# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 1167, Task ID: 4096

Task ID: 4096 Risk Level:

2016-07-04 04:18:06 (UTC) Date Processed:

63.29 seconds Processing Time: Virtual Environment: IntelliVM

"c:\windows\temp\RajivApp1.exe" **Execution Arguments:** 

1167 Sample ID: Type: basic Owner: admin Label: RajivApp1.exe

2016-07-04 04:18:06 (UTC) Date Added: PE32:win32:gui:.net File Type: File Size: 8704 bytes

MD5: 9bde8983ac767c24755443627cda99bc

SHA256: ca0dcf72ce74fa1084255dae79a6a787eccf04152cfadd23f775a1671f1149cf

Description:

## Pattern Matching Results

4 Reads process memory

2 Resolves local hostname

NET compiled executable

3 Long sleep detected

5 Query DNS from command line

4 Terminates process under Windows subfolder

## Process/Thread Events

C:\windows\temp\RajivApp1.exe ["C:\windows\temp\RajivApp1.exe" ]
C:\Windows\system32\cmd.exe ["cmd.exe"] Creates process:

Creates process:

Creates process: C:\Windows\system32\nslookup.exe [nslookup WORKGROUP] Creates process: C:\Windows\system32\nslookup.exe [nslookup \_\_MSBROWSE\_

Reads from process: PID:2588 C:\Windows\System32\nslookup.exe PID:2628 C:\Windows\System32\nslookup.exe Reads from process:

Terminates process: C:\Windows\System32\nslookup.exe Terminates process: C:\Windows\System32\cmd.exe

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1

\BaseNamedObjects\CorDBIPCSetupSyncEvent\_2484 Creates event:

Creates event: \KernelObjects\LowMemoryCondition

Creates event: \BaseNamedObjects\ConsoleEvent-0x00000A10 Creates event: \BaseNamedObjects\ConsoleEvent-0x00000A38

Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1 Creates semaphore: \Sessions\1\BaseNamedObjects\GdiplusFontCacheFileV1

## File System Events

Creates: C:\Users\Admin

C:\Users\Admin\AppData\Roaming Creates:

Creates: C:\Users\Admin\AppData\Local\GDIPFONTCACHEV1.DAT Opens: C:\Windows\Prefetch\RAJIVAPP1.EXE-4C2BBC3A.pf

Opens: C:\Windows\System32

C:\Windows\System32\mscoree.dll Opens: Opens: C:\windows\temp\VERSION.dll Opens: C:\Windows\System32\version.dll Opens: C:\Windows\System32\sechost.dll C:\Windows\SYSTEM32\MSCOREE.DLL.local Opens:

C:\Windows\Microsoft.NET\Framework\v2.0.50727 Opens: Opens: C:\Windows\Microsoft.NET\Framework\Upgrades.2.0.50727\

Opens: C:\Windows\System32\imm32.dll Opens: C:\windows\temp\RajivApp1.exe.config

C:\Windows\Temp\RajivApp1.exe Opens:  $\label{lem:c:windowsMicrosoft.NET\Framework\v2.0.50727\mbox{\corwks.dll}$ Opens:

C:\windows\temp\RajivApp1.exe.Local\ Opens:

Opens: C:\Windows\winsxs\x86\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.4940\_none\_d08cc06a442b34fc

C:\Windows\winsxs\x86\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.4940\_none\_d08cc06a442b34fc\msvcr80.dll

C:\ Opens:

Opens: C:\Windows

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config Opens: Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.localgac Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch Opens:

Opens:

