.default\software\microsoft\windows\currentversion\explorer\startmenu\startpanel
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\startmenu\startpanel
                                      {\tt HKU} \verb|.default\| software \verb||microsoft\| windows \verb||currentversion\| policies \verb|| system || and the property of the prop
  Opens key:
  Opens key:
                                       HKCR\directory\shellex\iconhandler
                                       HKCR\directory\clsid
  Opens key:
  Opens key:
                                       HKCR\folder
  Opens key:
                                       HKCR\folder\clsid
  Opens key:
                                       HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| explorer \verb|\| file exts
                                       HKCR\.ini
  Opens key:
  Opens key:
                                       HKCR\inifile\curver
  Opens key:
                                       HKCR\inifile\
                                       HKCR\inifile\shellex\iconhandler
  Opens kev:
  Opens key:
                                       HKCR\systemfileassociations\.ini
  Opens key:
                                       HKCR\*
                                       HKCR\*\clsid
  Opens key:
  Opens key:
                                       HKCR\inifile\shellex\propertyhandler
  Opens key:
                                       HKCR\.ini\shellex\propertyhandler
                                       HKCR\*\shellex\propertyhandler
  Opens kev:
  Opens key:
                                       HKCR\.sam\persistenthandler
  Opens key:
                                       HKCR\.sam
                                       HKCR\.sam\shellex\iconhandler
  Opens key:
  Opens key:
                                       HKCR\systemfileassociations\.sam
  Opens key:
                                       HKCR\.sam\clsid
  Opens key:
                                       HKCR\.sam\shellex\propertyhandler
  Opens key:
                                       HKCR\.xls\persistenthandler
  Opens key:
                                       HKCR\clsid\{98de59a0-d175-11cd-a7bd-
00006b827d94}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
  Opens key:
                                       HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}
  Opens key:
                                       HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\treatas
                                       \label{lem:hkcr} $$HKCR\clsid{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprocserverx86$
  Opens key:
  Opens key:
                                       HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\localserver32
  Opens key:
                                       HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprochandler32
                                       HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprochandlerx86
  Opens key:
  Opens key:
                                       HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\localserver
  Opens key:
                                       HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\treatas
                                       HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\tinprocserverx86
  Opens key:
  Opens key:
                                       HKCR \ clsid \ \{80a3e9b0-a246-11d3-bb8c-0090272fa362\} \ localserver 32
  Opens key:
                                       HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprochandler32
                                       HKCR \verb|\clsid|{80a3e9b0-a246-11d3-bb8c-0090272fa362} \verb|\inprochandlerx86|| \\
  Opens key:
  Opens key:
                                       HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\localserver
  Opens key:
                                       HKCR\.xls
                                       HKCR\excelviewer.sheet.8\curver
  Opens key:
  Opens key:
                                       HKCR\excelviewer.sheet.8\
                                       HKCR\excelviewer.sheet.8\shellex\iconhandler
  Opens kev:
  Opens key:
                                       HKCR\systemfileassociations\.xls
  Opens key:
                                       HKCR\systemfileassociations\.xls\shellex\iconhandler
  Opens key:
                                       HKCR\systemfileassociations\.xls\clsid
  Opens key:
                                       HKCR\excelviewer.sheet.8\shellex\propertyhandler
  Opens key:
                                       HKCR\.xls\shellex\propertyhandler
  Opens kev:
                                       HKCR\systemfileassociations\.xls\shellex\propertyhandler
  Opens key:
                                       HKCR\.wk4\persistenthandler
  Opens key:
                                       HKCR\.wk4
  Opens key:
                                       HKCR\.wk4\shellex\iconhandler
                                       HKCR\systemfileassociations\.wk4
  Opens kev:
  Opens key:
                                       HKCR\.wk4\clsid
  Opens key:
                                       HKCR\.wk4\shellex\propertyhandler
  Opens key:
                                       HKCR\.ppt\persistenthandler
  Opens key:
                                       HKCR\.shw\persistenthandler
  Opens key:
                                       HKCR\.shw
                                       HKCR\.shw\shellex\iconhandler
  Opens key:
  Opens key:
                                       HKCR\systemfileassociations\.shw
  Opens key:
                                       HKCR\.shw\clsid
  Opens key:
                                       HKCR\.shw\shellex\propertyhandler
  Opens key:
                                       HKCR\.wb2\persistenthandler
  Opens key:
                                       HKCR\.wb2
                                       HKCR\.wb2\shellex\iconhandler
  Opens key:
  Opens key:
                                       HKCR\systemfileassociations\.wb2
  Opens key:
                                       HKCR\.wb2\clsid
  Opens key:
                                       HKCR\.wb2\shellex\propertyhandler
  Opens key:
                                       HKCR\.wav\persistenthandler
                                       HKCR\clsid\{098f2470-bae0-11cd-b579-
  Opens kev:
08002b30bfeb}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
  Opens key:
                                       HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}
  Opens key:
                                       HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\treatas
  Opens key:
                                       HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\
  Opens key:
                                       HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\localserver32
                                       HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\ \ in prochandler 32
  Opens kev:
```

 $HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\ \ in prochandler x86$ 

Opens key:

```
HKCR \ clsid \ \{c3278e90-bea7-11cd-b579-08002b30bfeb\} \ local server
  Opens key:
  Opens key:
                                   HKCR\.wav
                                   HKCR\soundrec\curver
  Opens kev:
  Opens key:
                                   HKCR\soundrec\
  Opens kev:
                                   HKCR\soundrec\shellex\iconhandler
  Opens key:
                                   HKCR\systemfileassociations\.wav
                                   HKCR\systemfileassociations\.wav\shellex\iconhandler
  Opens key:
  Opens key:
                                   HKCR\systemfileassociations\audio
  Opens key:
                                   HKCR\systemfileassociations\audio\shellex\iconhandler
  Opens key:
                                   HKCR\clsid\{00020c01-0000-0000-c000-00000000046}\implemented
categories\{00021490-0000-0000-c000-00000000046}
  Opens key:
                                   HKCR\soundrec\shellex\propertyhandler
  Opens key:
                                   HKCR\.wav\shellex\propertyhandler
  Opens key:
                                   HKCR\systemfileassociations\.wav\shellex\propertyhandler
  Opens key:
                                   HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71\}\inprocserver32
  Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\verclsid.exe
  Opens key:
                                   HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}
  Opens key:
                                   HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71\}\ \treatas
  Opens key:
                                   HKCR\clsid\epsilon = 480b-92fd-7ddb47101d71\inprocserverx86
  Opens key:
                                   HKCR \ clsid \ \{e4b29f9d-d390-480b-92fd-7ddb47101d71\} \ localserver 32
  Opens key:
                                   HKCR\clsid\epsilon = 480b-92fd-7ddb47101d71\inprochandler32
  Opens key:
                                   HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\inprochandlerx86
  Opens key:
                                   HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\localserver
  Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvfw32.dll
  Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\avifil32.dll
  Opens kev:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shmedia.dll
  Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\vfw
                                   HKLM\software\microsoft\windows
  Opens key:
nt\currentversion\appcompatflags\custom\shmedia.dll
92fd-7ddb47101d71}
  Opens key:
                                   HKCR\.doc\persistenthandler
                                   HKCR\.doc
  Opens key:
  Opens key:
                                   HKCR\wordview.document.8\curver
  Opens key:
                                   HKCR\wordview.document.8\
  Opens key:
                                   HKCR\wordview.document.8\shellex\iconhandler
  Opens key:
                                   HKCR\systemfileassociations\.doc
  Opens key:
                                   HKCR\systemfileassociations\.doc\shellex\iconhandler
  Opens key:
                                   HKCR\systemfileassociations\.doc\clsid
  Opens key:
                                   HKCR\wordview.document.8\shellex\propertyhandler
  Opens key:
                                   HKCR\.doc\shellex\propertyhandler
                                   Opens key:
  Opens key:
                                   HKCR\.wpd\persistenthandler
                                   HKCR\.wpd
  Opens kev:
                                   HKCR\.wpd\shellex\iconhandler
  Opens key:
  Opens key:
                                   HKCR\systemfileassociations\.wpd
  Opens key:
                                   HKCR\.wpd\clsid
                                   HKCR\.wpd\shellex\propertyhandler
  Opens key:
  Opens key:
                                   HKCR\.wpg\persistenthandler
  Opens kev:
                                   HKCR\.wpg
                                   HKCR\.wpg\shellex\iconhandler
  Opens key:
  Opens key:
                                   HKCR\systemfileassociations\.wpg
  Opens key:
                                   HKCR\.wpg\clsid
                                   HKCR\.wpg\shellex\propertyhandler
  Opens key:
  Opens key:
                                   HKCR\.lnk\persistenthandler
  Opens key:
                                   HKCR\.lnk
                                   HKCR\lnkfile\clsid
  Opens key:
  Opens key:
                                   Opens key:
                                   HKCR\clsid\{00021401-0000-0000-c000-
00000000046}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
  Opens key:
                                   HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserver32
  Opens key:
                                   HKCR\clsid\{00021401-0000-0000-c000-00000000046}
                                   HKCR\clsid\{00021401-0000-0000-c000-00000000046}\treatas
  Opens key:
  Opens key:
                                   \label{locality} $$ HKCR\clsid_{00021401-0000-0000-c000-00000000046}\times \end{20} $$ in processor $$ except $$ in processor $$ except $$ except $$ in processor $$ except $$ exce
  Opens key:
                                   HKCR\clsid\{00021401-0000-0000-c000-000000000046}\localserver32
                                   Opens key:
  Opens key:
                                   HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprochandlerx86
  Opens key:
                                   HKCR\clsid\{00021401-0000-0000-c000-00000000046}\localserver
  Opens key:
                                   HKCR\appid\cidaemon.exe
  Opens key:
                                   HKLM\system\currentcontrolset\control\lsa
                                   HKCR\interface\{0000010b-0000-0000-c000-00000000046}
  Opens kev:
                                   Opens key:
  Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\linkinfo.dll
  Opens key:
                                   HKCR\network\sharinghandler
  Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntshrui.dll
  Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\xpsp2res.dll
  Opens key:
                                       HKCR\.exe
                                       HKCR\exefile\curver
  Opens kev:
  Opens key:
                                       HKCR\exefile\
  Opens kev:
                                       HKCR\exefile\shellex\iconhandler
  Opens key:
                                       HKCR\systemfileassociations\.exe
                                       HKCR\systemfileassociations\application
  Opens key:
                                       HKCR\interface\{89bcb740-6119-101a-bcb7-00dd010655af}
  Opens key:
  Opens key:
                                       HKCR\lnkfile
  Opens key:
                                       HKCR\lnkfile\curver
  Opens key:
                                       HKCR\lnkfile\
  Opens key:
                                       HKCR\lnkfile\shellex\iconhandler
  Opens key:
                                       HKCR\systemfileassociations\.lnk
                                       HKCR\clsid\{00021401-0000-0000-c000-00000000046}\implemented
  Opens key:
categories\{00021490-0000-0000-c000-000000000046}
                                       HKCR\lnkfile\shellex\propertyhandler
  Opens key:
                                       HKCR\.lnk\shellex\propertyhandler
  Opens key:
  Opens key:
HKLM \label{loop} \label{loop} HKLM \label{loop} HKLM \label{loop} \label{loop} HKLM \label{loop} \label{loop} HKLM \label{loop} \label{loop} \label{loop} HKLM \label{loop} \label{loop} \label{loop} \label{loop} \label{loop} HKLM \label{loop} \label{
a2ea-08002b30309d}
  Opens key:
                                       HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
  Opens key:
                                       HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
                                       HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
  Opens key:
  Opens key:
                                       HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86
  Opens key:
                                       HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32
                                       HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\tinprochandler 32
  Opens key:
  Opens key:
                                       HKCR \ clsid \ \{871c5380-42a0-1069-a2ea-08002b30309d\} \ in prochandler x 86
  Opens key:
                                       HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver
  Opens kev:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ieframe.dll
  Opens key:
                                       HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe
  Opens key:
                                       HKLM\software\microsoft\internet explorer\setup
  Opens key:
                                       HKLM\system\currentcontrolset\control\wmi\security
                                       HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib
  Opens key:
  Opens key:
                                       HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
                                       HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
  Opens key:
  Opens key:
                                       HKCR \land face \land \{79 eac9c4-baf9-11ce-8c82-00aa004ba90b\} \land proxystubclsid 32
  Opens key:
                                       HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32
  Opens key:
                                       HKCR \verb|\interface| \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\} \verb|\proxystubclsid32| 
  Opens key:
                                       HKCR\.zfsendtotarget
  Opens key:
                                       HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}\curver
                                       HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}\
  Opens key:
  Opens key:
                                       HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}\shellex\iconhandler
                                       HKCR\systemfileassociations\.zfsendtotarget
  Opens key:
                                       HKCR\clsid\{888dca60-fc0a-11cf-8f0f-
  Opens key:
00c04fd7d062}\shellex\propertyhandler
                                       HKCR\.zfsendtotarget\shellex\propertyhandler
  Opens kev:
                                       HKCR\drive\shellex\folderextensions
  Opens key:
  Opens key:
                                       HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
                                       HKCR\.ico
  Opens key:
  Opens key:
                                       HKCR\icofile\curver
  Opens kev:
                                       HKCR\icofile\
                                       HKCR\icofile\shellex\iconhandler
  Opens key:
  Opens key:
                                       HKCR\systemfileassociations\.ico
                                       HKCR\systemfileassociations\image
  Opens key:
                                       HKCR\systemfileassociations\image\shellex\iconhandler
  Opens kev:
  Opens key:
                                       HKCR\systemfileassociations\image\clsid
  Opens key:
                                       HKCR\.chm
                                       HKCR\chm.file
  Opens key:
  Opens key:
                                       HKCR\chm.file\curver
  Opens key:
                                       HKCR\chm.file\
                                       HKCR\chm.file\shellex\iconhandler
  Opens key:
  Opens key:
                                       HKCR\systemfileassociations\.chm
  Opens key:
                                       HKCR\chm.file\clsid
                                       HKCR\.msc
  Opens key:
  Opens key:
                                       HKCR\mscfile
  Opens key:
                                       HKCR\mscfile\curver
                                       HKCR\mscfile\
  Opens key:
  Opens key:
                                       HKCR\mscfile\shellex\iconhandler
  Opens key:
                                       HKCR\systemfileassociations\.msc
                                       HKCR\mscfile\clsid
  Opens key:
  Opens key:
                                       HKCR\.cpl
  Opens key:
                                       HKCR\cplfile\curver
                                       HKCR\cplfile\
  Opens key:
  Opens key:
                                       HKCR\cplfile\shellex\iconhandler
  Opens key:
                                       HKCR\systemfileassociations\.cpl
  Opens key:
                                       HKCR\.desklink\persistenthandler
```

 Opens key:
 HKCR\.desklink

 Opens key:
 HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}\curver

 Opens key:
 HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}\

Opens key: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}\shellex\iconhandler

Opens key: HKCR\systemfileassociations\.desklink
Opens key: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-

00a0c90a90ce}\shellex\propertyhandler

Opens key: HKCR\.desklink\shellex\propertyhandler
Opens key: HKCR\.mapimail\persistenthandler

Opens key: HKCR\.mapimail

Opens key: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}\curver Opens key: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}\

Opens key: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}\shellex\iconhandler

Opens key: HKCR\systemfileassociations\.mapimail
Opens key: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-

00a0c90a90ce}\shellex\propertyhandler

Opens key: HKCR\.mapimail\shellex\propertyhandler

Opens key: HKCR\.dat\persistenthandler

Opens key: HKCR\.dat

Opens key: HKCR\.dat\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.dat

Opens key: HKCR\.dat\clsid

Opens key: HKCR\.dat\shellex\propertyhandler
Opens key: HKCR\.pol\persistenthandler

Opens key: HKCR\.pol

Opens key: HKCR\systemfileassociations\.pol Opens key: HKCR\.jpg\persistenthandler

Opens key: HKCR\.jpg

Opens key: HKCR\jpegfile\curver

Opens key: HKCR\jpegfile\

Opens key: HKCR\jpegfile\shellex\iconhandler Opens key: HKCR\systemfileassociations\.jpg

Opens key: HKCR\systemfileassociations\.jpg\shellex\iconhandler

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented

categories\{00021490-0000-0000-c000-00000000046}

Opens key: HKCR\jpegfile\shellex\propertyhandler
Opens key: HKCR\.jpg\shellex\propertyhandler

Opens key: HKCR\systemfileassociations\.jpg\shellex\propertyhandler
Opens key: HKCR\systemfileassociations\image\shellex\propertyhandler
Opens key: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprocserver32

Opens key: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}

Opens key: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\treatas

 Opens key:
 HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprocserverx86

 Opens key:
 HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\localserver32

 Opens key:
 HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprochandler32

 Opens key:
 HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprochandlerx86

 Opens key:
 HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\localserver

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

options\gdiplus.dll

Opens key: HKCR\.wpl\persistenthandler

Opens key: HKCR\.wpl

Opens key: HKCR\wplfile\clsid
Opens key: HKCR\wplfile
Opens key: HKCR\wplfile\curver
Opens key: HKCR\wplfile\

Opens key: HKCR\wplfile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wpl

Opens key: HKCR\systemfileassociations\.wpl\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wpl\clsid
Opens key: HKCR\wplfile\shellex\propertyhandler
Opens key: HKCR\.wpl\shellex\propertyhandler

Opens key: HKCR\systemfileassociations\.wpl\shellex\propertyhandler

Opens key: HKCR\.wma\persistenthandler

Opens key: HKCR\.wma

Opens key: HKCR\wmafile\curver Opens key: HKCR\wmafile\

Opens key: HKCR\wmafile\shellex\iconhandler Opens key: HKCR\systemfileassociations\.wma

Opens key: HKCR\systemfileassociations\.wma\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wma\clsid

Opens key: HKCR\systemilleassociations\audio\clsid
Opens key: HKCR\mafile\shellex\propertyhandler
Opens key: HKCR\.wma\shellex\propertyhandler

Opens key: HKCR\systemfileassociations\.wma\shellex\propertyhandler
Opens key: HKCR\clsid\{875cb1a1-0f29-45de-a1ae-cfb4950d0b78}\inprocserver32

Opens key: HKCR\.lic\persistenthandler

Opens key: HKCR\.lic

Opens key: HKCR\systemfileassociations\.lic
Opens key: HKCR\.sst\persistenthandler

Opens key: HKCR\.sst

Opens key: HKCR\certificatestorefile\clsid
Opens key: HKCR\certificatestorefile
Opens key: HKCR\certificatestorefile\curver
Opens key: HKCR\certificatestorefile\

Opens key: HKCR\certificatestorefile\shellex\iconhandler

Opens key: HKCR\systemfileassociations\.sst