C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config

C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch

```
C:\Windows\Globalization\Sorting\SortDefault.nls
      Opens:
     Opens:
                                                                                 C:\windows\temp\profapi.dll
      Opens:
                                                                                C:\Windows\System32\profapi.dll
     Opens:
                                                                                C:\Users\Admin
     Opens:
                                                                                C:\Users\Admin\AppData\Roaming
     Opens:
                                                                                C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\security.config
                                                                                C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\security.config.cch
                                                                                C:\Windows\assembly\NativeImages_v2.0.50727_32\index145.dat
     Opens:
     Opens:
C: \verb|\windows| assembly \verb|\NativeImages_v2.0.50727_32 \verb|\windows| assembly \verb|\NativeImages_v2.0.50727_32 \verb|\windows| assembly \verb|\NativeImages_v2.0.50727_32 \verb|\windows| assembly \verb|\NativeImages_v2.0.50727_32 \verb|\windows| assembly a
                                                                                 C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0_b77a5c561934e089
      Opens:
     Opens:
                                                                                C:\Windows\Temp
     Opens:
                                                                                C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
     Opens:
                                                                                C:\Windows\System32\rpcss.dll
                                                                                C:\windows\temp\CRYPTBASE.dll
     Opens:
     Opens:
                                                                                C:\Windows\System32\cryptbase.dll
     Opens:
                                                                                 C:\Windows\System32\uxtheme.dll
     Opens:
                                                                                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
                                                                                C:\windows\temp\RajivApp1.config
     Opens:
     Opens:
                                                                                C:\Windows\System32\l_intl.nls
     Opens:
                                                                                C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
     Opens:
                                                                                 C:\Windows\assembly\pubpol4.dat
     Opens:
                                                                                 C:\Windows\assembly\GAC\PublisherPolicy.tme
     Opens:
C: \verb|Windows| assembly \verb|NativeImages_v2.0.50727_32 \verb|System| 9e0a 3b9b9f457233a335d7fba8f95419 \verb|System.ni.dll| and the standard of the sta
C: \verb|\windows| as sembly \verb|\NativeImages_v2.0.50727_32 \verb|\system.Drawing| dbfe8642a8ed7b2b103ad28e0c96418a \verb|\system.Drawing.ni.dll| and the semble of the
     Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\3afcd5168c7a6cb02eab99d7fd71e102\System.Windows.Forms.ni.dll
      Opens:
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0_b77a5c561934e089
                                                                                 \label{lem:c:windows} C: \windows \assembly \GAC\_MSIL \System \2.0.0.0\_b77a5c561934e089
     Opens:
     Opens:
                                                                                C:\Windows\assembly\GAC_MSIL\System.Drawing\2.0.0.0_b03f5f7f11d50a3a
     Opens:
{\tt C:\Windows\assembly\GAC\_MSIL\System.Windows.Forms\2.0.0.0\_b77a5c561934e089\\ \tt uxtheme.dll\ System.Windows.Forms\2.0.0.0\_b77a5c561934e089\\ \tt uxtheme.dll\ System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.Windows\assembly\GAC\_MSIL\System.
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0_b77a5c561934e089\System.Windows.Forms.dll
                                                                                 C:\Windows\Globalization\en-us.nlp
    Opens:
     Opens:
                                                                                C: \verb|\windows| Microsoft.NET| Framework \verb|\v2.0.50727| Gdiplus.dll| \\
     Opens:
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
     Opens:
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
     Opens:
                                                                                 C:\Users\Admin\AppData\Local\GDIPFONTCACHEV1.DAT
     Opens:
                                                                                C:\Windows\Fonts\marlett.ttf
     Opens:
                                                                                C:\Windows\Fonts\arial.ttf
     Opens:
                                                                                 C:\Windows\Fonts\ariali.ttf
     Opens:
                                                                                C:\Windows\Fonts\arialbd.ttf
     Opens:
                                                                                C:\Windows\Fonts\arialbi.ttf
     Opens:
                                                                                C:\Windows\Fonts\batang.ttc
     Opens:
                                                                                C:\Windows\Fonts\cour.ttf
     Opens:
                                                                                C:\Windows\Fonts\couri.ttf
      Opens:
                                                                                 C:\Windows\Fonts\courbd.ttf
     Opens:
                                                                                C:\Windows\Fonts\courbi.ttf
     Opens:
                                                                                C:\Windows\Fonts\daunpenh.ttf
     Opens:
                                                                                C:\Windows\Fonts\dokchamp.ttf
     Opens:
                                                                                C:\Windows\Fonts\estre.ttf
      Opens:
                                                                                 C:\Windows\Fonts\euphemia.ttf
      Opens:
                                                                                 C:\Windows\Fonts\gautami.ttf
     Opens:
                                                                                C:\Windows\Fonts\gautamib.ttf
     Opens:
                                                                                 C:\Windows\Fonts\Vani.ttf
     Opens:
                                                                                C:\Windows\Fonts\Vanib.ttf
     Opens:
                                                                                C:\Windows\Fonts\gulim.ttc
     Opens:
                                                                                C:\Windows\Fonts\impact.ttf
      Opens:
                                                                                 C:\Windows\Fonts\iskpota.ttf
     Opens:
                                                                                C:\Windows\Fonts\iskpotab.ttf
     Opens:
                                                                                C:\Windows\Fonts\kalinga.ttf
                                                                                C:\Windows\Fonts\kalingab.ttf
     Opens:
     Opens:
                                                                                C:\Windows\Fonts\kartika.ttf
      Opens:
                                                                                 C:\Windows\Fonts\kartikab.ttf
     Opens:
                                                                                 C:\Windows\Fonts\KhmerUI.ttf
                                                                                C:\Windows\Fonts\KhmerUIb.ttf
     Opens:
                                                                                 C:\Windows\Fonts\LaoUI.ttf
     Opens:
                                                                                C:\Windows\Fonts\LaoUIb.ttf
     Opens:
     Opens:
                                                                                C:\Windows\Fonts\latha.ttf
      Opens:
                                                                                 C:\Windows\Fonts\lathab.ttf
     Opens:
                                                                                C:\Windows\Fonts\lucon.ttf
     Opens:
                                                                                C:\Windows\Fonts\malgun.ttf
     Opens:
                                                                                C:\Windows\Fonts\malgunbd.ttf
      Opens:
                                                                                 C:\Windows\Fonts\mangal.ttf
     Opens:
                                                                                C:\Windows\Fonts\mangalb.ttf
      Opens:
                                                                                 C:\Windows\Fonts\meiryo.ttc
      Opens:
                                                                                C:\Windows\Fonts\meiryob.ttc
     Opens:
                                                                                C:\Windows\Fonts\himalava.ttf
      Opens:
                                                                                 C:\Windows\Fonts\msjh.ttf
```

Opens:

C:\Windows\Fonts\msjhbd.ttf

Opens: C:\Windows\Fonts\msyh.ttf Opens: C:\Windows\Fonts\msyhbd.ttf Opens: C:\Windows\Fonts\mingliu.ttc Opens: C:\Windows\Fonts\mingliub.ttc Opens: C:\Windows\Fonts\monbaiti.ttf Opens: C:\Windows\Fonts\msgothic.ttc Opens: C:\Windows\Fonts\msmincho.ttc Opens: C:\Windows\Fonts\mvboli.ttf Opens: C:\Windows\Fonts\ntailu.ttf Opens: C:\Windows\Fonts\ntailub.ttf C:\Windows\Fonts\nyala.ttf Opens: Opens: C:\Windows\Fonts\phagspa.ttf Opens: C:\Windows\Fonts\phagspab.ttf C:\Windows\Fonts\plantc.ttf Opens: Opens: C:\Windows\Fonts\raavi.ttf Opens: C:\Windows\Fonts\raavib.ttf Opens: C:\Windows\Fonts\segoesc.ttf Opens: C:\Windows\Fonts\segoescb.ttf C:\Windows\Fonts\segoeui.ttf Opens: Opens: C:\Windows\Fonts\segoeuib.ttf Opens: C:\Windows\Fonts\segoeuii.ttf C:\Windows\Fonts\segoeuiz.ttf Opens: Opens: C:\Windows\Fonts\seguisb.ttf Opens: C:\Windows\Fonts\segoeuil.ttf C:\Windows\Fonts\seguisym.ttf Opens: Opens: C:\Windows\Fonts\shruti.ttf Opens: C:\Windows\Fonts\shrutib.ttf Opens: C:\Windows\Fonts\simsun.ttc Opens: C:\Windows\Fonts\simsunb.ttf Opens: C:\Windows\Fonts\sylfaen.ttf Opens: C:\Windows\Fonts\taile.ttf Opens: C:\Windows\Fonts\taileb.ttf Opens: C:\Windows\Fonts\times.ttf Opens: C:\Windows\Fonts\timesi.ttf Opens: C:\Windows\Fonts\timesbd.ttf Opens: C:\Windows\Fonts\timesbi.ttf Opens: C:\Windows\Fonts\tunga.ttf Opens: C:\Windows\Fonts\tungab.ttf Opens: C:\Windows\Fonts\vrinda.ttf Opens: C:\Windows\Fonts\vrindab.ttf Opens: C:\Windows\Fonts\Shonar.ttf Opens: C:\Windows\Fonts\Shonarb.ttf Opens: C:\Windows\Fonts\msyi.ttf Opens: C:\Windows\Fonts\tahoma.ttf Opens: C:\Windows\Fonts\tahomabd.ttf Opens: C:\Windows\Fonts\micross.ttf Opens: C:\Windows\Fonts\angsa.ttf Opens: C:\Windows\Fonts\angsai.ttf Opens: C:\Windows\Fonts\angsab.ttf Opens: C:\Windows\Fonts\angsaz.ttf Opens: C:\Windows\Fonts\aparaj.ttf Opens: C:\Windows\Fonts\aparajb.ttf Opens: C:\Windows\Fonts\aparajbi.ttf Opens: C:\Windows\Fonts\aparaji.ttf Opens: C:\Windows\Fonts\cordia.ttf Opens: C:\Windows\Fonts\cordiai.ttf Opens: C:\Windows\Fonts\cordiab.ttf Opens: C:\Windows\Fonts\cordiaz.ttf Opens: C:\Windows\Fonts\ebrima.ttf Opens: C:\Windows\Fonts\ebrimabd.ttf Opens: C:\Windows\Fonts\gisha.ttf Opens: C:\Windows\Fonts\gishabd.ttf Opens: C:\Windows\Fonts\kokila.ttf Opens: C:\Windows\Fonts\kokilab.ttf Opens: C:\Windows\Fonts\kokilabi.ttf Opens: C:\Windows\Fonts\kokilai.ttf C:\Windows\Fonts\leelawad.ttf Opens: Opens: C:\Windows\Fonts\leelawdb.ttf Opens: C:\Windows\Fonts\msuighur.ttf Opens: C:\Windows\Fonts\moolbor.ttf Opens: C:\Windows\Fonts\symbol.ttf Opens: C:\Windows\Fonts\utsaah.ttf Opens: C:\Windows\Fonts\utsaahb.ttf Opens: C:\Windows\Fonts\utsaahbi.ttf C:\Windows\Fonts\utsaahi.ttf Opens: Opens: C:\Windows\Fonts\vijaya.ttf Opens: C:\Windows\Fonts\vijayab.ttf C:\Windows\Fonts\wingding.ttf Opens: Opens: C:\Windows\Fonts\modern.fon Opens: C:\Windows\Fonts\roman.fon Opens: C:\Windows\Fonts\script.fon Opens: C:\Windows\Fonts\andlso.ttf Opens: C:\Windows\Fonts\arabtype.ttf Opens: C:\Windows\Fonts\simpo.ttf Opens: C:\Windows\Fonts\simpbdo.ttf C:\Windows\Fonts\simpfxo.ttf Opens: Opens: C:\Windows\Fonts\majalla.ttf Opens: C:\Windows\Fonts\majallab.ttf