```
HKCR\certificatestorefile\shellex\propertyhandler
 Opens key:
                         HKCR\.sst\shellex\propertyhandler
 Opens key:
 Opens kev:
                         HKCR\.mydocs\persistenthandler
 Opens key:
                         HKCR\.mydocs
 Opens kev:
                         HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}\curver
 Opens key:
                         HKCR\clsid\\\{ecf03a32-103d-11d2-854d-006008059367\}\\\\
                         HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}\\\ \shellex\\\ \clsid\{ecf03a32-103d-11d2-854d-006008059367}\
 Opens key:
                         HKCR\systemfileassociations\.mydocs
 Opens key:
 Opens key:
                         HKCR\clsid\{ecf03a32-103d-11d2-854d-
006008059367}\shellex\propertyhandler
                         HKCR\.mydocs\shellex\propertyhandler
 Opens kev:
 Opens key:
                         HKCR\.url\persistenthandler
 Opens key:
                         HKCR\clsid\{8cd34779-9f10-4f9b-adfb-
b3faeabdab5a\} \persistent add in sregistered \\ \{89bcb740-6119-101a-bcb7-00dd010655af\}
 Opens key:
                         HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\nprocserver32
 Opens key:
                         HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}
 Opens key:
                         HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\treatas
 Opens key:
                         HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\
 Opens key:
                         HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\localserver32
                         HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\inprochandler32
 Opens key:
 Opens key:
                         HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\tinprochandlerx86
 Opens key:
                         HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\localserver
                         HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}
 Opens kev:
 Opens key:
                         HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\treatas
 Opens key:
                         HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\ \ inprocserver 32
                         HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprocserverx86
 Opens key:
 Opens key:
                         HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\localserver32
 Opens key:
                         HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprochandler32
                         \label{local-observable} HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\ \ in prochandler x86
 Opens key:
 Opens key:
                         HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\localserver
 Opens key:
                         HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance
                         HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}
 Opens key:
 Opens key:
                         HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\treatas
 Opens key:
                         HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprocserver32
                         HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprocserverx86
 Opens key:
 Opens key:
                         HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\localserver32
 Opens key:
                         HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprochandler32
                         HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprochandlerx86
 Opens key:
 Opens key:
                         HKCR \ clsid \ \{942bc614-676c-464e-b384-d3202aaa02da\} \ localserver
 Opens key:
                         HKCR\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\initpropertybag
                         Opens key:
                         HKCR\clsid\{06eee834-461c-42c2-8dcf-
 Opens kev:
1502b527b1f9}\instance\propertysetstorage
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings
                         HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
 Opens key:
 Opens key:
                         HKU\.default\software\policies\microsoft\internet
explorer\main\featurecontrol
                         HKLM\software\microsoft\internet explorer\main\featurecontrol
 Opens key:
 Opens key:
                         HKU\.default\software\microsoft\internet explorer\main\featurecontrol
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_urlfile_cacheflush_kb936881
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
 Opens key:
                         HKCR\protocols\name-space handler\
 Opens key:
                         HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet settings
 Opens key:
                         HKU\.default\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\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\
                         HKU\.default\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\domains\
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\ranges\
                         HKU\.default\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\ranges\
 Opens key:
                         HKU\.default\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
                         HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}
 Opens key:
 Opens key:
                         HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\ \ treat as
                         HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprocserver32
 Opens kev:
 Opens key:
                         HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprocserverx86
```

HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\localserver32 Opens key: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprochandler32 Opens key: Opens kev: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprochandlerx86 HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\localserver Opens key: Opens kev: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad} Opens key:  $HKCR \verb|\clsid|{6f237df9-9ddb-47ad-b218-400d54c286ad} \verb|\treatas|$  $HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprocserver32$ Opens key: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprocserverx86 Opens key: Opens key:  $HKCR \clsid \end{6f237df9-9ddb-47ad-b218-400d54c286ad} \localserver 32$ Opens key:  $HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\) in prochandler 32$ HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprochandlerx86 Opens key: Opens key:  $HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\localserver$ Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-00000000046} Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\2 HKCR\.url Opens kev: Opens key: HKCR\internetshortcut\curver Opens key: HKCR\internetshortcut\ Opens key: HKCR\internetshortcut\shellex\iconhandler Opens key: HKCR\systemfileassociations\.url HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\implemented Opens key: categories\{00021490-0000-0000-c000-00000000046} Opens key: HKCR\internetshortcut\shellex\propertyhandler Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\inprocserver32 Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\treatas Opens key:  $\label{lem:hkcr} $$ HKCR\clsid{fbf23b40-e3f0-101b-8488-00aa003e56f8} \in \clsid{fbf23b40-e3f0-101b-8488-00aa003e56f8} = \clid{fbf23b40-e3f0-101b-8488-00aa003e56f8} = \clid{fbf23b40-e3f0-101b-8488-00aa003e566f8} = \clid{fbf23b40-e3f0-101b-8488-00aa003e566f8} = \clid{fbf23b40-e3f0-101b-8488-00aa003e$ Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\localserver32 Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\inprochandler32 Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\inprochandlerx86 Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\localserver HKCR\appid\{fbf23b40-e3f0-101b-8488-00aa003e56f8} Opens key: Opens key: HKCR\.txt\persistenthandler Opens key: HKCR\.txt HKCR\txtfile\curver Opens key: Opens key: HKCR\txtfile\ Opens key: HKCR\txtfile\shellex\iconhandler HKCR\systemfileassociations\.txt Opens key: Opens key: HKCR\systemfileassociations\text Opens key: HKCR\systemfileassociations\text\shellex\iconhandler Opens key: HKCR\systemfileassociations\text\clsid Opens key: HKCR\txtfile\shellex\propertyhandler Opens key: HKCR\.txt\shellex\propertyhandler Opens key: HKCR\systemfileassociations\text\shellex\propertyhandler Opens key: HKCR\.bat\persistenthandler Opens key: HKCR\.bat HKCR\batfile\curver Opens key: Opens key: HKCR\batfile\ HKCR\batfile\shellex\iconhandler Opens kev: Opens key: HKCR\systemfileassociations\.bat Opens key: HKCR\batfile\shellex\propertyhandler Opens key: HKCR\.bat\shellex\propertyhandler Opens key: HKCR\.sys\persistenthandler Opens key: HKCR\.sys Opens kev: HKCR\sysfile\curver Opens key: HKCR\sysfile\ Opens key: HKCR\sysfile\shellex\iconhandler Opens key: HKCR\systemfileassociations\.sys HKCR\sysfile\shellex\propertyhandler Opens key: Opens key: HKCR\.sys\shellex\propertyhandler Opens key: HKCR\.log\persistenthandler Opens key: HKCR\.log Opens key: HKCR\systemfileassociations\.log Opens key: HKCR\.log\shellex\propertyhandler Opens key: HKCR\.com\persistenthandler Opens key: HKCR\.com Opens key: HKCR\comfile\curver Opens key: HKCR\comfile\ Opens key: HKCR\comfile\shellex\iconhandler Opens key: HKCR\svstemfileassociations\.com Opens key: HKCR\comfile\shellex\propertyhandler Opens key: HKCR\.com\shellex\propertyhandler Opens key: HKCR\.\persistenthandler Opens key: HKCR\. Opens key: HKCR\.bmp\persistenthandler Opens kev: HKCR\.bmp Opens key: HKCR\paint.picture\curver Opens key: HKCR\paint.picture\ Opens key: HKCR\paint.picture\shellex\iconhandler Opens key: HKCR\systemfileassociations\.bmp Opens key: HKCR\systemfileassociations\.bmp\shellex\iconhandler  $HKCR \verb|\cl| sid \verb|\d3e34b21-9d75-101a-8c3d-00aa001a1652| \verb|\implemented| \\$ Opens key: categories\{00021490-0000-0000-c000-000000000046}

```
HKCR\paint.picture\shellex\propertyhandler
   Opens key:
   Opens key:
                                                         HKCR\.bmp\shellex\propertyhandler
                                                         HKCR\systemfileassociations\.bmp\shellex\propertyhandler
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\ws2help.dll
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\wsock32.dll
                                                         HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
   Opens key:
   Opens key:
                                                         HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
   Opens key:
                                                         HKCR \ clsid \ \{4590f811-1d3a-11d0-891f-00aa004b2e24\} \ \ inprocserver 32
   Opens key:
                                                         \label{lem:hkcr} $$ HKCR\clsid_{4590f811-1d3a-11d0-891f-00aa004b2e24} \in \clsid_{4590f811-1d3a-11d0-891f-00aa004b2e24} $$
                                                         HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver32
   Opens key:
   Opens key:
                                                         HKCR \ clsid \ \{4590f811-1d3a-11d0-891f-00aa004b2e24\} \ inprochandler 32
                                                         HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86
   Opens key:
                                                         HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver
   Opens key:
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemcomn.dll
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemprox.dll
   Opens key:
                                                         HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
   Opens key:
                                                         HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
   Opens key:
                                                         HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\inprocserver32
   Opens key:
                                                         \label{localserver32} $$ HKCR\clsid_{8bc3f05e-d86b-11d0-a075-00c04fb68820} \le 1.0 calserver 32. $$
   Opens key:
   Opens key:
                                                         \label{lem:hkcr} $$ HKCR\clsid_{8bc3f05e-d86b-11d0-a075-00c04fb68820} \in $$ Abc3f05e-d86b-11d0-a075-00c04fb68820} $$ Abc3f05e-d86b-11d0-a075-00c04fb68820. $$ A
   Opens key:
                                                         HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandlerx86
   Opens key:
                                                         HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver
   Opens key:
                                                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
   Opens key:
                                                         HKCR\appid\cisvc.exe
                                                         HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
   Opens key:
   Opens key:
                                                         HKCR \land f309ad18-d86a-11d0-a075-00c04fb68820 \rbrace \land proxystubclsid32
   Opens key:
                                                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
                                                         HKCR \ clsid \ \{7c857801-7381-11cf-884d-00aa004b2e24\} \ treat as
   Opens key:
   Opens key:
                                                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
   Opens key:
                                                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86
                                                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32
   Opens key:
   Opens key:
                                                         HKCR\.exe\persistenthandler
   Opens key:
                                                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32
                                                         HKCR \ clsid \ \{7c857801-7381-11cf-884d-00aa004b2e24\} \ in prochandler x 86
   Opens key:
   Opens key:
                                                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemsvc.dll
   Opens key:
                                                         HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
   Opens key:
                                                         HKCR\ interface \ \{d4781cd6-e5d3-44df-ad94-930efe48a887\}\ proxystubclsid32
                                                         HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
   Opens key:
   Opens key:
                                                         HKCR \land eface \land \{9556dc99-828c-11cf-a37e-00aa003240c7\} \land proxystubclsid32\} \land efactor for the proxystubcl in the proxystubcl of the proxystubcl of
   Opens key:
                                                         HKCR\exefile\shellex\propertyhandler
   Opens key:
                                                         HKCR\.exe\shellex\propertyhandler
   Opens key:
                                                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
   Opens key:
                                                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
   Opens key:
                                                         HKCR\clsid\\d68af00a-29cb-43fa-8504-ce99a996d9ea\\\inprocserver32
   Opens key:
                                                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\timescreerverx86
   Opens kev:
                                                         \label{localserver32} HKCR\clsid\\ \{d68af00a-29cb-43fa-8504-ce99a996d9ea\\ \localserver32
   Opens key:
                                                         HKCR \clsid \d68af00a-29cb-43fa-8504-ce99a996d9ea \label{eq:hkcr} \label{eq:hkcr} \\ hKCR \clsid \d68af00a-29cb-43fa-8504-ce99a996d9ea \label
   Opens key:
                                                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\tinprochandlerx86
   Opens key:
                                                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver
   Opens key:
                                                         HKCR\.scf\persistenthandler
   Opens key:
                                                         HKCR\.scf
   Opens key:
                                                         HKCR\shcmdfile\clsid
                                                         HKCR\clsid\{57651662-ce3e-11d0-8d77-00c04fc99d61}\persistenthandler
   Opens key:
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp60.dll
                                                         \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
   Opens key:
options\dnsapi.dll
   Opens key:
                                                         HKLM\system\currentcontrolset\services\dnscache\parameters
                                                         HKLM\software\policies\microsoft\windows nt\dnsclient
   Opens key:
   Opens key:
                                                         HKCR\shcmdfile
   Opens key:
                                                         HKCR\shcmdfile\curver
                                                         HKCR\shcmdfile\
   Opens key:
   Opens key:
                                                         HKCR\shcmdfile\shellex\iconhandler
   Opens key:
                                                         HKCR\systemfileassociations\.scf
                                                        HKCR\clsid\{57651662-ce3e-11d0-8d77-00c04fc99d61}\ implemented
   Opens key:
categories\{00021490-0000-0000-c000-000000000046}
                                                         HKCR\shcmdfile\shellex\propertyhandler
   Opens kev:
   Opens key:
                                                         HKCR\.scf\shellex\propertyhandler
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdsapi.dll
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\fastprox.dll
   Opens key:
                                                         HKLM\software\microsoft\wbem\cimom
```

Opens key: HKCR\interface\{027947e1-d731-11ce-a357-00000000001}

```
Opens key:
    Opens key:
                                                         HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
    Opens key:
                                                         HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\ \ treat as
                                                         HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32
    Opens key:
    Opens key:
                                                         Opens key:
                                                         HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver32
    Opens key:
                                                         HKCR \clsid \ \{1b1cad8c-2dab-11d2-b604-00104b703efd\} \ \ in prochandler 32
                                                         HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandlerx86
    Opens key:
    Opens key:
                                                         HKCR \clsid \ \{1b1cad8c-2dab-11d2-b604-00104b703efd\} \localserver
    Opens key:
                                                         HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
                                                        Opens key:
    Opens key:
                                                         HKCR\interface {423ec01e-2e35-11d2-b604-00104b703efd}
    Opens key:
                                                         HKCR \land (423ec01e-2e35-11d2-b604-00104b703efd) \land (23ec01e-2e35-11d2-b604-00104b703efd) \land (23ec01e-2e35-11d2-b604-00104b703effd) \land (23ec01e-2e35-11d2-b604-0
    Opens key:
                                                         HKCR\.bak\persistenthandler
    Opens key:
                                                         HKCR\.bak
    Opens key:
                                                         HKCR\systemfileassociations\.bak
    Opens kev:
                                                        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 \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col_catalog 9 \setminus catalog\_entries
Opens key:
Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col_catalog 9 \cap catalog_entries \setminus 0000000000003 \cap catalog_entries \setminus view 1 \cap col_catalog 9 \cap catalog_entries \cap col_catalog 9 \cap catalog 9 \cap ca
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
    Opens key:
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\0000000000008
    Opens key:
Opens key:
Opens key:
Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
   Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
    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\mswsock.dll
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options\hnetcfg.dll
    Opens key:
                                                         HKLM\software\microsoft\rpc\securityservice
    Opens key:
                                                         \label{lem:hklm} \verb+Kklm \+ services + winsock + parameters + winsock + wins
    Opens kev:
                                                         HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock
    Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
    Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
    Opens key:
                                                         HKLM\system\currentcontrolset\services\tcpip\linkage
                                                         HKLM\system\currentcontrolset\services\tcpip\parameters\
    Opens kev:
    Opens key:
                                                         HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
    Opens key:
                                                         HKLM\system\currentcontrolset\services\netbt\parameters
    Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
    Opens kev:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winrnr.dll
    Opens key:
                                                         HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
    Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
    Oueries value:
                                                         HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
    Queries value:
```