Opens: C:\Windows\Fonts\trado.ttf Opens: C:\Windows\Fonts\tradbdo.ttf Opens: C:\Windows\Fonts\ahronbd.ttf Opens: C:\Windows\Fonts\david.ttf Opens: C:\Windows\Fonts\davidbd.ttf Opens: C:\Windows\Fonts\frank.ttf Opens: C:\Windows\Fonts\lvnm.ttf Opens: C:\Windows\Fonts\lvnmbd.ttf Opens: C:\Windows\Fonts\mriam.ttf Opens: C:\Windows\Fonts\mriamc.ttf Opens: C:\Windows\Fonts\nrkis.ttf Opens: C:\Windows\Fonts\rod.ttf Opens: C:\Windows\Fonts\simfang.ttf Opens: C:\Windows\Fonts\simhei.ttf Opens: C:\Windows\Fonts\simkai.ttf  ${\tt C:\Windows\Fonts\angsau.ttf}$ Opens: Opens: C:\Windows\Fonts\angsaui.ttf Opens: C:\Windows\Fonts\angsaub.ttf C:\Windows\Fonts\angsauz.ttf Opens: Opens: C:\Windows\Fonts\browa.ttf Opens: C:\Windows\Fonts\browai.ttf Opens: C:\Windows\Fonts\browab.ttf Opens: C:\Windows\Fonts\browaz.ttf Opens: C:\Windows\Fonts\browau.ttf Opens: C:\Windows\Fonts\browaui.ttf Opens: C:\Windows\Fonts\browaub.ttf Opens: C:\Windows\Fonts\browauz.ttf Opens: C:\Windows\Fonts\cordiau.ttf Opens: C:\Windows\Fonts\cordiaub.ttf Opens: C:\Windows\Fonts\cordiauz.ttf C:\Windows\Fonts\cordiaui.ttf Opens: Opens: C:\Windows\Fonts\upcdl.ttf Opens: C:\Windows\Fonts\upcdi.ttf C:\Windows\Fonts\upcdb.ttf Opens: Opens: C:\Windows\Fonts\upcdbi.ttf Opens: C:\Windows\Fonts\upcel.ttf Opens: C:\Windows\Fonts\upcei.ttf Opens: C:\Windows\Fonts\upceb.ttf Opens: C:\Windows\Fonts\upcebi.ttf Opens: C:\Windows\Fonts\upcfl.ttf Opens: C:\Windows\Fonts\upcfi.ttf Opens: C:\Windows\Fonts\upcfb.ttf C:\Windows\Fonts\upcfbi.ttf Opens: Opens: C:\Windows\Fonts\upcil.ttf Opens: C:\Windows\Fonts\upcii.ttf Opens: C:\Windows\Fonts\upcib.ttf Opens: C:\Windows\Fonts\upcibi.ttf Opens: C:\Windows\Fonts\upcjl.ttf Opens: C:\Windows\Fonts\upcji.ttf Opens: C:\Windows\Fonts\upcjb.ttf Opens: C:\Windows\Fonts\upcjbi.ttf Opens: C:\Windows\Fonts\upckl.ttf Opens: C:\Windows\Fonts\upcki.ttf Opens: C:\Windows\Fonts\upckb.ttf C:\Windows\Fonts\upckbi.ttf Opens: Opens: C:\Windows\Fonts\upcll.ttf C:\Windows\Fonts\upcli.ttf Opens: Opens: C:\Windows\Fonts\upclb.ttf Opens: C:\Windows\Fonts\upclbi.ttf Opens: C:\Windows\Fonts\kaiu.ttf  $C:\Windows\Fonts\l_10646.ttf$ Opens: Opens: C:\Windows\Fonts\ariblk.ttf Opens: C:\Windows\Fonts\calibri.ttf Opens: C:\Windows\Fonts\calibrii.ttf Opens: C:\Windows\Fonts\calibrib.ttf Opens: C:\Windows\Fonts\calibriz.ttf Opens: C:\Windows\Fonts\cambria.ttc Opens: C:\Windows\Fonts\cambriai.ttf Opens: C:\Windows\Fonts\cambriab.ttf Opens: C:\Windows\Fonts\cambriaz.ttf Opens: C:\Windows\Fonts\Candara.ttf Opens: C:\Windows\Fonts\Candarai.ttf Opens: C:\Windows\Fonts\Candarab.ttf Opens: C:\Windows\Fonts\Candaraz.ttf C:\Windows\Fonts\comic.ttf Opens: Opens: C:\Windows\Fonts\comicbd.ttf Opens: C:\Windows\Fonts\consola.ttf Opens: C:\Windows\Fonts\consolai.ttf Opens: C:\Windows\Fonts\consolab.ttf Opens: C:\Windows\Fonts\consolaz.ttf Opens: C:\Windows\Fonts\constan.ttf Opens: C:\Windows\Fonts\constani.ttf Opens: C:\Windows\Fonts\constanb.ttf Opens: C:\Windows\Fonts\constanz.ttf Opens: C:\Windows\Fonts\corbel.ttf Opens: C:\Windows\Fonts\corbeli.ttf Opens: C:\Windows\Fonts\corbelb.ttf Opens: C:\Windows\Fonts\corbelz.ttf

```
Opens:
                         C:\Windows\Fonts\framd.ttf
 Opens:
                         C:\Windows\Fonts\framdit.ttf
 Opens:
                         C:\Windows\Fonts\Gabriola.ttf
 Opens:
                         C:\Windows\Fonts\georgia.ttf
 Opens:
                         C:\Windows\Fonts\georgiai.ttf
 Opens:
                         C:\Windows\Fonts\georgiab.ttf
 Opens:
                         C:\Windows\Fonts\georgiaz.ttf
 Opens:
                         C:\Windows\Fonts\pala.ttf
 Opens:
                         C:\Windows\Fonts\palai.ttf
                         C:\Windows\Fonts\palab.ttf
 Opens:
                         C:\Windows\Fonts\palabi.ttf
 Opens:
 Opens:
                         C:\Windows\Fonts\segoepr.ttf
 Opens:
                         C:\Windows\Fonts\segoeprb.ttf
                         C:\Windows\Fonts\trebuc.ttf
 Opens:
 Opens:
                         C:\Windows\Fonts\trebucit.ttf
 Opens:
                         C:\Windows\Fonts\trebucbd.ttf
 Opens:
                         C:\Windows\Fonts\trebucbi.ttf
 Opens:
                         C:\Windows\Fonts\verdana.ttf
 Opens:
                         C:\Windows\Fonts\verdanai.ttf
 Opens:
                         C:\Windows\Fonts\verdanab.ttf