```
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                          HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\compatibility32[35644f3d0029f81c3d478d3c2407fac3]
                         HKLM\software\microsoft\windows nt\currentversion\ime
 Oueries value:
compatibility[35644f3d0029f81c3d478d3c2407fac3]
                          HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 Queries value:
                          HKCU\control panel\desktop[multiuilanguageid]
 Oueries value:
 Queries value:
                          HKCU\control panel\desktop[smoothscroll]
 Oueries value:
                          HKLM\system\setup[systemsetupinprogress]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
 Oueries value:
                          HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
 Queries value:
                          HKLM\software\microsoft\ole[rwlockresourcetimeout]
 Queries value:
                          HKCR\interface[interfacehelperdisableall]
                          HKCR\interface[interfacehelperdisableallforole32]
 Oueries value:
 Queries value:
                          HKCR\interface[interfacehelperdisabletypelib]
 Queries value:
                          HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
                          HKCR\interface\{00020400-0000-0000-c000-
 Queries value:
00000000046}[interfacehelperdisableallforole32]
                         HKLM\software\microsoft\rpc[maxrpcsize]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\control\computername[computername]
                          HKLM\system\currentcontrolset\control\servicecurrent[]
 Oueries value:
                          HKLM\software\microsoft\ctf\systemshared[cuas]
 Queries value:
 Queries value:
                          HKCU\keyboard layout\toggle[language hotkey]
                          HKCU\keyboard layout\toggle[hotkey]
 Queries value:
                          HKCU\keyboard layout\toggle[layout hotkey]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\ctf[enableanchorcontext]
                          \label{lem:hklm} \verb+Kklm \+ software \+ microsoft \+ windows nt \+ current version \+ ime file]
 Oueries value:
                          HKCU\software\microsoft\ctf[disable thread input manager]
 Queries value:
                          HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
                          HKLM\system\wpa\mediacenter[installed]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\compatibility32[cisvc]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[cisvc]
                          HKU\.default\control panel\desktop[multiuilanguageid]
 Oueries value:
 Oueries value:
                          HKU\.default\control panel\desktop[smoothscroll]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
 Oueries value:
                          HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 2]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midil
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi31]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
 Oueries value:
                          \label{lem:hklm} \mbox{\sc hkklm\software\mbox{\sc microsoft\windows} nt\current\version\drivers32[aux3]}
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
 Queries value:
Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
```

Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9] Queries value: HKU\.default\software\microsoft\multimedia\audio[systemformats] HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.imaadpcm] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags] Oueries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags] HKLM\software\microsoft\windows Queries value: nt\currentversion\drivers32[msacm.msadpcm] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags] HKLM\software\microsoft\windows Queries value: nt\currentversion\drivers32[msacm.msg711] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport] Oueries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msgsm610] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]  $HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msgsm610[cformattags]$ Oueries value: Oueries value:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. msgsm610 [cfilter tags]$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.trspch] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache] Queries value: HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msg723] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport] Oueries value: Queries value:  $HKLM \verb|\software\microsoft\audiocompression manager\driver cache\mbox{\software}. msg723[aformattag cache] \\$ Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msaudio1] Queries value: Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags] HKLM\software\microsoft\windows Queries value: nt\currentversion\drivers32[msacm.sl\_anet] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[fdwsupport]

Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[aformattagcache]
Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[cformattags]

Oueries value:

```
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. sl\_anet[cfilter tags]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
 Oueries value:
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
 Oueries value:
Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
 Oueries value:
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.13acm[fdwsupport]
 Oueries value:
Oueries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. 13 acm [a formattag cache]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
                          HKU \verb|\|.default\| software \verb|\| multimedia \verb|\| audio compression |
 Queries value:
manager\msacm[nopcmconverter]
 Queries value:
                          HKU\.default\software\microsoft\multimedia\audio compression
manager\priority v4.00[priority1]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[userenvdebuglevel]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[chkaccdebuglevel]
                          HKLM\system\currentcontrolset\control\productoptions[producttype]
 Queries value:
                          HKU\.default\software\microsoft\windows\currentversion\explorer\user
 Oueries value:
shell folders[personal]
                          HKU\.default\software\microsoft\windows\currentversion\explorer\user
 Oueries value:
shell folders[local settings]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[rsopdebuglevel]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
 Queries value:
HKU\.default\software\microsoft\windows\currentversion\thememanager[compositing]
 Oueries value:
                          HKU\.default\control panel\desktop[lamebuttontext]
                          HKLM\system\currentcontrolset\control\contentindex[donotstartcisvc]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[cataloginactive]
HKLM\svstem\currentcontrolset\control\contentindex\catalogs\svstem[location]
 Queries value:
                          HKLM\system\wpa\pnp[seed]
                          HKLM\system\setup[osloaderpath]
 Oueries value:
                          HKLM\system\setup[systempartition]
 Queries value:
 Oueries value:
                          HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus setup[sourcepath]
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus setup [service pack cachepath] \\
                          HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion[devicepath]
                          HKLM\software\microsoft\windows\currentversion\setup[loglevel]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\setup[logpath]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[mountremovablecatalogs]
                          HKLM\system\currentcontrolset\control\contentindex[maxcachedpipes]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex[maxsimultaneousrequests]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[requesttimeout]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[minimizeworkingset]
                          HKLM\system\currentcontrolset\control\contentindex[minclientidletime]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[startupdelay]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex[maxactiverequestthreads]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[minidlerequestthreads]
 Queries value:
                          HKLM\software\microsoft\com3[com+enabled]
 Oueries value:
                          HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
 Queries value:
                          HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
                          HKLM\software\microsoft\com3[regdbversion]
 Oueries value:
 Oueries value:
                          HKCR\clsid\{2a488070-6fd9-11d0-a808-
00a0c906241a}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprocserver32[]
                          HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}[appid]
 Oueries value:
 Queries value:
                          HKCR\clsid\{2a488070-6fd9-11d0-a808-
00a0c906241a}\inprocserver32[threadingmodel]
                          HKLM\system\currentcontrolset\control\contentindex[dllstoregister]
 Oueries value:
 Oueries value:
                          HKCR\.386[]
 Queries value:
                          HKCR\.audiocd[]
 Oueries value:
                          HKCR\.desklink[]
 Queries value:
                          HKCR\.folder[]
```

```
Queries value:
                          HKCR\.mapimail[]
                          HKCR\.zfsendtotarget[]
Oueries value:
Oueries value:
                          HKCR\.aif[]
Queries value:
                          HKCR\.aifc[]
                          HKCR\.aiff[]
Oueries value:
Queries value:
                          HKCR\.aps[]
                          HKCR\.asf[]
Queries value:
                          HKCR\.asx[]
Oueries value:
Queries value:
                          HKCR\.au[]
                          HKCR\.avi[]
Queries value:
                          HKCR\avifile\clsid[]
Oueries value:
Queries value:
                          HKCR\.bin[]
Queries value:
                          HKCR\.bkf[]
                          HKCR\.bmp[]
Oueries value:
Queries value:
                          HKCR\paint.picture\clsid[]
Queries value:
                          HKCR\.bsc[]
Oueries value:
                          HKCR\.cab[]
Queries value:
                          HKCR\clsid\{0cd7a5c0-9f37-11ce-ae65-08002b2e1262}\clsid[]
Queries value:
                          HKCR\.cda[]
                          HKCR\.cgm[]
Oueries value:
Queries value:
                          HKCR\.com[]
Queries value:
                          HKCR\.cpl[]
                          HKCR\.cur[]
Oueries value:
Queries value:
                          HKCR\.dbg[]
Queries value:
                          HKCR\.dct[]
Queries value:
                          HKCR\.dib[]
Queries value:
                          HKCR\.dl_[]
Queries value:
                          HKCR\.dll[]
                          HKCR\.drv[]
Oueries value:
Queries value:
                          HKCR\.dvd[]
Queries value:
                          HKCR\.emf[]
Queries value:
                          HKCR\.eps[]
Queries value:
                          HKCR\.ex_[]
Queries value:
                          HKCR\.exe[]
Oueries value:
                          HKCR\.exp[]
Queries value:
                          HKCR\.eyb[]
                          HKCR\.fnd[]
Oueries value:
Oueries value:
                          HKCR\.fnt[]
Queries value:
                          HKCR\.fon[]
                          HKCR\.ghi[]
Queries value:
Oueries value:
                          HKCR\.gif[]
Queries value:
                          HKCR\giffile\clsid[]
                          HKCR\.gz[]
Oueries value:
Queries value:
                          HKCR\.hqx[]
                          HKCR\.icm[]
Oueries value:
                          HKCR\.ico[]
Queries value:
Queries value:
                          HKCR\.idb[]
Queries value:
                          HKCR\.ilk[]
                          HKCR\.imc[]
Oueries value:
Queries value:
                          HKCR\.in_[]
                          HKCR\.inv[]
Queries value:
Oueries value:
                          HKCR\.ivf[]
Queries value:
                          HKCR\.jbf[]
Queries value:
                          HKCR\.jfif[]
                          HKCR\pjpegfile\clsid[]
Oueries value:
Queries value:
                          HKCR\.jpe[]
                          HKCR\jpegfile\clsid[]
Queries value:
Oueries value:
                          HKCR\.jpeg[]
Oueries value:
                          HKCR\.jpg[]
Queries value:
                          HKCR\.latex[]
Queries value:
                          HKCR\.lib[]
Oueries value:
                          HKCR\.m14[]
                          HKCR\.m1v[]
Queries value:
Queries value:
                          HKCR\.m3u[]
                          HKCR\.mdb[]
Queries value:
Queries value:
                          HKCR\.mid[]
Queries value:
                          HKCR\midfile\clsid[]
Queries value:
                          HKCR\.midi[]
Queries value:
                          HKCR\.mmf[]
                          HKCR\.mov[]
Oueries value:
Queries value:
                          HKCR\.movie[]
                          HKCR\.mp2[]
Queries value:
Oueries value:
                          HKCR\.mp2v[]
Queries value:
                          HKCR\.mp3[]
Queries value:
                          HKCR\.mpa[]
Oueries value:
                          HKCR\.mpe[]
Queries value:
                          HKCR\.mpeg[]
                          HKCR\.mpg[]
Queries value:
Oueries value:
                          HKCR\.mpv2[]
Queries value:
                          HKCR\.msg[]
Queries value:
                          HKCR\.mv[]
                          HKCR\.mydocs[]
Oueries value:
Queries value:
                          HKCR\.ncb[]
```

HKCR\.obj[] Queries value: HKCR\.oc\_[] Oueries value: Oueries value: HKCR\.ocx[] HKCR\.pch[] Queries value: Oueries value: HKCR\.pdb[] Queries value: HKCR\.pds[] Queries value: HKCR\.pic[] HKCR\.pma[] Oueries value: Queries value: HKCR\.pmc[] Queries value: HKCR\.pml[] HKCR\.pmr[] Oueries value: Queries value: HKCR\.png[] Queries value: HKCR\pngfile\clsid[] Oueries value: HKCR\.psd[] Queries value: HKCR\.res[] Queries value: HKCR\.rle[] HKCR\.rmi[] Oueries value: Queries value: HKCR\.rpc[] Queries value: HKCR\.rsp[] Queries value: HKCR\.sbr[] Queries value: HKCR\.sc2[] Queries value: HKCR\.sit[] Oueries value: HKCR\.snd[] Queries value: HKCR\.sr\_[] HKCR\.sy\_[] Queries value: Queries value: HKCR\.sym[] Queries value: HKCR\.sys[] Queries value: HKCR\.tar[] Oueries value: HKCR\.tgz[] Queries value: HKCR\.tif[] HKCR\.tiff[] Oueries value: Queries value: HKCR\.tlb[] Queries value: HKCR\.tsp[] Queries value: HKCR\.ttc[] Oueries value: HKCR\.ttf[] Queries value: HKCR\.vbx[] HKCR\.vxd[] Oueries value: Oueries value: HKCR\.wav[] HKCR\soundrec\clsid[] Queries value: Queries value: HKCR\.wax[] Queries value: HKCR\.wll[] HKCR\.wlt[] Queries value: HKCR\.wm[] Oueries value: Queries value: HKCR\.wma[] HKCR\.wmf[] Queries value: HKCR\.wmp[] Queries value: HKCR\.wmv[] Queries value: Queries value: HKCR\.wmx[] HKCR\.wmz[] Oueries value: Queries value: HKCR\.wsz[] HKCR\.wvx[] Queries value: HKCR\.xix[] Oueries value: Queries value: HKCR\.z[] HKCR\.z96[] Queries value: Oueries value: HKCR\.zip[] Queries value: HKCR\compressedfolder\clsid[] HKCR\rtffile\clsid[] Queries value: Oueries value: HKCR\xmlfile\clsid[] Oueries value: HKCR\.dic[] Queries value: HKCR\.txt[] HKCR\.wtx[] Queries value: Queries value: HKCR\.bat[] HKCR\.cmd[] Queries value: Oueries value: HKCR\.ida[] Queries value: HKCR\.ini[] HKCR\.inx[] Queries value: HKCR\.reg[] Queries value: Queries value: HKCR\.inf[] Queries value: HKCR\.vbs[] HKCR\.asm[] Oueries value: Queries value: HKCR\.c[] HKCR\.cpp[] Queries value: Oueries value: HKCR\.cxx[] Queries value: HKCR\.def[] Queries value: HKCR\.h[] Oueries value: HKCR\.hpp[] Queries value: HKCR\.hxx[] HKCR\.idl[] Queries value: Oueries value: HKCR\.inc[] Queries value: HKCR\.js[] Queries value: HKCR\.log[] Oueries value: HKCR\.pl[] Queries value: HKCR\.rc[]

```
Oueries value:
                         HKCR\.url[1
 Oueries value:
                         HKCR\internetshortcut\clsid[]
 Queries value:
                         HKCR\.xml[]
                         HKCR\.xsl[1
 Oueries value:
 Queries value:
                         HKCR\xslfile\clsid[]
 Oueries value:
                         HKLM\software\microsoft\ole[maximumallowedallocationsize]
                         HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0[]
 Oueries value:
 Oueries value:
                         HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0\flags[]
 Oueries value:
                         HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0\409\win32[]
 Oueries value:
                         HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}[]
 Queries value:
                         HKCR \land f7456c32-6ff0-11d1-a260-0000f8753d7c \land proxystubclsid[]
 Oueries value:
                         HKCR \ | \ f7456c32-6ff0-11d1-a260-0000f8753d7c \ | \ proxystubclsid32[]
 Oueries value:
                         HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}\typelib[]
 Queries value:
                         HKCR \setminus \{f7456c32-6ff0-11d1-a260-0000f8753d7c\} \setminus \{typelib[version]\}
 Oueries value:
                         HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}[]
                         HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}\proxystubclsid[]
 Queries value:
 Queries value:
                         HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}\proxystubclsid32[]
 Oueries value:
                         HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}\typelib[]
                         HKCR \land face \land \{7d74218f-4858-42f9-99cc-ef2ba840425a\} \land typelib[version]
 Oueries value:
 Queries value:
                         HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}[]
 Queries value:
                         HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}\proxystubclsid[]
                         HKCR = \frac{3b34e346-6cf1-11d1-a260-0000f8753d7c}{proxystubclsid32[]}
 Oueries value:
 Queries value:
                         HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}\typelib[]
 Queries value:
                         HKCR \setminus \{3b34e346-6cf1-11d1-a260-0000f8753d7c\} \setminus \{ypelib[version]\}
 Oueries value:
                         HKCR\htmlfile\clsid[]
                         HKCR\htafile\clsid[]
 Queries value:
 Queries value:
                         HKCR\.odc[]
                         HKCR\.hhc[]
 Oueries value:
                         HKCR\.htm[]
 Queries value:
 Queries value:
                         HKCR\.html[]
 Queries value:
                         HKCR\.htx[]
                         HKCR\.stm[]
 Queries value:
 Queries value:
                         HKCR\.htw[]
 Oueries value:
                         HKCR\.asp[]
                         HKCR\.aspx[]
 Queries value:
 Oueries value:
                         HKCR\.ascx[]
 Oueries value:
                         HKCR\.css[]
                         HKCR\.hta[]
 Queries value:
                         HKCR\.htt[]
 Queries value:
 Oueries value:
                         HKCR\.doc[]
                         HKCR\.dot[]
 Queries value:
 Oueries value:
                         HKCR\.pot[]
 Oueries value:
                         HKCR\.ppt[]
 Oueries value:
                         HKCR\.pps[]
 Queries value:
                         HKCR\.xlb[]
 Oueries value:
                         HKCR\.xlc[]
 Queries value:
                         HKCR\.xls[]
 Oueries value:
                         HKCR\.xlt[]
                         HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0[]
 Oueries value:
                         HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\flags[]
 Oueries value:
 Oueries value:
                         HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\0\win32[1
 Oueries value:
                         HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\helpdir[]
 Queries value:
                         HKCR \cdot \{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d\}[]
                         Oueries value:
 Queries value:
                         HKCR \ interface \ \{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d\} \ proxystubclsid32[]
                         HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\typelib[]
 Queries value:
 Queries value:
                         HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\typelib[version]
                         HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}[]
 Oueries value:
                         Queries value:
 Queries value:
                         Oueries value:
                         HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}\typelib[]
                         HKCR \ interface \ \{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d\} \ typelib[version]
 Queries value:
 Queries value:
                         HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}[]
 Oueries value:
                         HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid[]
                         \label{local-equation} HKCR\interface \ \{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d\}\ proxystubclsid32[]
 Oueries value:
 Queries value:
                         HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}\typelib[]
 Oueries value:
                         HKCR \ \ typelib[version] \\
 Queries value:
                         HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0[]
 Oueries value:
                         HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\flags[]
 Queries value:
                         HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\0\win32[]
                         HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\helpdir[]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\control\contentindex[maxcatalogs]
 Oueries value:
                         HKLM\system\currentcontrolset\control\contentindex[leavecorruptcatalog]
 Queries value:
                         HKLM\system\currentcontrolset\control\contentindex[useole]
 Oueries value:
                         HKLM\system\currentcontrolset\control\contentindex[filtercontents]
 Queries value:
                         HKLM\system\currentcontrolset\control\contentindex[filterdelayinterval]
 Oueries value:
HKLM \setminus system \setminus current control \setminus content index [filter remaining threshold]
 Queries value:
                         HKLM\system\currentcontrolset\control\contentindex[maxfilesizefiltered]
 Queries value:
                         HKLM\system\currentcontrolset\control\contentindex[mastermergetime]
 Oueries value:
HKLM \setminus system \setminus current control \setminus content index [maxfiles ize multiplier] \\
```

Oueries value:

HKCR\.rtf[]

```
Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[threadclassfilter]
                          HKLM\system\currentcontrolset\control\contentindex[threadpriorityfilter]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex[daemonresponsetimeout]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[maxcharacterization]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[generatecharacterization]
                          HKLM\system\currentcontrolset\control\contentindex[isautoalias]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[maxautoaliasrefresh]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[isindexingw3svc]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[isindexingnntpsvc]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[isindexingimapsvc]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[isreadonly]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[isenumallowed]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[filterdirectories]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[filterfileswithunknownextensions]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[cataloginactive]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[forcepathalias]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex[propertystoremappedcache]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[propertystorebackupsize]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[secpropertystoremappedcache]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[secpropertystorebackupsize]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[forcednetpathscaninterval]
                          HKLM\system\currentcontrolset\control\contentindex[maxmergeinterval]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[threadprioritymerge]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[maxupdates]
                          HKLM\system\currentcontrolset\control\contentindex[maxwordlists]
 Queries value:
 Queries value:
HKLM \setminus system \setminus current control \setminus content index [minsizemergeword lists]
                          HKLM\system\currentcontrolset\control\contentindex[maxwordlistsize]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[minwordlistmemory]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[maxwordlistio]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[maxwordlistiodiskperf]
                          HKLM\system\currentcontrolset\control\contentindex[minwordlistbattery]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[lowresourcecheckinterval]
                          HKLM\system\currentcontrolset\control\contentindex[maxfreshdeletes]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[lowresourcesleep]
 Oueries value:
 Queries value:
{\tt HKLM \ } system \verb|\ current control \verb|\ contentindex[maxwordlist memory load]|
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[maxfreshcount]
                          HKLM\system\currentcontrolset\control\contentindex[maxqueuechunks]
 Oueries value:
 Queries value:
HKLM \setminus system \setminus current control \setminus content index [mastermerge checkpoint interval]
                          HKLM\system\currentcontrolset\control\contentindex[filterbuffersize]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[filterretries]
                          HKLM\system\currentcontrolset\control\contentindex[filterretryinterval]
 Queries value:
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[maxshadowindexsize]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[mindiskfreeforcemerge]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex[maxshadowfreeforcemerge]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[maxindexes]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[maxidealindexes]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[minmergeidletime]
                          HKLM\system\currentcontrolset\control\contentindex[maxpendingdocuments]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[minidlequerythreads]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex[maxactivequerythreads]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[maxquerytimeslice]
 Oueries value:
HKLM \setminus system \setminus current control \setminus content index [maxquery execution time] \\
                          HKLM\system\currentcontrolset\control\contentindex[w3svcinstance]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[nntpsvcinstance]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[imapsvcinstance]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[eventlogflags]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[cimiscflags]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[cicatalogflags]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[maxusnlogsize]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex[usnlogallocationdelta]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[scanbackoff]
 Oueries value:
                          HKLM\system\currentcontrolset\control\contentindex[usnreadtimeout]
 Queries value:
                          HKLM\system\currentcontrolset\control\contentindex[usnreadminsize]
```

Queries value: HKLM\system\currentcontrolset\control\contentindex[delayusnreadonlowresource]

```
HKLM\system\currentcontrolset\control\contentindex[maxdaemonvmuse]
 Oueries value:
 Oueries value:
                    HKLM\system\currentcontrolset\control\contentindex[delayedfilterretries]
 Oueries value:
                    HKLM\system\currentcontrolset\control\contentindex[maxrestrictionnodes]
                    HKLM\system\currentcontrolset\control\contentindex[stomplastaccessdelay]
 Queries value:
                    HKLM\svstem\currentcontrolset\control\contentindex[wordlistuseridle]
 Oueries value:
 Queries value:
                    HKLM\system\currentcontrolset\control\contentindex[mindiskspacetoleave]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[useole]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filtercontents]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterremainingthreshold]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxfilesizefiltered]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[mastermergetime]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[threadclassfilter]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[threadpriorityfilter]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxcharacterization]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[generatecharacterization]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isautoalias]
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxautoaliasrefresh]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isindexingw3svc]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isindexingnntpsvc]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isindexingimapsvc]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isreadonly]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isenumallowed]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterdirectories]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[forcepathalias]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[propertystoremappedcache]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[propertystorebackupsize]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[secpropertystoremappedcache]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[secpropertystorebackupsize]
 Oueries value:
Queries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxupdates]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minsizemergewordlists]
 Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxwordlistsize]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minwordlistmemory]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxwordlistiodiskperf]
 Oueries value:
```

HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minwordlistbattery]

HKLM\system\currentcontrolset\control\contentindex\catalogs\system[lowresourcecheckinterval]

Queries value:

Queries value:

- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxfreshdeletes]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[lowresourcesleep]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxwordlistmemoryload]
   Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxfreshcount]
   Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxqueuechunks]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[mastermergecheckpointinterval]
  Queries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterbuffersize]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterretries]
   Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterretryinterval]
  Queries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxshadowindexsize]
  Queries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[mindiskfreeforcemerge]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxshadowfreeforcemerge]
   Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxindexes]
   Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxidealindexes]
   Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minmergeidletime]
  Queries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxpendingdocuments]
   Oueries value:
- $\label{lem:hklmsystem} HKLM \system [minidle query threads] \\ Queries value:$
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxactivequerythreads]
  Queries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxquerytimeslice]
  Oueries value:
- $\label{lem:hklmsystem} HKLM \system [maxquery execution time] \\ Oueries value:$
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minidlerequestthreads]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minclientidletime]
   Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxactiverequestthreads]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxsimultaneousrequests]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxcachedpipes]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[wordlistuseridle]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[requesttimeout]
  Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \control \content in dex \catalogs \system \current \controls et \control \content in dex \catalogs \system \current \controls \control \content \control \contr$
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[nntpsvcinstance]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[imapsvcinstance]
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minimizeworkingset]
   Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[eventlogflags]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[cimiscflags]
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[cicatalogflags]
  Queries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxrestrictionnodes]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxusnlogsize]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[scanbackoff]
  Oueries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[startupdelay]
  Queries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[usnreadtimeout]
   Queries value:
- HKLM\system\currentcontrolset\control\contentindex\catalogs\system[usnreadminsize]
  Oueries value:

Oueries value: HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxdaemonvmuse] Oueries value: HKLM\system\currentcontrolset\control\contentindex\catalogs\system[delayedfilterretries] Oueries value: HKLM\system\currentcontrolset\control\contentindex\catalogs\system[stomplastaccessdelay] Oueries value: HKLM\system\currentcontrolset\control\contentindex\catalogs\system[mindiskspacetoleave] Oueries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity] HKCR\clsid\{1e9685e6-db6d-11d0-bb63-Oueries value: 00c04fc2f410}\inprocserver32[inprocserver32] Queries value:  $HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\inprocserver32[]$ Oueries value: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}[appid] HKCR\clsid\{1e9685e6-db6d-11d0-bb63-Oueries value: 00c04fc2f410}\inprocserver32[threadingmodel] Queries value: HKLM\system\currentcontrolset\control\networkprovider\hworder[providerorder] Queries value: HKLM\system\currentcontrolset\services\rdpnp\networkprovider[name] Queries value: HKLM\system\currentcontrolset\services\rdpnp\networkprovider[class] Oueries value: HKLM\system\currentcontrolset\services\rdpnp\networkprovider[providerpath] Oueries value: HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[name] Queries value: HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[class] Queries value: HKLM\system\currentcontrolset\services\webclient\networkprovider[name] Queries value: HKLM\system\currentcontrolset\services\webclient\networkprovider[class] Oueries value: Queries value: HKLM\system\currentcontrolset\services\webclient\networkprovider[providerpath] HKLM\software\microsoft\windows nt\currentversion\network\world full Queries value: access shared parameters[sort hyphens] Queries value: HKU\.default\control panel\international[locale] Oueries value: HKLM\system\currentcontrolset\control\session manager\appcompatibility[disableappcompat] HKLM\software\microsoft\windows Oueries value: nt\currentversion\compatibility32[cidaemon] HKLM\software\microsoft\windows nt\currentversion\ime Queries value: compatibility[cidaemon] HKCR\clsid\{aa205a4d-681f-11d0-a243-Oueries value: 08002b36fca4}\inprocserver32[inprocserver32] HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\inprocserver32[] Oueries value: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}[appid] Oueries value: HKCR\clsid\{aa205a4d-681f-11d0-a243-Oueries value: 08002b36fca4}\inprocserver32[threadingmodel] Oueries value: HKLM\system\currentcontrolset\control\contentindex[filtertrackers] Oueries value: Queries value: HKLM\system\currentcontrolset\control\contentindex\catalogs\system\scopes[] Oueries value: HKLM\system\currentcontrolset\control\contentindex\language\dutch\_dutch[locale] HKLM\system\currentcontrolset\control\contentindex\language\english\_uk[locale] Queries value: HKLM\system\currentcontrolset\control\contentindex\language\english\_us[locale] Oueries value: HKLM\system\currentcontrolset\control\contentindex\language\french\_french[locale] HKLM\system\currentcontrolset\control\contentindex\language\german\_german[locale] Oueries value: HKLM\system\currentcontrolset\control\contentindex\language\italian\_italian[locale] Oueries value: HKLM\system\currentcontrolset\control\contentindex\language\neutral[locale] Queries value: Oueries value: HKLM\system\currentcontrolset\control\contentindex\language\neutral[noisefile] HKCR\clsid\{369647e0-17b0-11ce-9950-Oueries value: 00aa004bbb1f}\inprocserver32[inprocserver32]  $\label{local-equation} $HKCR\clsid{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprocserver32[]$ Queries value: Queries value: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}[appid] Oueries value: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprocserver32[threadingmodel]

3d01-b289-befc77a11a1e}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-4ca4-87b4-2f83217002ff}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{350c97b0-3d7c-4ee8-baa9-00bcb3d54227}[installlocation]

Oueries value:

```
Queries value:
                                               4037-7777-5f2748764d10}[installlocation]
   Queries value:
                                               0409-0000-0000000ff1ce}[installlocation]
                                               Oueries value:
11d3-8cfe-0150048383c9}[installlocation]
   Queries value:
                                               HKLM \ software \ microsoft \ windows \ current version \ uninstall \ \{95120000-003f-00000\} \ description \ desc
0409-0000-0000000ff1ce}[installlocation]
                                               Queries value:
0409-0000-0000000ff1ce}[installlocation]
                                               HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-
   Oueries value:
3813-a88d-b8dccde8f8c7}[installlocation]
                                               Queries value:
1033-7b44-a9300000001}[installlocation]
                                               Queries value:
3f2d-899a-6a1d67f2073f}[installlocation]
                                               HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-
   Oueries value:
4027-b136-2b3e1f5ab6e2}[installlocation]
                                              HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-
   Queries value:
36ca-84d3-9f4dcf5c5bd9}[installlocation]
                                               HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-
   Queries value:
36ca-84d3-9f4dcf5c5bd9}.kb953595[installlocation]
   Oueries value:
                                              HKCR\.ini\persistenthandler[]
                                               HKCR\clsid\{5e941d80-bf96-11cd-b579-
   Queries value:
08002b30bfeb\\ persistent add in sregistered \\ \{89bcb740-6119-101a-bcb7-00dd010655af\}[]
                                              HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprocserver32[]
   Queries value:
                                               HKCR\clsid\{c1243ca0-bf96-11cd-b579-
   Queries value:
08002b30bfeb}\inprocserver32[threadingmodel]
                                              HKCR\clsid\{c1243ca0-bf96-11cd-b579-
   Oueries value:
08002b30bfeb}\inprocserver32[inprocserver32]
                                              HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}[appid]
   Oueries value:
   Queries value:
                                               HKLM\system\currentcontrolset\control\contentindex[maxtextfilterbytes]
   Queries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nonethood]
   Oueries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
   Oueries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
   Oueries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
   Oueries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
                                               \label{local-condition} HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\ \ inprocserver32[]
   Oueries value:
   Queries value:
HKU \verb|\| . default \verb|\| software \verb|\| microsoft \verb|\| windows \verb|\| current version \verb|\| policies \verb|\| explorer [dontshow superhidden] | the first that the 
HKU\.default\software\microsoft\windows\currentversion\explorer[shellstate]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\startmenu\startpanel[defaultstartpaneloff]
   Oueries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
   Queries value:
HKU\. default\software\mbox{\mbox{$m$icrosoft\windows\currentversion\policies\explorer[noactivedesktop]}}
   Queries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Oueries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[classicshell]
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
   Queries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
   Oueries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                                               HKCR\directory[docobject]
   Oueries value:
                                               HKCR\directory[browseinplace]
   Queries value:
   Queries value:
                                               HKCR\directory[isshortcut]
   Queries value:
                                               HKCR\directory[alwaysshowext]
                                               HKCR\directory[nevershowext]
   Oueries value:
   Queries value:
HKU\. default\software\mbox{\tt microsoft\windows\currentversion\policies\explorer[allowfileclsid]unctions]}
   Oueries value:
                                               HKCR\.ini[perceivedtype]
   Queries value:
                                               HKCR\inifile[docobject]
   Queries value:
                                               HKCR\inifile[browseinplace]
   Oueries value:
                                               HKCR\inifile[isshortcut]
   Queries value:
                                               HKCR\inifile[alwaysshowext]
   Oueries value:
                                               HKCR\inifile[nevershowext]
                                               HKCR\.sam[]
   Oueries value:
   Oueries value:
                                               HKCR\.sam[perceivedtype]
```

Queries value: HKCR\.sam[perceivedtype]
Queries value: HKCR\.sam[docobject]
Queries value: HKCR\.sam[browseinplace]
Queries value: HKCR\.sam[isshortcut]