 Opens:
                         C:\Windows\Fonts\verdanaz.ttf
 Opens:
                         C:\Windows\Fonts\webdings.ttf
                         C:\Windows\Fonts\coure.fon
 Opens:
 Opens:
                         C:\Windows\Fonts\serife.fon
 Opens:
                         C:\Windows\Fonts\sserife.fon
 Opens:
                         C:\Windows\Fonts\smalle.fon
 Opens:
                         C:\Windows\Fonts\smallf.fon
 Opens:
                         C:\windows\temp\dwmapi.dll
                         C:\Windows\System32\dwmapi.dll
 Opens:
 Opens:
                         C:\Windows\Fonts\StaticCache.dat
                         C:\Windows\System32\en-US\user32.dll.mui
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                         C:\Windows\winsxs\x86_microsoft.windows.common-
 Opens:
controls\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2 \setminus comctl32.dl1
                         C:\Windows\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\Windows\system32\uxtheme.dll.Config
 Opens:
                         C:\windows\temp\cmd.exe
 Opens:
                         C:\Windows\System32\cmd.exe
 Opens:
                         C:\Windows\System32\apphelp.dll
 Opens:
                         C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
 Opens:
 Opens:
                         C:\Program Files
 Opens:
                         C:\Program Files\Adobe
 Opens:
                         C:\Program Files\Adobe\Reader 9.0
 Opens:
                         C:\Program Files\Adobe\Reader 9.0\Reader
 Opens:
                         C:\Windows\Branding
 Opens:
                         C:\Windows\Branding\Basebrd
 Opens:
                         C:\Windows\Branding\Basebrd\en-US
 Opens:
                         C:\Windows\Globalization
 Opens:
                         C:\Windows\Globalization\Sorting
 Opens:
                         C:\Windows\System32\en-US
 Opens:
                         C:\Windows\System32\ntdll.dll
 Opens:
                         C:\Windows\System32\kernel32.dll
 Opens:
                         C:\Windows\System32\apisetschema.dll
 Opens:
                         C:\Windows\System32\KernelBase.dll
 Opens:
                         C:\Windows\System32\locale.nls
 Opens:
                         C:\Windows\System32\msvcrt.dll
 Opens:
                         C:\Windows\System32\winbrand.dll
 Opens:
                         C:\Windows\System32\user32.dll
 Opens:
                         C:\Windows\System32\gdi32.dll
 Opens:
                         C:\Windows\System32\lpk.dll
 Opens:
                         C:\Windows\System32\usp10.dll
 Opens:
                         C:\Windows\System32\msctf.dll
 Opens:
                         C:\Windows\System32\en-US\cmd.exe.mui
 Opens:
                         C:\Windows\Branding\Basebrd\basebrd.dll
                         C:\Windows\Branding\Basebrd\en-US\basebrd.dll.mui
 Opens:
 Opens:
                         C:\Program Files\Adobe\Reader 9.0\Reader\icucnv36.dll
 Opens:
                         C:\windows\temp\CRYPTSP.dll
 Opens:
                         C:\Windows\System32\cryptsp.dll
 Opens:
                         C:\Windows\System32\rsaenh.dll
 Opens:
                         C:\windows\temp\RpcRtRemote.dll
 Opens:
                         C:\Windows\System32\RpcRtRemote.dll
 Opens:
                         C:\Windows\system32\Branding\Basebrd\Basebrd.dll
                         C:\Windows\System32\nslookup.exe
 Opens:
 Opens:
                         C:\Windows\AppPatch\sysmain.sdb
 Opens:
                         C:\Windows\system32\ui\SwDRM.dll
 Opens:
                         C:\Windows\Prefetch\NSLOOKUP.EXE-3D06E09F.pf
 Opens:
                         C:\Windows\System32\wsock32.dll
 Opens:
                         C:\Windows\System32\mswsock.dll
 Opens:
                         C:\Windows\System32\dnsapi.dll
 Opens:
                         C:\Windows\System32\en-US\nslookup.exe.mui
 Opens:
                         C:\Windows\System32\WSHTCPIP.DLL
 Opens:
                         C:\Windows\System32\nlaapi.dll
 Opens:
                         C:\Windows\System32\NapiNSP.dll
                         C:\Windows\System32\pnrpnsp.dll
 Opens:
 Opens:
                         C:\Windows\System32\winrnr.dll
                         C:\Windows\System32\IPHLPAPI.DLL
 Opens:
```

C:\Windows\System32\winnsi.dll Opens: Opens: C:\Windows\System32\dhcpcsvc6.dll C:\Windows\System32\dhcpcsvc.dll Opens:

Reads from: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config

Reads from: C:\Windows\Fonts\StaticCache.dat Reads from: C:\Windows\Prefetch\CMD.EXE-4A81B364.pf Reads from: C:\Windows\System32\nslookup.exe

#### **Network Events**

8.8.8.8.in-addr.arpa DNS query:

WORKGROUP DNS query: MSBROWSE DNS query: 8.8.8.8:53 Connects to: Sends data to: 8.8.8.8:53 Receives data from: 8.8.8.8:53

## Windows Registry Events

Creates key: HKLM\software\microsoft\fusion\gacchangenotification\default

Creates key: HKCU\software\microsoft\gdiplus

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKCU\

Opens key:  ${\tt HKCU \backslash control\ panel \backslash desktop \backslash muicached \backslash machine language configuration}$ 

Opens key: HKLM\software\policies\microsoft\mui\settings

Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens kev: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ side by side$ 

Opens key:

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

HKLM\software\microsoft\.netframework\policy\ Opens key: Opens key: HKLM\software\microsoft\.netframework\policy\v2.0

Opens key: HKLM\software\microsoft\.netframework

HKLM\software\microsoft\.netframework\policy\upgrades Opens key: Opens key: HKLM\software\microsoft\.netframework\policy\standards HKLM\software\microsoft\.netframework\policy\apppatch Opens key: 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 kev: HKLM\software\microsoft\windows nt\currentversion\windows  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ .net framework\+ policy\+ standards$ Opens key:

Opens key:  $HKLM \ software \ `microsoft\ .net framework \ policy \ standards \ \ v2.0.50727$ 

Opens key:

 $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} which is a function of the local properties of the local pro$ 

Opens key: HKCU\software\microsoft\.netframework Opens kev: HKLM\software\microsoft\fusion

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

options\rajivapp1.exe

Opens key: HKCU\software\microsoft\fusion

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

options Opens kev:

 $HKLM \verb|\software\microsoft|. netframework \verb|\security\policy\extensions\namedpermission sets|$ 

 $HKLM \ 's of tware \ 'microsoft'. net framework \ 's ecurity \ 'policy' extensions \ 'n amed permission sets \ 'internet \ 'policy' extensions \ 'n amed permission sets \ 'internet \ 'policy' extensions \ 'n amed \ 'policy' extensions \ 'policy' extensio$ Opens key:

 $HKLM \ software \ microsoft \ .net framework \ security \ policy \ extensions \ named permission sets \ local intranet$  $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \software \microsoft \windows nt \current version \profile list \s-1-5-21-1000 \end{tabular} .$ Opens key:

2160590473-689474908-1361669368-1002

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions

Opens key: HKLM\software\microsoft\ole Opens key: HKLM\software\microsoft\ole\tracing

Opens key:

a03a-e3ef65729f3d}

Opens key:

a03a-e3ef65729f3d}\propertybag

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

Opens key:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in following \ description \ for the constraint \ description \$ 

Opens key:

 $\label{thm:local_hammon} HKCU \software \microsoft \windows \current version \explorer \session in folders \current \c$ 