```
Oueries value:
                          HKCR\.sam[alwaysshowext]
                          HKCR\.sam[nevershowext]
 Oueries value:
                          HKCR\.xls\persistenthandler[]
 Oueries value:
                          HKCR\clsid\{98de59a0-d175-11cd-a7bd-
 Queries value:
00006b827d94\\ \texttt{persistentaddinsregistered} \{89bcb740-6119-101a-bcb7-00dd010655af\}[]
 Queries value:
                          HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprocserver32[]
                          HKCR\clsid\{f07f3920-7b8c-11cf-9be8-
 Oueries value:
00aa004b9986}\inprocserver32[threadingmodel]
                          HKCR \verb|\clsid| \{f07f3920-7b8c-11cf-9be8-
 Oueries value:
00aa004b9986}\inprocserver32[inprocserver32]
                          HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}[appid]
 Oueries value:
 Queries value:
                          HKU\.default\control panel\international[scurrency]
 Oueries value:
                          HKU\.default\control panel\international[icurrency]
 Oueries value:
                          HKU\.default\control panel\international[inegcurr]
 Queries value:
                          HKU\.default\control panel\international[icurrdigits]
 Oueries value:
                          HKU\.default\control panel\international[smondecimalsep]
 Oueries value:
                          HKU\.default\control panel\international[smonthousandsep]
 Queries value:
                          HKU\.default\control panel\international[idigits]
 Oueries value:
                          HKU\.default\control panel\international[ilzero]
 Oueries value:
                          HKU\.default\control panel\international[sdecimal]
 Queries value:
                          HKU\.default\control panel\international[sthousand]
 Queries value:
                          HKU\.default\control panel\international[itime]
 Oueries value:
                          HKU\.default\control panel\international[itlzero]
 Queries value:
                          HKU\.default\control panel\international[itimeprefix]
 Queries value:
                          HKU\.default\control panel\international[s1159]
                          HKU \verb|\|.default\\| control panel\\| international[s2359]
 Oueries value:
 Queries value:
                          HKU\.default\control panel\international[stime]
 Queries value:
                          HKU\.default\control panel\international[sshortdate]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\language\english_uk[wbreakerclass]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\language\english_uk[noisefile]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\language\english_us[wbreakerclass]
 Oueries value:
HKLM\system\currentcontrolset\control\contentindex\language\english_us[stemmerclass]
HKLM\system\currentcontrolset\control\contentindex\language\english_us[noisefile]
 Queries value:
                          HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-
0090272fa362}\inprocserver32[inprocserver32]
                          HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserver32[]
 Oueries value:
                          HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}[appid]
 Oueries value:
                          HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-
 Oueries value:
0090272fa362}\inprocserver32[threadingmodel]
 Oueries value:
                          HKCR\.xls[perceivedtype]
 Queries value:
                          HKCR\excelviewer.sheet.8[docobject]
 Oueries value:
                          HKCR\svstemfileassociations\.xls[docobject]
 Oueries value:
                          HKCR\excelviewer.sheet.8[browseinplace]
 Oueries value:
                          HKCR\systemfileassociations\.xls[browseinplace]
 Oueries value:
                          HKCR\excelviewer.sheet.8[isshortcut]
 Oueries value:
                          HKCR\systemfileassociations\.xls[isshortcut]
 Queries value:
                          HKCR\excelviewer.sheet.8[alwaysshowext]
 Oueries value:
                          HKCR\systemfileassociations\.xls[alwaysshowext]
 Queries value:
                          HKCR\excelviewer.sheet.8[nevershowext]
 Oueries value:
                          HKCR\systemfileassociations\.xls[nevershowext]
 Oueries value:
                          HKCR\.wk4[]
 Oueries value:
                          HKCR\.wk4[perceivedtype]
                          HKCR\.wk4[docobject]
 Queries value:
 Queries value:
                          HKCR\.wk4[browseinplace]
                          HKCR\.wk4[isshortcut]
 Oueries value:
                          HKCR\.wk4[alwaysshowext]
 Queries value:
 Queries value:
                          HKCR\.wk4[nevershowext]
                          HKCR\.ppt\persistenthandler[]
 Oueries value:
                          HKCR\.shw[]
 Oueries value:
 Queries value:
                          HKCR\.shw[perceivedtype]
 Oueries value:
                          HKCR\.shw[docobject]
 Queries value:
                          HKCR\.shw[browseinplace]
                          HKCR\.shw[isshortcut]
 Oueries value:
 Queries value:
                          HKCR\.shw[alwaysshowext]
                          HKCR\.shw[nevershowext]
 Oueries value:
 Oueries value:
                          HKCR\.wb2[1
 Oueries value:
                          HKCR\.wb2[perceivedtype]
 Queries value:
                          HKCR\.wb2[docobject]
 Oueries value:
                          HKCR\.wb2[browseinplace]
 Queries value:
                          HKCR\.wb2[isshortcut]
 Oueries value:
                          HKCR\.wb2[alwaysshowext]
 Oueries value:
                          HKCR\.wb2[nevershowext]
 Oueries value:
                          HKCR\.wav\persistenthandler[]
 Queries value:
                          HKCR\clsid\{098f2470-bae0-11cd-b579-
08002b30bfeb\} \persistent add in sregistered \verb|\{89bcb740-6119-101a-bcb7-00dd010655af\}|[]
 Queries value:
                          HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\tinprocserver32[]
```

```
HKCR\clsid\{c3278e90-bea7-11cd-b579-
 Queries value:
08002b30bfeb}\inprocserver32[threadingmodel]
 Oueries value:
                          HKCR\clsid\{c3278e90-bea7-11cd-b579-
08002b30bfeb}\inprocserver32[inprocserver32]
                          HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}[appid]
 Oueries value:
 Queries value:
                          HKCR\soundrec[docobject]
 Oueries value:
                          HKCR\systemfileassociations\.wav[docobject]
 Oueries value:
                          HKCR\systemfileassociations\audio[docobject]
 Oueries value:
                          HKCR\soundrec[browseinplace]
 Oueries value:
                          HKCR\systemfileassociations\.wav[browseinplace]
 Oueries value:
                          HKCR\systemfileassociations\audio[browseinplace]
 Queries value:
                          HKCR\soundrec[isshortcut]
 Oueries value:
                          HKCR\systemfileassociations\.wav[isshortcut]
                          HKCR\systemfileassociations\audio[isshortcut]
 Oueries value:
 Queries value:
                          HKCR\soundrec[alwaysshowext]
 Queries value:
                          HKCR\systemfileassociations\.wav[alwaysshowext]
                          HKCR\systemfileassociations\audio[alwaysshowext]
 Oueries value:
 Queries value:
                          HKCR\soundrec[nevershowext]
 Queries value:
                          HKCR\systemfileassociations\.wav[nevershowext]
 Oueries value:
                          HKCR\systemfileassociations\audio[nevershowext]
 Queries value:
                          HKCR\systemfileassociations\.wav\shellex\propertyhandler[]
 Queries value:
                          HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\inprocserver32[]
                          HKCR\clsid\{e4b29f9d-d390-480b-92fd-
 Oueries value:
7ddb47101d71}\inprocserver32[loadwithoutcom]
                          HKLM\software\microsoft\windows\currentversion\shell
 Queries value:
extensions\blocked[{e4b29f9d-d390-480b-92fd-7ddb47101d71}]
                          HKU\.default\software\microsoft\windows\currentversion\shell
 Queries value:
extensions\blocked[{e4b29f9d-d390-480b-92fd-7ddb47101d71}]
 Oueries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{e4b29f9d-d390-480b-92fd-7ddb47101d71} {0000010b-0000-0000-c000-0000000000046}
0x401]
 Queries value:
                          HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached[{e4b29f9d-d390-480b-92fd-7ddb47101d71} {0000010b-0000-0000-c000-000000000046}}
0x4011
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\compatibility32[verclsid]
                          HKLM\software\microsoft\windows nt\currentversion\ime
 Queries value:
compatibility[verclsid]
                          HKCR\clsid\{e4b29f9d-d390-480b-92fd-
 Queries value:
7ddb47101d71}\inprocserver32[inprocserver32]
                          HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}[appid]
 Oueries value:
                          HKCR\clsid\{e4b29f9d-d390-480b-92fd-
 Queries value:
7ddb47101d71}\inprocserver32[threadingmodel]
 Queries value:
                          HKCR\.doc\persistenthandler[]
 Oueries value:
                          HKCR\.doc[perceivedtype]
 Queries value:
                          HKCR\wordview.document.8[docobject]
 Oueries value:
                          HKCR\svstemfileassociations\.doc[docobject]
 Queries value:
                          HKCR\wordview.document.8[browseinplace]
 Oueries value:
                          HKCR\systemfileassociations\.doc[browseinplace]
 Oueries value:
                          HKCR\wordview.document.8[isshortcut]
 Queries value:
                          HKCR\systemfileassociations\.doc[isshortcut]
 Queries value:
                          HKCR\wordview.document.8[alwaysshowext]
 Oueries value:
                          HKCR\systemfileassociations\.doc[alwaysshowext]
 Queries value:
                          HKCR\wordview.document.8[nevershowext]
 Oueries value:
                          HKCR\systemfileassociations\.doc[nevershowext]
 Oueries value:
                          HKCR\.wpd[]
                          HKCR\.wpd[perceivedtype]
 Oueries value:
                          HKCR\.wpd[docobject]
 Queries value:
 Queries value:
                          HKCR\.wpd[browseinplace]
 Oueries value:
                          HKCR\.wpd[isshortcut]
                          HKCR\.wpd[alwaysshowext]
 Queries value:
 Oueries value:
                          HKCR\.wpd[nevershowext]
 Queries value:
                          HKCR\.wpg[]
                          HKCR\.wpg[perceivedtype]
 Oueries value:
 Queries value:
                          HKCR\.wpg[docobject]
 Queries value:
                          HKCR\.wpg[browseinplace]
 Queries value:
                          HKCR\.wpg[isshortcut]
 Oueries value:
                          HKCR\.wpg[alwaysshowext]
 Queries value:
                          HKCR\.wpg[nevershowext]
 Oueries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
 Queries value:
                          HKCR\.lnk[]
 Queries value:
                          HKCR\lnkfile\clsid[]
                          HKCR\clsid\{00021401-0000-0000-c000-00000000046}\persistenthandler[]
 Oueries value:
 Queries value:
                          HKCR\clsid\{00021401-0000-0000-c000-
00000000046}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
                          HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserver32[]
 Oueries value:
 Oueries value:
                          HKCR\clsid\{00021401-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
                          HKCR\clsid\{00021401-0000-0000-c000-
 Oueries value:
00000000046}\inprocserver32[inprocserver32]
```

```
HKCR\clsid\{00021401-0000-0000-c000-00000000046}[appid]
   Oueries value:
   Oueries value:
                                               HKLM\software\microsoft\ole[defaultaccesspermission]
   Oueries value:
                                               HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
   Queries value:
                                               HKLM\software\microsoft\com3[gipactivitybypass]
                                               HKCR\interface\{0000010b-0000-0000-c000-00000000046}\proxystubclsid32[]
   Oueries value:
   Queries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[normalizelinknetpidls]
   Oueries value:
                                               HKCR\network\sharinghandler[]
   Oueries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[comparejunctionness]
   Oueries value:
                                               HKCR\exefile[docobiect]
   Queries value:
                                               HKCR\exefile[browseinplace]
   Oueries value:
                                               HKCR\exefile[isshortcut]
                                               HKCR\exefile[alwaysshowext]
   Oueries value:
   Queries value:
                                               HKCR\exefile[nevershowext]
   Queries value:
                                               HKCR\lnkfile\shellex\iconhandler[]
                                               HKCR\lnkfile[docobject]
   Oueries value:
   Queries value:
                                               HKCR\.lnk[perceivedtype]
   Queries value:
                                               HKCR\lnkfile[browseinplace]
   Oueries value:
                                               HKCR\lnkfile[isshortcut]
   Queries value:
                                               HKCR\lnkfile[alwaysshowext]
   Queries value:
                                               HKCR\lnkfile[nevershowext]
                                               HKLM\software\microsoft\windows\currentversion[programfilesdir]
   Oueries value:
   Queries value:
                                               HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
                                               HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\inprocserver32[loadwithoutcom]
                                               HKLM\software\microsoft\windows\currentversion\shell
   Queries value:
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
                                               HKU\.default\software\microsoft\windows\currentversion\shell
   Oueries value:
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
                                               HKLM\software\microsoft\windows\currentversion\shell
   Oueries value:
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}}
0x401]
   Queries value:
                                               HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}}
0x4011
                                               HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\inprocserver32[inprocserver32]
                                               HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
   Queries value:
                                               HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\inprocserver32[threadingmodel]
                                               HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
   Queries value:
   Oueries value:
                                               HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
   Queries value:
                                               HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
                                               HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
   Queries value:
ab78-1084642581fb]
   Queries value:
                                               HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000000
   Queries value:
                                               HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
                                               HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\internet explorer\setup[installstarted]
                                               \label{local-eq:hkcr} \begin{tabular}{ll} HKCR \end{tabular} HKCR \end{tabular} $$ 101b-a2bc-00aa00404770 \end{tabular} $$ 101b-a2bc-00aa0040470 \end{tabular} $$ 101b-a2bc-00aa0040404000000000000000000000
   Queries value:
                                               HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
   Oueries value:
   Queries value:
                                               HKCR \ interface \ \{000214e6-0000-0000-c000-00000000046\} \ proxystubclsid32[]
   Oueries value:
                                               HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32[]
   Oueries value:
                                               HKCR\.zfsendtotarget[perceivedtype]
                                               HKCR \land \{888dca60-fc0a-11cf-8f0f-00c04fd7d062\} [docobject]
   Oueries value:
                                               HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}[browseinplace]
   Queries value:
   Queries value:
                                               HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}[isshortcut]
                                               HKCR \verb|\clsid|{888dca60-fc0a-11cf-8f0f-00c04fd7d062}[always showext]|
   Oueries value:
                                               HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}[nevershowext]
   Queries value:
   Oueries value:
                                               HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
   Oueries value:
                                               HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common documents]
   Queries value:
                                               HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| explorer \verb|\| user | leaves to the constraint of the cons
shell folders[desktop]
   Oueries value:
                                               HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common desktop]
                                               HKCR\icofile[docobject]
   Oueries value:
                                               HKCR\systemfileassociations\image[docobject]
   Oueries value:
   Queries value:
                                               HKCR\icofile[browseinplace]
   Queries value:
                                               HKCR\systemfileassociations\image[browseinplace]
   Oueries value:
                                               HKCR\icofile[isshortcut]
   Queries value:
                                               HKCR\systemfileassociations\image[isshortcut]
   Oueries value:
                                               HKCR\icofile[alwaysshowext]
                                               HKCR\systemfileassociations\image[alwaysshowext]
   Oueries value:
   Oueries value:
                                               HKCR\icofile[nevershowext]
   Queries value:
                                               HKCR\systemfileassociations\image[nevershowext]
                                               HKCR\.chm[]
   Oueries value:
   Queries value:
                                               HKCR\.chm[perceivedtype]
```