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders

HKLM\svstem\currentcontrolset\control\nls\customlocale Opens kev: Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\software\policies\microsoft\windows\explorer

```
Opens key:
                                                                                                                                 HKCU\software\policies\microsoft\windows\explorer
        Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}
        Opens key:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-164e7descriptions\} \ for the software \ microsoft \ windows \ for the software \ microsoft \ micr
9afe-ea3317b67173}\propertybag
         Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
                                                                                                                                HKLM\software\microsoft\.netframework\v2.0.50727\securitv\policv
        Opens kev:
        Opens key:
                                                                                                                                HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32
        Opens key:
                                                                                                                                HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ in dex 145
        Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ii \ 181938c6 \ 7950e2c5
       Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89
        Opens key:
ba85-6007caedcf9d}
        Opens key:
ba85-6007caedcf9d}\propertybag
        Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\38c56119\1d3ee2d7
                                                                                                                                \label{lem:hklm} \verb+Kklm \software \verb+ microsoft \verb+ net framework setup \verb+ dotnetclient \verb+ v3.5+ \\
        Opens kev:
                                                                                                                                HKLM\software\microsoft\strongname
        Opens key:
        Opens key:
                                                                                                                                HKLM\software\microsoft\fusion\publisherpolicy\default
        Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default \setminus policy. 2.0. system. windows. forms \underline{\phantom{}}b77a5c561934e089
        Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 32\ni\61e7e666\c991064
       Opens kev
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82
         Opens key:
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ il \ 475 dce 40 \ 2d382 ce 6 \ 8ccc \ mages in dex \ v2.0.50727\_32 \ il \ 475 dce 40 \ 2d382 ce 6 \ 8ccc \ mages in dex \ v2.0.50727\_32 \ il \ 475 dce 40 \ 2d382 ce 6 \ 8ccc \ mages in dex \ v2.0.50727\_32 \ il \ 475 dce 40 \ 2d382 ce 6 \ 8ccc \ mages in dex \ v2.0.50727\_32 \ il \ 475 dce 40 \ 2d382 ce 6 \ 8ccc \ mages in dex \ v2.0.50727\_32 \ il \ 475 dce 40 \ 2d382 ce 6 \ 8ccc \ mages in dex \ v2.0.50727\_32 \ il \ 475 dce 40 \ 2d382 ce 6 \ 8ccc \ mages in dex \ v2.0.50727\_32 \ il \ 475 dce 40 \ 2d382 ce 6 \ 8ccc \ mages in dex \ v2.0.50727\_32 \ il \ 475 dce 40 \ 2d382 ce 6 \ 8ccc \ mages in dex \ mages in de
       Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus i1 \setminus 19ab8d57 \setminus 1bd7b0d8 \setminus 8e
       Opens kev
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 163e1f5e \ 188e1 \ native images in dex \ v2.0.50727\_32 \ il\ 2dd6ac50 \ 188e1 \ native images in dex \ native im
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ il \ 424bd4d8 \ 1c83327b \ 8d
       Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\80
        Opens key
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ il\ 3ced59c5 \ 1b2590b1 \ 84ex \ descriptions \ description \ 
        Opens key:
Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus mi \setminus 30bc7c4f \setminus 3f50fe4f \setminus 8ff \setminus 8f
       Opens key:
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ il\ 3f50 fe4f \ bf1 da7aa \ bf1 da7aaa \ bf1 d
        Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83
        Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ i1 \ 6dc7d4c0 \ a5cd4db \ 86dc7d4c0 \ a5cd4db \
       Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.drawing_b03f5f7f11d50a3a
         Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system_b77a5c561934e089
       Opens key:
HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ policy. 2.0. \ system. \ xml\_b77a5c561934e089
       Opens key:
HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ policy. 2.0. system. configuration \underline{\ \ } b03f5f7f11d50a3a
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.deployment__b03f5f7f11d50a3a
       Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default \setminus policy. 2.0. system. runtime. serialization. for matters. so ap\_b03f5f7f11d50a3a
        Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.accessibility_b03f5f7f11d50a3a
         Opens key:
HKLM \label{lem:hklm} Which is a fixed by the second of 
                                                                                                                                HKLM\software\microsoft\.netframework\policy\aptca
        Opens key:
        Opens key:
                                                                                                                                 HKLM\hardware\devicemap\video
        Opens key:
                                                                                                                                HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000
        Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&0&10
                                                                                                                                HKLM\software\microsoft\windows nt\currentversion\fonts
        Opens key:
        Opens key:
                                                                                                                                HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
        Opens key:
                                                                                                                                HKCU\eudc\1252
        Opens key:
                                                                                                                                HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
         Opens key:
                                                                                                                                 HKLM\system\currentcontrolset\control\nls\locale
        Opens key:
                                                                                                                                 HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
        Opens kev:
                                                                                                                                HKLM\system\currentcontrolset\control\nls\language groups
                                                                                                                                HKLM\software\microsoft\windows
        Opens key:
```

nt\currentversion\languagepack\datastore\_v1.0

```
HKLM\software\microsoft\windows
   Opens key:
nt\currentversion\languagepack\surrogatefallback
   Opens key:
                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
   Opens key:
                                            HKLM\system\currentcontrolset\control\cmf\config
   Opens key:
                                            HKLM\software\microsoft\windows\currentversion\policies\explorer
   Opens key:
                                            HKCU\software\microsoft\windows\currentversion\policies\explorer
   Opens key:
                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
   Opens kev:
                                            HKLM\system\currentcontrolset\control\session manager\appcertdlls
   Opens key:
                                            HKLM\system\currentcontrolset\control\session manager\appcompatibility
   Opens key:
                                            HKLM\software\policies\microsoft\windows\appcompat
   Opens key:
                                            HKCU\software\microsoft\windows nt\currentversion
   Opens key:
                                            \label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\windows} nt\current\version\app\compatflags\layers} \\
   Opens key:
                                            HKLM\software\microsoft\windows nt\currentversion\appcompatflags
   Opens key:
                                            HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
   Opens kev:
                                            HKLM\software\microsoft\rpc
   Opens key:
                                            HKLM\system\currentcontrolset\control\computername\activecomputername
   Opens key:
                                            HKLM\system\setup
   Opens key:
                                            HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
                                            HKLM\software\policies\microsoft\sqmclient\windows
                                            HKLM\software\microsoft\sqmclient\windows
   Opens key:
   Opens key:
                                            HKCU\software\classes\
                                            HKCU\software\classes\appid\rajivapp1.exe
   Opens key:
   Opens key:
                                            HKCR\appid\rajivapp1.exe
   Opens key:
                                            HKLM\software\microsoft\ole\appcompat
   Opens kev:
                                            HKLM\system\currentcontrolset\control\lsa
   Opens key:
                                            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
                                            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
   Opens key:
   Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
                                            HKLM\software\policies\microsoft\cryptography
   Opens kev:
   Opens key:
                                            HKLM\software\microsoft\cryptography
   Opens key:
                                            {\tt HKLM \ } software \verb|\ microsoft \verb|\ cryptography \verb|\ offload|
   Opens key:
                                            \label{local-cond} \mbox{HKCU\software\classes\interface} \ \{00000134-0000-0000-c000-000000000046\} \ \mbox{HKCU\software\classes\second} \ \ \mbox{HKCU\software\classes\secon
   Opens key:
                                            HKCR\interface\{00000134-0000-0000-c000-00000000046}
   Opens key:
                                            HKCU\software\classes\interface\{00000134-0000-0000-c000-
00000000046}\proxystubclsid32
   Opens key:
                                            Opens key:
                                            HKLM\software\microsoft\rpc\extensions
   Opens key:
                                            HKLM\system\currentcontrolset\services\bfe
   Opens key:
                                            HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
   Opens key:
                                            HKLM\software\microsoft\sqmclient\windows\disabledsessions\
   Opens key:
                                            HKCU\software\policies\microsoft\windows\system
   Opens key:
                                            HKLM\software\microsoft\command processor
   Opens key:
                                            HKCU\software\microsoft\command processor
   Opens key:
                                            HKLM\software\microsoft\windows\windows error reporting\wmr
   Opens key:
                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\nslookup.exe
   Opens key:
                                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\shell} folders}
   Opens key:
                                            \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \en
   Opens key:
                                            HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\nslookup.exe
   Opens key:
                                            HKLM\system\currentcontrolset\services\winsock2\parameters
   Opens kev:
                                            HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\3a41eaa2-3373a944
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\3a41eaa2
   Opens key:
\label{lem:hklm} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9 \end{tabular}
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000003
  Opens key:
Opens kev
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens kev:
```