```
Oueries value:
                           HKCR\chm.file[docobject]
 Oueries value:
                           HKCR\chm.file[browseinplace]
 Oueries value:
                           HKCR\chm.file[isshortcut]
 Queries value:
                           HKCR\chm.file[alwaysshowext]
 Oueries value:
                           HKCR\chm.file[nevershowext]
 Queries value:
                           HKCR\.msc[]
 Oueries value:
                           HKCR\mscfile\shellex\iconhandler[]
 Oueries value:
                           HKCR\mscfile[docobject]
 Oueries value:
                           HKCR\.msc[perceivedtype]
 Oueries value:
                           HKCR\mscfile[browseinplace]
 Oueries value:
                           HKCR\mscfile[isshortcut]
 Queries value:
                           HKCR\mscfile[alwaysshowext]
 Oueries value:
                           HKCR\mscfile[nevershowext]
                           HKCR\.cpl[perceivedtype]
 Oueries value:
 Queries value:
                           HKCR\cplfile[docobject]
 Queries value:
                           HKCR\cplfile[browseinplace]
                           HKCR\cplfile[isshortcut]
 Oueries value:
 Queries value:
                           HKCR\cplfile[alwaysshowext]
 Oueries value:
                           HKCR\cplfile[nevershowext]
                           HKCR\.desklink\persistenthandler[]
 Oueries value:
 Queries value:
                           HKCR\.desklink[perceivedtype]
 Queries value:
                           HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}[docobject]
                           HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}[browseinplace]
 Oueries value:
 Queries value:
                           HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}[isshortcut]
 Queries value:
                           HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}[always showext]
                           \label{lem:hkcrclsid} $$HKCR\clsid{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}[nevershowext]$
 Oueries value:
                           HKCR\.mapimail\persistenthandler[]
 Queries value:
 Queries value:
                           HKCR\.mapimail[perceivedtype]
                           HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}[docobject]
 Oueries value:
                           HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}[browseinplace]
 Queries value:
                           HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}[isshortcut]
 Oueries value:
                           \label{local-equation} HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce} [always showext]
 Queries value:
                           \label{localization} HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce} [nevershowext]
 Queries value:
 Queries value:
                           HKCR\.dat[]
 Oueries value:
                           HKCR\.dat[perceivedtype]
                           HKCR\.dat[docobject]
 Queries value:
 Oueries value:
                           HKCR\.dat[browseinplace]
 Oueries value:
                           HKCR\.dat[isshortcut]
                           HKCR\.dat[alwaysshowext]
 Queries value:
 Queries value:
                           HKCR\.dat[nevershowext]
 Oueries value:
                           HKCR\.jpg\persistenthandler[]
 Queries value:
                           HKCR\jpegfile[docobject]
                           HKCR\systemfileassociations\.jpg[docobject]
 Oueries value:
 Oueries value:
                           HKCR\jpegfile[browseinplace]
 Oueries value:
                           HKCR\systemfileassociations\.jpg[browseinplace]
 Queries value:
                           HKCR\jpegfile[isshortcut]
 Oueries value:
                           HKCR\systemfileassociations\.jpg[isshortcut]
 Queries value:
                           HKCR\jpegfile[alwaysshowext]
 Oueries value:
                           HKCR\systemfileassociations\.jpg[alwaysshowext]
 Queries value:
                           HKCR\jpegfile[nevershowext]
 Oueries value:
                           HKCR\systemfileassociations\.jpg[nevershowext]
 Oueries value:
                           HKCR\systemfileassociations\image\shellex\propertyhandler[]
 Queries value:
                           HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprocserver32[]
 Queries value:
                           HKCR\clsid\{eb9b1153-3b57-4e68-959a-
a3266bc3d7fe}\inprocserver32[loadwithoutcom]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}]
                          HKU\.default\software\microsoft\windows\currentversion\shell
 Oueries value:
extensions\blocked[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}]
                           HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe} {0000010b-0000-0000-c000-000000000046}}
0x4011
                           HKU\.default\software\microsoft\windows\currentversion\shell
 Queries value:
extensions\cached[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe} {0000010b-0000-0000-c000-000000000046}}
0x4011
                           HKCR\clsid\{eb9b1153-3b57-4e68-959a-
 Oueries value:
a3266bc3d7fe}\inprocserver32[inprocserver32]
                          HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}[appid]
 Queries value:
 Queries value:
                           HKCR\clsid\{eb9b1153-3b57-4e68-959a-
a3266bc3d7fe}\inprocserver32[threadingmodel]
 Queries value:
                           HKCR\.wpl[]
 Oueries value:
                           HKCR\.wpl[perceivedtype]
 Oueries value:
                           HKCR\wplfile[docobiect]
 Queries value:
                           HKCR\systemfileassociations\.wpl[docobject]
 Queries value:
                           HKCR\wplfile[browseinplace]
 Oueries value:
                           HKCR\systemfileassociations\.wpl[browseinplace]
 Queries value:
                           HKCR\wplfile[isshortcut]
 Oueries value:
                           HKCR\systemfileassociations\.wpl[isshortcut]
                           HKCR\wplfile[alwaysshowext]
 Oueries value:
 Oueries value:
                           HKCR\systemfileassociations\.wpl[alwaysshowext]
 Queries value:
                           HKCR\wplfile[nevershowext]
 Oueries value:
                           HKCR\systemfileassociations\.wpl[nevershowext]
 Queries value:
                           HKCR\.wma\persistenthandler[]
```

```
Oueries value:
                                               HKCR\wmafile[docobject]
                                               HKCR\systemfileassociations\.wma[docobject]
   Oueries value:
   Oueries value:
                                               HKCR\wmafile[browseinplace]
                                               HKCR\systemfileassociations\.wma[browseinplace]
   Queries value:
   Oueries value:
                                               HKCR\wmafile[isshortcut]
   Queries value:
                                               HKCR\systemfileassociations\.wma[isshortcut]
   Oueries value:
                                               HKCR\wmafile[alwaysshowext]
   Oueries value:
                                               HKCR\systemfileassociations\.wma[alwaysshowext]
   Oueries value:
                                               HKCR\wmafile[nevershowext]
   Oueries value:
                                               HKCR\systemfileassociations\.wma[nevershowext]
                                               HKCR\systemfileassociations\.wma\shellex\propertyhandler[]
   Oueries value:
   Queries value:
                                               HKCR\clsid\{875cb1a1-0f29-45de-a1ae-cfb4950d0b78}\tinprocserver32[]
   Queries value:
                                               HKCR\clsid\{875cb1a1-0f29-45de-a1ae-
cfb4950d0b78}\inprocserver32[loadwithoutcom]
   Queries value:
                                               HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{875cb1a1-0f29-45de-a1ae-cfb4950d0b78}]
                                               HKU\.default\software\microsoft\windows\currentversion\shell
   Queries value:
extensions\blocked[{875cb1a1-0f29-45de-a1ae-cfb4950d0b78}]
   Queries value:
                                               HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{875cb1a1-0f29-45de-a1ae-cfb4950d0b78} {0000010b-0000-0000-c000-000000000046}
0x401]
   Queries value:
                                               HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached[{875cb1a1-0f29-45de-a1ae-cfb4950d0b78} {0000010b-0000-0000-c000-000000000046}}
0x401]
   Queries value:
                                               HKCR\.sst[]
   Queries value:
                                               HKCR\.sst[perceivedtype]
   Queries value:
                                               HKCR\certificatestorefile[docobject]
   Queries value:
                                               HKCR\certificatestorefile[browseinplace]
   Queries value:
                                               HKCR\certificatestorefile[isshortcut]
   Queries value:
                                               HKCR\certificatestorefile[alwaysshowext]
   Queries value:
                                               HKCR\certificatestorefile[nevershowext]
   Queries value:
                                               HKCR\.mydocs\persistenthandler[]
                                               HKCR\.mydocs[perceivedtype]
   Queries value:
   Queries value:
                                               HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}[docobject]
                                               HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}[browseinplace]
   Oueries value:
                                               HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}[isshortcut]
   Queries value:
                                               HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}[alwaysshowext]
   Oueries value:
                                               HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}[nevershowext]
   Oueries value:
                                               HKCR\.url\persistenthandler[]
   Queries value:
                                               HKCR\clsid\{8cd34779-9f10-4f9b-adfb-
   Queries value:
b3 faeabdab5a \} \\ versistent add in sregistered \\ \{89bcb740-6119-101a-bcb7-00dd010655af\}[]
                                               HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\tinprocserver32[]
   Queries value:
   Oueries value:
                                               HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-
8e7c3d18aeaf}\inprocserver32[threadingmodel]
                                               HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-
   Oueries value:
8e7c3d18aeaf}\inprocserver32[inprocserver32]
                                               HKCR \verb|\clsid|{7}ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}[appid]
   Queries value:
                                               HKCR\clsid\{06eee834-461c-42c2-8dcf-
   Queries value:
1502b527b1f9}\inprocserver32[inprocserver32]
                                               Queries value:
                                               HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}[appid]
   Oueries value:
                                               HKCR\clsid\{06eee834-461c-42c2-8dcf-
   Oueries value:
1502b527b1f9}\inprocserver32[threadingmodel]
                                               HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\nstance[clsid]
   Queries value:
                                               HKCR\clsid\{06eee834-461c-42c2-8dcf-
   Oueries value:
1502b527b1f9}\instance[loadwithoutcom]
                                               HKCR\clsid\{942bc614-676c-464e-b384-
   Oueries value:
d3202aaa02da}\inprocserver32[inprocserver32]
                                               HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\tinprocserver32[]
   Oueries value:
                                               HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}[appid]
   Queries value:
   Queries value:
                                               HKCR\clsid\{942bc614-676c-464e-b384-
\verb|d3202aaa02da| \land \verb|inprocserver32[threadingmodel]|
                                               HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[disableimprovedzonecheck]
   Queries value:
                                               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[cidaemon.exe]
                                              HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[*]
   Queries value:
                                               HKCR\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}\inprocserver32[inprocserver32]
                                               \label{local-equation} HKCR\clsid \ \{4516cee1-97da-4030-a444-2d8e296b96b6\} \ \ inprocserver 32[]
   Queries value:
                                               HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}[appid]
   Oueries value:
   Oueries value:
                                               HKCR\clsid\{4516cee1-97da-4030-a444-
2d8e296b96b6}\inprocserver32[threadingmodel]
   Queries value:
                                               HKCR\clsid\{6f237df9-9ddb-47ad-b218-
400d54c286ad}\inprocserver32\inprocserver321
                                               HKCR \c1sid \end{6f237df9-9ddb-47ad-b218-400d54c286ad} \label{fig:equation} In processing the control of the 
   Queries value:
                                               HKCR \clsid \end{6f237df9-9ddb-47ad-b218-400d54c286ad} \clappid \clappid \end{6f237df9-9ddb-47ad-b218-400d54c286ad} \clappid \cl
   Oueries value:
                                               HKCR\clsid\{6f237df9-9ddb-47ad-b218-
   Oueries value:
400d54c286ad}\inprocserver32[threadingmodel]
   Queries value:
                                               HKCR\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-00000000046}\2[section]
   Queries value:
                                               HKCR\clsid\{06eee834-461c-42c2-8dcf-
```

```
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}[section]
                         HKCR\clsid\{06eee834-461c-42c2-8dcf-
 Oueries value:
1502b527b1f9 \\ instance \\ property sets to rage \\ \{000214a0-0000-0000-c000-0000000000046\} \\ \\ [key]
                          HKCR\clsid\{06eee834-461c-42c2-8dcf-
 Queries value:
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\2[vartype]
 Queries value:
                          HKCR\internetshortcut\shellex\iconhandler[]
 Oueries value:
                          HKCR\internetshortcut[docobject]
 Oueries value:
                          HKCR\.url[perceivedtype]
 Oueries value:
                          HKCR\internetshortcut[browseinplace]
 Oueries value:
                          HKCR\internetshortcut[isshortcut]
 Oueries value:
                          HKCR\internetshortcut[alwaysshowext]
 Queries value:
                          HKCR\internetshortcut[nevershowext]
 Oueries value:
                          HKCR\internetshortcut\shellex\propertyhandler[]
                          HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\inprocserver32[]
 Oueries value:
 Queries value:
                          HKCR\clsid\{fbf23b40-e3f0-101b-8488-
00aa003e56f8}\inprocserver32[loadwithoutcom]
                         HKLM\software\microsoft\windows\currentversion\shell
 Oueries value:
extensions\blocked[{fbf23b40-e3f0-101b-8488-00aa003e56f8}]
                         HKU\.default\software\microsoft\windows\currentversion\shell
 Queries value:
extensions\blocked[{fbf23b40-e3f0-101b-8488-00aa003e56f8}]
                         HKLM\software\microsoft\windows\currentversion\shell
 Queries value:
extensions\cached[{fbf23b40-e3f0-101b-8488-00aa003e56f8} {0000010b-0000-0000-c000-000000000046}}
0x4011
 Queries value:
                          HKU\.default\software\microsoft\windows\currentversion\shell
0x4011
                          HKCR\clsid\{fbf23b40-e3f0-101b-8488-
 Queries value:
00aa003e56f8}\inprocserver32[inprocserver32]
                         HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}[appid]
 Oueries value:
 Queries value:
                          HKCR\appid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}[dllsurrogate]
 Queries value:
                         HKCR\clsid\{fbf23b40-e3f0-101b-8488-
00aa003e56f8}\inprocserver32[threadingmodel]
                          HKCR\.txt\persistenthandler[]
 Queries value:
 Queries value:
                          HKCR\.txt[perceivedtype]
 Oueries value:
                          HKCR\txtfile[docobject]
                          HKCR\systemfileassociations\text[docobject]
 Queries value:
 Oueries value:
                          HKCR\txtfile[browseinplace]
 Oueries value:
                          HKCR\systemfileassociations\text[browseinplace]
                          HKCR\txtfile[isshortcut]
 Queries value:
                          HKCR\systemfileassociations\text[isshortcut]
 Queries value:
 Oueries value:
                          HKCR\txtfile[alwaysshowext]
                          {\tt HKCR \ } {\tt Systemfile associations \ } {\tt text[always showext]}
 Queries value:
 Oueries value:
                          HKCR\txtfile[nevershowext]
                          HKCR\systemfileassociations\text[nevershowext]
 Oueries value:
 Oueries value:
                          HKCR\.bat\persistenthandler[]
                          HKCR\batfile[docobject]
 Queries value:
 Oueries value:
                          HKCR\batfile[browseinplace]
 Queries value:
                          HKCR\batfile[isshortcut]
 Oueries value:
                          HKCR\batfile[alwaysshowext]
 Queries value:
                          HKCR\batfile[nevershowext]
 Oueries value:
                          HKCR\.sys\persistenthandler[]
                          HKCR\.sys[perceivedtype]
 Oueries value:
 Queries value:
                          HKCR\sysfile[docobject]
                          HKCR\sysfile[browseinplace]
 Queries value:
 Oueries value:
                          HKCR\svsfile[isshortcut]
 Queries value:
                          HKCR\sysfile[alwaysshowext]
 Oueries value:
                          HKCR\sysfile[nevershowext]
 Oueries value:
                          HKCR\.log\persistenthandler[]
 Queries value:
                          HKCR\.log[perceivedtype]
 Queries value:
                          HKCR\.com\persistenthandler[]
 Queries value:
                          HKCR\comfile[docobject]
 Oueries value:
                          HKCR\comfile[browseinplace]
                          HKCR\comfile[isshortcut]
 Queries value:
 Queries value:
                          HKCR\comfile[alwaysshowext]
 Oueries value:
                          HKCR\comfile[nevershowext]
 Oueries value:
                          HKCR\.bmp\persistenthandler[]
 Queries value:
                          HKCR\paint.picture[docobject]
 Oueries value:
                          HKCR\systemfileassociations\.bmp[docobject]
 Queries value:
                          HKCR\paint.picture[browseinplace]
 Oueries value:
                          HKCR\systemfileassociations\.bmp[browseinplace]
 Queries value:
                          HKCR\paint.picture[isshortcut]
 Oueries value:
                          HKCR\systemfileassociations\.bmp[isshortcut]
 Oueries value:
                          HKCR\paint.picture[alwaysshowext]
 Queries value:
                          HKCR\systemfileassociations\.bmp[alwaysshowext]
 Queries value:
                          HKCR\paint.picture[nevershowext]
 Oueries value:
                          HKCR\systemfileassociations\.bmp[nevershowext]
 Queries value:
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
 Oueries value:
 Oueries value:
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]
 Queries value:
                         HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[logging directory]
```

```
Oueries value:
                          HKLM\software\microsoft\wbem\cimom[logging]
 Oueries value:
                          HKLM\software\microsoft\wbem\cimom[log file max size]
 Oueries value:
                          HKLM\software\microsoft\wbem\cimom[repository directory]
                          HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
 Queries value:
                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[dllsurrogate]
 Oueries value:
 Queries value:
                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
                          HKCR \land f309ad18-d86a-11d0-a075-00c04fb68820 \rbrace \land proxystubclsid32[]
 Oueries value:
                         HKCR\clsid\{7c857801-7381-11cf-884d-
 Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
 Oueries value:
                         HKCR\.exe\persistenthandler[]
 Oueries value:
 Queries value:
                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
 Oueries value:
                         HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
 Queries value:
                         HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]
 Oueries value:
                         HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
 Oueries value:
                         HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
 Queries value:
                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
 Oueries value:
                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
 Queries value:
                         HKCR\.scf[]
 Queries value:
                         HKCR\shcmdfile\clsid[]
                         HKCR\clsid\{d68af00a-29cb-43fa-8504-
 Oueries value:
ce99a996d9ea}\inprocserver32[threadingmodel]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
                         HKCR\shcmdfile\shellex\iconhandler[]
 Queries value:
 Queries value:
                         HKCR\shcmdfile[docobject]
                         HKCR\.scf[perceivedtype]
 Oueries value:
 Queries value:
                         HKCR\shcmdfile[browseinplace]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [prioritize record data]
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
 Oueries value:
                         HKCR\shcmdfile[isshortcut]
 Oueries value:
                         HKCR\shcmdfile[alwaysshowext]
 Queries value:
                         HKCR\shcmdfile[nevershowext]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Queries value:
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [enable adapter domain name registration]
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]
```

```
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Oueries value:
Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
                                  HKI M\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Oueries value:
  Queries value:
                                  HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
  Queries value:
                                  HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [maxcached sockets]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicast listen level]
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquick query time outs]
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
                                  HKLM\software\microsoft\wbem\cimom[processid]
  Queries value:
                                  HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
  Queries value:
                                  HKLM\software\microsoft\wbem\cimom[contextlimit]
  Queries value:
  Oueries value:
                                  HKLM\software\microsoft\wbem\cimom[objectlimit]
                                  HKLM\software\microsoft\wbem\cimom[identifierlimit]
  Queries value:
                                  HKCR\interface\{027947e1-d731-11ce-a357-0000000001}\proxystubclsid32[]
  Oueries value:
  Oueries value:
                                  HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
  Queries value:
                                  HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[appid]
  Queries value:
  Queries value:
                                  HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
                                  HKCR \ interface \ \{1c1c45ee-4395-11d2-b60b-00104b703efd\} \ proxystubclsid32[]
  Queries value:
                                  HKCR \land (423ec01e-2e35-11d2-b604-00104b703efd) \land (23ec01e-2e35-11d2-b604-00104b703efd) \land (23ec01e-2e36-11d2-b604-00104b703efd) \land (23ec01e-2e36-11d2-b604-00104b703eff) \land (23ec01e-2e36-11d2-b604-00104b703eff) \land (23ec01e-2e36-11d2-b604-00104b704-00104b704-00104b704-00104b704-00104b704-00
  Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 [serial\_access\_num]
```

Oueries value:

Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ [num\_catalog\_entries]$ 

Oueries value:

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

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

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

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

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

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_catal$ 

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

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]

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

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

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

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

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

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

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

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

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

Queries value:

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

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

folders[common appdata]

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: KLM\svstem\cı

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

Queries value.

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

Queries value:

Queries value:

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:

c7d49d7cecdc}[leaseterminatestime]

Queries value:

c7d49d7cecdc}[dhcpserver]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d40d7cocdc}\ruservadantcename\

c7d49d7cecdc}[queryadaptername]

```
Oueries value:
c7d49d7cecdc}[disableadapterdomainname]
c7d49d7cecdc}[registrationenabled]
    Oueries value:
\label{thm:local_equation} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$$ \end{tabular} $$ \end{tabular} $$$ \end{tabular} $$ \end{tabular} $$$ \end{tabular} $$$ \end{tabular} $
c7d49d7cecdc}[registeradaptername]
    Oueries value:
c7d49d7cecdc}[registrationmaxaddresscount]
    Oueries value:
\label{thm:local_equation} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$$ \end{tabular} $$ \end{tabular} $$$ \end{tabular} $$ \end{tabular} $$$ \end{tabular} $$$ \end{tabular} $
c7d49d7cecdc}[maxnumberofaddressestoregister]
c7d49d7cecdc}[domain]
    Queries value:
c7d49d7cecdc}[dhcpdomain]
    Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[ipautoconfigurationenabled]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[addresstype]
    Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[nameserver]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
    Queries value:
                                                                   HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
                                                                   HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
    Oueries value:
cryptographic provider[type]
                                                                   HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
    Queries value:
cryptographic provider[image path]
                                                                   HKCR\msidxs[]
    Sets/Creates value:
    Sets/Creates value:
                                                                   HKCR\msidxs\clsid[]
    Sets/Creates value:
                                                                   HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}[]
                                                                   HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\progid[]
    Sets/Creates value:
                                                                   HKCR\clsid\{f9ae8980-7e52-11d0-8964-
    Sets/Creates value:
00c04fd611d7}\versionindependentprogid[]
                                                                   HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\inprocserver32[]
    Sets/Creates value:
    Sets/Creates value:
                                                                   HKCR\clsid\{f9ae8980-7e52-11d0-8964-
00c04fd611d7}\inprocserver32[threadingmodel]
                                                                  HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\ole db provider[]
    Sets/Creates value:
    Sets/Creates value:
                                                                   HKCR\msidxs errorlookup[]
    Sets/Creates value:
                                                                   HKCR\msidxs errorlookup\clsid[]
                                                                   HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}[]
    Sets/Creates value:
                                                                   HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\progid[]
    Sets/Creates value:
    Sets/Creates value:
                                                                   HKCR\clsid\{f9ae8981-7e52-11d0-8964-
00c04fd611d7}\versionindependentprogid[]
                                                                   HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\inprocserver32[]
    Sets/Creates value:
    Sets/Creates value:
                                                                   HKCR\clsid\{f9ae8981-7e52-11d0-8964-
00c04fd611d7}\inprocserver32[threadingmodel]
                                                                   HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\extendederrors[]
    Sets/Creates value:
    Sets/Creates value:
                                                                   HKCR\clsid\{f9ae8980-7e52-11d0-8964-
00c04fd611d7\} \\ \text{(f9ae8981-7e52-11d0-8964-00c04fd611d7)[]}
                                                                   HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}[]
    Sets/Creates value:
                                                                   HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\progid[]
    Sets/Creates value:
    Sets/Creates value:
                                                                   HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-
00c04fc2f410}\versionindependentprogid[]
    Sets/Creates value:
                                                                   HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\inprocserver32[]
    Sets/Creates value:
                                                                   HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-
00c04fc2f410}\inprocserver32[threadingmodel]
                                                                   HKCR\clsid\{0cd7a5c0-9f37-11ce-ae65-08002b2e1262}\persistenthandler[]
    Sets/Creates value:
    Sets/Creates value:
                                                                   HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\persistenthandler[]
    Sets/Creates value:
                                                                   HKCR\.xbm\persistenthandler[]
    Sets/Creates value:
                                                                   HKCR\clsid\{e88dcce0-b7b3-11d1-a9f0-00aa0060fa31}\persistenthandler[]
    Sets/Creates value:
                                                                   HKCR\clsid\{48123bc4-99d9-11d1-a6b3-00c04fd91555}\persistenthandler[]
    Sets/Creates value:
                                                                   \label{local-equation} HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\persistenthandler[]
    Sets/Creates value:
                                                                   HKCR\.xml\persistenthandler[]
    Sets/Creates value:
                                                                   HKCR\.xsl\persistenthandler[]
                                                                   HKCR\clsid\{3050f4d8-98b5-11cf-bb82-00aa00bdce0b}\persistenthandler[]
    Sets/Creates value:
    Sets/Creates value:
                                                                   HKCR\.hta\persistenthandler[]
                                                                   HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}[]
    Sets/Creates value:
    Sets/Creates value:
                                                                   HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\progid[]
                                                                   HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-
    Sets/Creates value:
```

00c04fc2db8d}\versionindependentprogid[]

```
Sets/Creates value:
                         HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32[]
                         HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-
 Sets/Creates value:
00c04fc2db8d}\inprocserver32[threadingmodel]
                         HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}[]
 Sets/Creates value:
 Sets/Creates value:
                         HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\progid[]
 Sets/Creates value:
                         HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-
00c04fc2db8d}\versionindependentprogid[]
                         HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32[]
 Sets/Creates value:
 Sets/Creates value:
                         HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-
00c04fc2db8d}\inprocserver32[threadingmodel]
                         HKCR\clsid\{\(\bar{3}\)bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}[]
 Sets/Creates value:
 Sets/Creates value:
                         Sets/Creates value:
                         HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-
00c04fc2db8d}\versionindependentprogid[]
 Sets/Creates value:
                         HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32[]
 Sets/Creates value:
                         HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-
00c04fc2db8d}\inprocserver32fthreadingmodel1
 Sets/Creates value:
                         HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}[]
 Sets/Creates value:
                         HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\progid[]
                         HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-
 Sets/Creates value:
0090272fa362}\versionindependentprogid[]
 Sets/Creates value:
                         HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserver32[]
                         HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-
 Sets/Creates value:
0090272fa362}\inprocserver32[threadingmodel]
 Sets/Creates value:
                         HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}[]
                         HKCR\clsid \ \{363f1015-fd5f-4ba8-ac58-29634f378a42\} \ \ []
 Sets/Creates value:
 Sets/Creates value:
                         HKCR\clsid\{363f1015-fd5f-4ba8-ac58-
29634f378a42}\versionindependentprogid[]
                         HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}\inprocserver32[]
 Sets/Creates value:
 Sets/Creates value:
                         HKCR\clsid\{363f1015-fd5f-4ba8-ac58-
29634f378a42}\inprocserver32[threadingmodel]
                        HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}[]
 Sets/Creates value:
 Sets/Creates value:
                         HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\progid[]
 Sets/Creates value:
                         HKCR\clsid\{f14e6b48-fbca-4d32-bd79-
7829d4f7e43b}\versionindependentprogid[]
                         HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\nprocserver32[]
 Sets/Creates value:
                         HKCR\clsid\{f14e6b48-fbca-4d32-bd79-
 Sets/Creates value:
7829d4f7e43b}\inprocserver32[threadingmodel]
                         HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}[]
 Sets/Creates value:
                         HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\progid[]
 Sets/Creates value:
 Sets/Creates value:
                         HKCR\clsid\{91870674-de84-4313-b07d-
a387415bb4f5}\versionindependentprogid[]
                         HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\inprocserver32[]
 Sets/Creates value:
                         HKCR\clsid\{91870674-de84-4313-b07d-
 Sets/Creates value:
a387415bb4f5}\inprocserver32[threadingmodel]
                         HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}[]
 Sets/Creates value:
 Sets/Creates value:
                         HKCR \clsid \ \{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf\} \progid[]
 Sets/Creates value:
                         HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-
c4825abbe5cf}\versionindependentprogid[]
                         HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\inprocserver32[]
 Sets/Creates value:
                         HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-
 Sets/Creates value:
c4825abbe5cf}\inprocserver32[threadingmodel]
 Sets/Creates value:
                        HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached[{e4b29f9d-d390-480b-92fd-7ddb47101d71} {0000010b-0000-0000-c000-000000000046}
0x4011
 Sets/Creates value:
                         HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe} {0000010b-0000-0000-c000-000000000046}
0x4011
 Sets/Creates value:
                         HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached[{875cb1a1-0f29-45de-a1ae-cfb4950d0b78} {0000010b-0000-0000-c000-000000000046}
0x4011
                         HKU\.default\software\microsoft\windows\currentversion\shell
 Sets/Creates value:
extensions\cached[{fbf23b40-e3f0-101b-8488-00aa003e56f8} {0000010b-0000-0000-c000-000000000046}
0x4011
 Value changes:
                         Value changes:
                         HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}[]
                         Value changes:
                         HKCR\clsid\{aa205a4d-681f-11d0-a243-
 Value changes:
08002b36fca4}\inprocserver32[threadingmodel]
                         HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}[]
 Value changes:
 Value changes:
                         HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprocserver32[]
                         HKCR\clsid\{2a488070-6fd9-11d0-a808-
 Value changes:
00a0c906241a}\inprocserver32[threadingmodel]
 Value changes:
                         HKCR\clsid\{098f2470-bae0-11cd-b579-08002b30bfeb}[]
 Value changes:
                         HKCR\clsid\{098f2470-bae0-11cd-b579-
08002b30bfeb\} \persistent add in sregistered \verb|\{89bcb740-6119-101a-bcb7-00dd010655af\}|[]
 Value changes:
                         HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}[]
                         HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprocserver32[]
 Value changes:
                         HKCR\clsid\{c3278e90-bea7-11cd-b579-
 Value changes:
08002b30bfeb}\inprocserver32[threadingmodel]
 Value changes:
                         \label{local-bound} \mbox{HKCR\clsid\{00022602-0000-0000-c000-000000000046}\persistenthandler[]}
                         HKCR\clsid\{d3e34b21-9d75-101a-8c3d-00aa001a1652}\persistenthandler[]
 Value changes:
 Value changes:
                         HKCR \clsid \end{25336920-03f9-11cf-8fd0-00aa00686f13} \persistenthandler[]
```

```
Value changes:
                                                                                               HKCR\clsid\{00020c01-0000-0000-c000-00000000046}\persistenthandler[]
      Value changes:
                                                                                               HKCR \clsid \ \{5e941d80-bf96-11cd-b579-08002b30bfeb\}[]
      Value changes:
                                                                                               HKCR\clsid\{5e941d80-bf96-11cd-b579-
      Value changes:
08002b30bfeb\} \persistent add in sregistered \verb|\{89bcb740-6119-101a-bcb7-00dd010655af\}|[]
      Value changes:
                                                                                              HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}[]
                                                                                               HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprocserver32[]
      Value changes:
                                                                                              HKCR\clsid\{c1243ca0-bf96-11cd-b579-
      Value changes:
08002b30bfeb}\inprocserver32[threadingmodel]
                                                                                              HKCR\clsid\{73fddc80-aea9-101a-98a7-00aa00374959}\persistenthandler[]
      Value changes:
      Value changes:
                                                                                              Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\neutral[locale]
      Value changes:
                                                                                             HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}[]
      Value changes:
                                                                                              HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprocserver32[]
                                                                                              HKCR\clsid\{369647e0-17b0-11ce-9950-
      Value changes:
00aa004bbb1f}\inprocserver32[threadingmodel]
      Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\neutral[wbreakerclass]
                                                                                              HKCR\clsid\{78fe669a-186e-4108-96e9-77b586c1332f}[]
      Value changes:
      Value changes:
                                                                                               HKCR\clsid\{78fe669a-186e-4108-96e9-77b586c1332f}\inprocserver32[]
      Value changes:
                                                                                              HKCR\clsid\{78fe669a-186e-4108-96e9-
77b586c1332f}\inprocserver32[threadingmodel]
      Value changes:
                                                                                              HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}[]
      Value changes:
                                                                                              HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\nprocserver32[]
                                                                                             HKCR\clsid\{1e9685e6-db6d-11d0-bb63-
     Value changes:
00c04fc2f410}\inprocserver32[threadingmodel]
      Value changes:
                                                                                              HKCR\clsid\{1f247dc0-902e-11d0-a80c-00a0c906241a}[]
                                                                                             HKCR\clsid\{1f247dc0-902e-11d0-a80c-00a0c906241a}\inprocserver32[]
      Value changes:
      Value changes:
                                                                                              HKCR\clsid\{1f247dc0-902e-11d0-a80c-
00a0c906241a}\inprocserver32[threadingmodel]
                                                                                             HKCR\clsid\{c04efa90-e221-11d2-985e-00c04f575153}\inprocserver32[]
      Value changes:
      Value changes:
                                                                                              HKCR\clsid\{c04efa90-e221-11d2-985e-
00c04f575153}\inprocserver32[threadingmodel]
                                                                                              HKCR\clsid\{c04efa90-e221-11d2-985e-00c04f575153}[]
      Value changes:
      Value changes:
                                                                                               HKCR\interface\{f4eb8260-8dda-11d1-b3aa-00a0c9063796}\proxystubclsid32[]
      Value changes:
                                                                                               HKCR\interface\{f4eb8260-8dda-11d1-b3aa-00a0c9063796}[]
                                                                                               HKCR \setminus \{f4eb8260-8dda-11d1-b3aa-00a0c9063796\} \setminus \{f4eb8260-6da-11d1-b3aa-00a0c9063796\} \setminus \{f4eb8260-6da-11d1-b3aa-00a0c9063796\} \setminus \{f4eb8260-6da-11d1-b3aa-00a0c9063796\} \setminus \{f4eb8260-6da-11d1-b3aa-00a0c9063796\} \setminus \{f4eb8260-6da-11d1-b3aa-00a0c9063796\} \setminus \{f4eb8260-6da-11d1-b3aa-00a0c9064
      Value changes:
      Value changes:
                                                                                               HKCR\clsid\{95ad72f0-44ce-11d0-ae29-00aa004b9986}[]
      Value changes:
                                                                                               HKCR\clsid\{95ad72f0-44ce-11d0-ae29-00aa004b9986}\inprocserver32[]
      Value changes:
                                                                                              HKCR\clsid\{95ad72f0-44ce-11d0-ae29-
00aa004b9986}\inprocserver32[threadingmodel]
      Value changes:
                                                                                              HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-
00aa004b9986}[namestring]
                                                                                               HKLM \setminus software \setminus microsoft \setminus mmc \setminus snapins \setminus \{95ad72f0-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d
      Value changes:
00aa004b9986}[about]
      Value changes:
                                                                                               HKLM \ software \ microsoft \ mmc \ snapins \ \{95ad72f0-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46c-11d0-ae29-46
00aa004b9986}[nodetype]
      Value changes:
                                                                                               HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-
00aa004b9986}[provider]
                                                                                               HKLM \setminus software \setminus microsoft \setminus mmc \setminus snapins \setminus \{95ad72f0-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-44ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d0-ae29-46ce-11d
      Value changes:
00aa004b9986}[version]
      Value changes:
                                                                                               HKLM \setminus software \setminus microsoft \setminus mmc \setminus nodetypes \setminus \{5401e3e9-f5f6-11d1-b4f7-mg\} \setminus \{5401e3e9-f5f6-11d1-b4f6-mg\} \setminus \{5401e3e9-f5f6-mg\} \setminus \{
00c04fc2db8d}[]
                                                                                               HKLM\software\microsoft\mmc\nodetvpes\{476e6449-aaff-11d0-b944-
      Value changes:
00c04fd8d5b0}\extensions\namespace[{95ad72f0-44ce-11d0-ae29-00aa004b9986}]
                                                                                              HKLM \setminus software \setminus microsoft \setminus mmc \setminus nodetypes \setminus \{476e6449 - aaff-11d0 - b944 - aaff-11d
      Value changes:
00c04fd8d5b0}\dynamic extensions[{95ad72f0-44ce-11d0-ae29-00aa004b9986}]
      Value changes:
                                                                                              HKLM\system\currentcontrolset\control\server applications[{95ad72f0-
44ce-11d0-ae29-00aa004b9986}]
      Value changes:
                                                                                              HKCR\ixsso.guery[]
      Value changes:
                                                                                              HKCR\ixsso.query\clsid[]
      Value changes:
                                                                                               HKCR\ixsso.query\curver[]
      Value changes:
                                                                                               HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}[]
      Value changes:
                                                                                              HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}\inprocserver32[]
      Value changes:
                                                                                               HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-
1e486b2fef9d}\inprocserver32[threadingmodel]
                                                                                              \label{lem:hkcrclsid} $$HKCR\clsid{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d} \rightarrow []
      Value changes:
      Value changes:
                                                                                               HKCR\ixsso.query.3[]
                                                                                               HKCR\ixsso.query.3\clsid[]
      Value changes:
      Value changes:
                                                                                               HKCR\ixsso.query.2[]
      Value changes:
                                                                                               HKCR\ixsso.query.2\clsid[]
      Value changes:
                                                                                               HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}[]
                                                                                              HKCR\clsid\a4463024-2b6f-11d0-bfbc-0020f8008024\\\inprocserver32[]
      Value changes:
      Value changes:
                                                                                               HKCR\clsid\{a4463024-2b6f-11d0-bfbc-
0020f8008024}\inprocserver32[threadingmodel]
                                                                                              HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\progid[]
      Value changes:
                                                                                               HKCR\ixsso.util[]
      Value changes:
      Value changes:
                                                                                               HKCR\ixsso.util\clsid[]
      Value changes:
                                                                                               HKCR\ixsso.util\curver[]
      Value changes:
                                                                                               HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}[]
                                                                                               \label{localization} HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\nprocserver32[]
      Value changes:
      Value changes:
                                                                                              HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-
```

```
0020f8008024}\inprocserver32[threadingmodel]
                                   HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\progid[]
  Value changes:
  Value changes:
                                    HKCR\ixsso.util.2[]
  Value changes:
                                    HKCR\ixsso.util.2\clsid[]
  Value changes:
                                    HKCR\clsid\{eec97550-47a9-11cf-b952-00aa0051fe20}[]
  Value changes:
                                    HKCR\clsid\{eec97550-47a9-11cf-b952-
00aa0051fe20}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
  Value changes:
                                   HKCR\clsid\{e0ca5340-4534-11cf-b952-00aa0051fe20}[]
                                    HKCR\clsid\{e0ca5340-4534-11cf-b952-00aa0051fe20}\inprocserver32[]
  Value changes:
  Value changes:
                                    HKCR\clsid\{e0ca5340-4534-11cf-b952-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
                                    HKCR\.odc\persistenthandler[]
  Value changes:
                                    HKCR\.hhc\persistenthandler[]
  Value changes:
                                    HKCR\.htm\persistenthandler[]
  Value changes:
                                    HKCR\.html\persistenthandler[]
  Value changes:
                                    HKCR\.htx\persistenthandler[]
  Value changes:
                                    HKCR\.stm\persistenthandler[]
  Value changes:
                                    HKCR\.htw\persistenthandler[]
  Value changes:
                                    HKCR\.asp\persistenthandler[]
  Value changes:
                                    HKCR\.aspx\persistenthandler[]
  Value changes:
                                    HKCR\.ascx\persistenthandler[]
  Value changes:
                                    HKCR\.css\persistenthandler[]
  Value changes:
                                    HKCR\clsid\{3050f4d8-98b5-11cf-bb82-00aa00bdce0b}\persistenthandler[]
  Value changes:
                                    HKCR\.htt\persistenthandler[]
  Value changes:
                                    HKCR\clsid\{98de59a0-d175-11cd-a7bd-00006b827d94}[]
                                    HKCR\clsid\{98de59a0-d175-11cd-a7bd-
  Value changes:
00006b827d94\\ \texttt{persistentaddinsregistered} \{89bcb740-6119-101a-bcb7-00dd010655af\}[]
  Value changes:
                                    HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}[]
                                    HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprocserver32[]
  Value changes:
  Value changes:
                                    HKCR\clsid\{f07f3920-7b8c-11cf-9be8-
00aa004b9986}\inprocserver32[threadingmodel]
                                   HKCR\clsid\{00020906-0000-0000-c000-00000000046}\persistenthandler[]
  Value changes:
  Value changes:
                                    HKCR\clsid\{64818d11-4f9b-11cf-86ea-00aa00b929e8}\persistenthandler[]
  Value changes:
                                    HKCR\clsid\{64818d10-4f9b-11cf-86ea-00aa00b929e8}\persistenthandler[]
                                    Value changes:
  Value changes:
                                    HKCR\clsid\{00020821-0000-0000-c000-00000000046}\persistenthandler[]
  Value changes:
                                    HKCR\clsid\{00020900-0000-0000-c000-00000000046}\persistenthandler[]
  Value changes:
                                    HKCR\clsid\{ea7bae70-fb3b-11cd-a903-00aa00510ea3}\persistenthandler[]
  Value changes:
                                    HKCR\clsid\\ea7bae71-fb3b-11cd-a903-00aa00510ea3\\persistenthandler[]
  Value changes:
                                    HKCR\clsid\{00020811-0000-0000-c000-00000000046}\persistenthandler[]
  Value changes:
                                    \label{local_equation} \mbox{HKCR\clsid\{00020810-0000-0000-c000-000000000046\}\persistenthandler[]}} \mbox{ } \mbox{ }
  Value changes:
                                    HKCR\.doc\persistenthandler[]
  Value changes:
                                    HKCR\.dot\persistenthandler[]
  Value changes:
                                    HKCR\.pot\persistenthandler[]
  Value changes:
                                    HKCR\.ppt\persistenthandler[]
  Value changes:
                                    HKCR\.pps\persistenthandler[]
  Value changes:
                                    HKCR\.xlb\persistenthandler[]
  Value changes:
                                    HKCR\.xlc\persistenthandler[]
  Value changes:
                                    HKCR\.xls\persistenthandler[]
  Value changes:
                                    HKCR\.xlt\persistenthandler[]
  Value changes:
                                    HKCR\microsoft.isadm.1[]
  Value changes:
                                    HKCR\microsoft.isadm.1\clsid[]
  Value changes:
                                    HKCR\microsoft.isadm[]
  Value changes:
                                    HKCR\microsoft.isadm\curver[]
  Value changes:
                                    HKCR\microsoft.isadm\clsid[]
  Value changes:
                                    HKCR\microsoft.iscatadm.1[]
  Value changes:
                                    HKCR\microsoft.iscatadm.1\clsid[]
  Value changes:
                                    HKCR\microsoft.iscatadm[]
  Value changes:
                                    HKCR\microsoft.iscatadm\curver[]
  Value changes:
                                    HKCR\microsoft.iscatadm\clsid[]
  Value changes:
                                    HKCR\microsoft.isscopeadm.1[]
  Value changes:
                                    HKCR\microsoft.isscopeadm.1\clsid[]
  Value changes:
                                    HKCR\microsoft.isscopeadm[]
  Value changes:
                                    HKCR\microsoft.isscopeadm\curver[]
  Value changes:
                                    HKCR\microsoft.isscopeadm\clsid[]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\english_us[locale]
                                    HKCR\clsid\{eeed4c20-7f1b-11ce-be57-00aa0051fe20}[]
  Value changes:
  Value changes:
                                    \label{local-condition} HKCR\clsid\\ \{eeed4c20-7f1b-11ce-be57-00aa0051fe20\\ \}\ inprocserver32[]
  Value changes:
                                    HKCR\clsid\{eeed4c20-7f1b-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\english_us[stemmerclass]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\english_uk[locale]
                                    HKCR\clsid\{d99f7670-7f1a-11ce-be57-00aa0051fe20}[]
  Value changes:
  Value changes:
                                    HKCR\clsid\{d99f7670-7f1a-11ce-be57-00aa0051fe20}\inprocserver32[]
                                    HKCR\clsid\{d99f7670-7f1a-11ce-be57-
  Value changes:
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
Value changes:
```

```
HKCR\clsid\{59e09848-8099-101b-8df3-00000b65c3b5}[]
  Value changes:
  Value changes:
                                HKCR\clsid\{59e09848-8099-101b-8df3-00000b65c3b5}\inprocserver32[]
  Value changes:
                                HKCR\clsid\{59e09848-8099-101b-8df3-
00000b65c3b5}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\french_french[wbreakerclass]
                                HKCR\clsid\{2a6eb050-7f1c-11ce-be57-00aa0051fe20}[]
  Value changes:
                                HKCR\clsid\{2a6eb050-7f1c-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes:
                                HKCR\clsid\{2a6eb050-7f1c-11ce-be57-
  Value changes:
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\german_german[locale]
  Value changes:
                                HKCR\clsid\{9b08e210-e51b-11cd-bc7f-00aa003db18e}[]
                                HKCR\clsid\{9b08e210-e51b-11cd-bc7f-00aa003db18e}\inprocserver32[]
  Value changes:
  Value changes:
                                HKCR\clsid\{9b08e210-e51b-11cd-bc7f-
00aa003db18e}\inprocserver32[threadingmodel]
  Value changes:
\label{thm:local} \begin{tabular}{ll} HKLM\system\currentcontrolset\control\contentindex\language\german\_german[wbreakerclass]]{ } \end{tabular}
  Value changes:
                                HKCR\clsid\{510a4910-7f1c-11ce-be57-00aa0051fe20}[]
                                HKCR\clsid\{510a4910-7f1c-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes:
  Value changes:
                                HKCR\clsid\{510a4910-7f1c-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\italian_italian[locale]
                                HKCR\clsid\{fd86b5d0-12c6-11ce-bd31-00aa004bbb1f}[]
  Value changes:
  Value changes:
                                HKCR\clsid\{fd86b5d0-12c6-11ce-bd31-00aa004bbb1f}\inprocserver32[]
  Value changes:
                                HKCR\clsid\{fd86b5d0-12c6-11ce-bd31-
00aa004bbb1f}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\italian_italian[wbreakerclass]
                                HKCR\clsid\{6d36ce10-7f1c-11ce-be57-00aa0051fe20}[]
  Value changes:
  Value changes:
                                HKCR\clsid\{6d36ce10-7f1c-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes:
                                HKCR\clsid\{6d36ce10-7f1c-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\swedish_default[locale]
  Value changes:
                                HKCR\clsid\{01c6b350-12c7-11ce-bd31-00aa004bbb1f}[]
                                HKCR\clsid\{01c6b350-12c7-11ce-bd31-00aa004bbb1f}\inprocserver32[]
  Value changes:
  Value changes:
                                HKCR\clsid\{01c6b350-12c7-11ce-bd31-
00aa004bbb1f}\inprocserver32[threadingmodel]
  Value changes:
HKCR\clsid\{9478f640-7f1c-11ce-be57-00aa0051fe20}[]
  Value changes:
                                HKCR\clsid\{9478f640-7f1c-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes:
  Value changes:
                                HKCR\clsid\{9478f640-7f1c-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\spanish_modern[locale]
  Value changes:
                                HKCR\clsid\{0285b5c0-12c7-11ce-bd31-00aa004bbb1f}[]
  Value changes:
                                HKCR\clsid\{0285b5c0-12c7-11ce-bd31-00aa004bbb1f}\inprocserver32[]
  Value changes:
                                HKCR\clsid\{0285b5c0-12c7-11ce-bd31-
00aa004bbb1f}\inprocserver32[threadingmodel]
  Value changes:
Value changes:
                                HKCR\clsid\{b0516ff0-7f1c-11ce-be57-00aa0051fe20}[]
  Value changes:
                                HKCR\clsid\{b0516ff0-7f1c-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes:
                                HKCR\clsid\{b0516ff0-7f1c-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\dutch_dutch[locale]
                                HKCR\clsid\{66b37110-8bf2-11ce-be59-00aa0051fe20}[]
  Value changes:
  Value changes:
                                HKCR\clsid\{66b37110-8bf2-11ce-be59-00aa0051fe20}\inprocserver32[]
  Value changes:
                                HKCR\clsid\{66b37110-8bf2-11ce-be59-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
HKCR\clsid\{860d28d0-8bf4-11ce-be59-00aa0051fe20}[]
  Value changes:
  Value changes:
                                \label{lem:hkcr} $$ HKCR\clsid_{860d28d0-8bf4-11ce-be59-00aa0051fe20} \in \clsid_{860d28d0-8bf4-11ce-be59-00aa0051fe20} $$ inprocessor of the context of the
  Value changes:
                                HKCR\clsid\{860d28d0-8bf4-11ce-be59-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
Value changes:
                                HKCR\.nws[]
```

```
Value changes:
                          HKCR\microsoft internet news message[]
                          HKCR\microsoft internet news message\clsid[]
 Value changes:
                          HKCR\clsid\{5645c8c0-e277-11cf-8fda-00aa00a14f93}[]
 Value changes:
 Value changes:
                          HKCR\clsid\{5645c8c0-e277-11cf-8fda-00aa00a14f93}\persistenthandler[]
 Value changes:
                          HKCR\clsid\{5645c8c1-e277-11cf-8fda-
00aa00a14f93}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
                          HKCR\clsid\{5645c8c2-e277-11cf-8fda-00aa00a14f93}\inprocserver32[]
 Value changes:
 Value changes:
                          HKCR\clsid\{5645c8c2-e277-11cf-8fda-
00aa00a14f93}\inprocserver32[threadingmodel]
                          HKCR\.eml[]
 Value changes:
 Value changes:
                          HKCR\microsoft internet mail message[]
 Value changes:
                          HKCR\microsoft internet mail message\clsid[]
 Value changes:
                          HKCR\clsid\{5645c8c3-e277-11cf-8fda-00aa00a14f93}[]
                          \label{local-equation} $$HKCR\clsid_{5645c8c3-e277-11cf-8fda-00aa00a14f93}\operatorname{persistenthandler[]} $$
 Value changes:
                          HKCR\clsid\{5645c8c4-e277-11cf-8fda-
 Value changes:
00aa00a14f93}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
 Value changes:
                          HKCR\enguswrdbrk.enguswrdbrk.1[]
 Value changes:
                          HKCR\enguswrdbrk.enguswrdbrk.1\clsid[]
 Value changes:
                          HKCR\enguswrdbrk.enguswrdbrk[]
                          HKCR\enguswrdbrk.enguswrdbrk\curver[]
 Value changes:
 Value changes:
                          HKCR\engukwrdbrk.1[]
                          HKCR\engukwrdbrk.engukwrdbrk.1\clsid[]
 Value changes:
                          HKCR\engukwrdbrk.engukwrdbrk[]
 Value changes:
 Value changes:
                          HKCR\engukwrdbrk.engukwrdbrk\curver[]
 Value changes:
                          HKCR\frnfrnwrdbrk.frnfrnwrdbrk.1[]
                          HKCR\frnfrnwrdbrk.frnfrnwrdbrk.1\clsid[]
 Value changes:
 Value changes:
                          HKCR\frnfrnwrdbrk.frnfrnwrdbrk[]
 Value changes:
                          HKCR\frnfrnwrdbrk.frnfrnwrdbrk\curver[]
                          HKCR\itlitlwrdbrk.itlitlwrdbrk.1[]
 Value changes:
 Value changes:
                          HKCR\itlitlwrdbrk.itlitlwrdbrk.1\clsid[]
 Value changes:
                          HKCR\itlitlwrdbrk.itlitlwrdbrk[]
 Value changes:
                          HKCR\itlitlwrdbrk.itlitlwrdbrk\curver[]
 Value changes:
                          HKCR\spnmdrwrdbrk.spnmdrwrdbrk.1[]
 Value changes:
                          HKCR\spnmdrwrdbrk.spnmdrwrdbrk.1\clsid[]
                          HKCR\spnmdrwrdbrk.spnmdrwrdbrk[]
 Value changes:
 Value changes:
                          HKCR\spnmdrwrdbrk.spnmdrwrdbrk\curver[]
```

Value changes:

 $HKU\.default\software\microsoft\windows\currentversion\explorer\mountpoints2\clbaseclass]$ 

Value changes: HKU\.default\software\microsoft\windows\currentversion\explorer\shell folders[personal]

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

folders[common documents]

Value changes: HKU\.default\software\microsoft\windows\currentversion\explorer\shell

folders[desktop] Value changes:

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

folders[common desktop]

 $\label{thm:local_ham} \begin{tabular}{ll} HKU\label{thm:local_ham} HKU\label{thm:local_ham} \end{tabular} $$ is the limit of the local ham also a substitution of the local ham also a substitutio$ Value changes:

extensions\cached[{fbf23b40-e3f0-101b-8488-00aa003e56f8} {0000010b-0000-0000-c000-000000000046}

0x401]

HKU\.default\software\microsoft\windows\currentversion\shell Value changes:

extensions\cached[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe} {0000010b-0000-0000-c000-000000000046}

0x4011

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

folders[common appdata]