Opens key:

```
Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ catalog\_entries \ 100000000000012
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000013
 Opens key:
HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ protocol\_catalog\_entries \ \ 000000000014
 Opens key:
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog_entries\00000000017
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000000
 Opens key:
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\0000000000003
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005
 Opens key:
Opens kev:
                     HKLM\svstem\currentcontrolset\services\winsock\parameters
 Opens key:
                     HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
 Opens key:
                     HKLM\system\currentcontrolset\services\psched\parameters\winsock
 Opens key:
                     HKLM\system\currentcontrolset\services\winsock\setup migration\providers
 Opens key:
                     HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
                     HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock
 Opens kev:
 Opens key:
                     HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
                     HKLM \verb|\system| current control set \verb|\services| tcpip \verb|\parameters| \\
 Opens key:
 Opens key:
                     HKLM\software\policies\microsoft\windows nt\dnsclient
 Opens key:
                     HKLM\system\currentcontrolset\services\dnscache\parameters
 Opens key:
                     HKLM\software\policies\microsoft\system\dnsclient
 Opens key:
                     HKLM\system\currentcontrolset\services\dns
 Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
 Opens key:
                     HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens key:
c19ce8a73253}
 Opens kev:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
1709a0196aed}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
 Opens key:
                     HKLM\system\currentcontrolset\services\tcpip\linkage
 Opens key:
                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\microsoft sans serif
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\3a41eaa2-2d47c47e
                     HKLM\software\microsoft\ctf\compatibility\rajivapp1.exe
 Opens key:
 Opens key:
                     Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key:
                     HKLM\software\microsoft\ctf\
                     HKLM\system\currentcontrolset\control\session
 Oueries value:
manager[cwdillegalindllsearch]
                     HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Queries value:
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Oueries value:
                     HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Oueries value:
                     HKCU\control panel\desktop[preferreduilanguages]
 Queries value:
                     HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus side by side [preferex ternal manifest]
 Oueries value:
                     HKLM\software\microsoft\.netframework[installroot]
                     HKLM\software\microsoft\.netframework[clrloadlogdir]
 Oueries value:
 Oueries value:
                     HKLM\software\microsoft\.netframework[onlyuselatestclr]
```

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles] HKLM\software\microsoft\windows

Queries value:

nt\currentversion\compatibility32[rajivapp1]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

HKLM\software\microsoft\.netframework[gcstressstart] Queries value: Queries value: HKLM\software\microsoft\.netframework[gcstressstartatjit] Queries value: HKLM\software\microsoft\.netframework[disableconfigcache]

HKLM\system\currentcontrolset\control\wmi\security[e13c0d23-ccbc-4e12-Oueries value:

931b-d9cc2eee27e41

Queries value: HKLM\system\currentcontrolset\control\wmi\security[cc2bcbba-16b6-4cf3-

8990-d74c2e8af500]

Queries value: HKLM\software\microsoft\fusion[cachelocation]

HKLM\software\microsoft\fusion[downloadcacheguotainkb] Queries value:

HKLM\software\microsoft\fusion[enablelog] Oueries value: Oueries value: HKLM\software\microsoft\fusion[logginglevel] Oueries value: HKLM\software\microsoft\fusion[forcelog] HKLM\software\microsoft\fusion[logfailures] Queries value: HKLM\software\microsoft\fusion[versioninglog] Queries value: HKLM\software\microsoft\fusion[logresourcebinds] Queries value: Oueries value: HKLM\software\microsoft\fusion[uselegacyidentityformat]

Queries value: HKLM\software\microsoft\fusion[disablemsipeek] HKLM\software\microsoft\fusion[noclientchecks] Queries value:

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options[devoverrideenable]

HKLM\software\microsoft\ole[pageallocatorusesystemheap] Oueries value: Oueries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

Queries value:

a03a-e3ef65729f3d}[category]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[name]

Queries value:

a03a-e3ef65729f3d}[parentfolder]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[description]

Queries value:

a03a-e3ef65729f3d}[relativepath]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[parsingname]

Oueries value:

a03a-e3ef65729f3d}[infotip]

Queries value:

a03a-e3ef65729f3d}[localizedname]

a03a-e3ef65729f3d}[icon]

Oueries value:

a03a-e3ef65729f3d}[security]

Queries value:

a03a-e3ef65729f3d}[streamresource]

Queries value:

a03a-e3ef65729f3d}[streamresourcetype]

Queries value:

a03a-e3ef65729f3d}[localredirectonly]

Queries value:

a03a-e3ef65729f3d}[roamable]

Oueries value:

a03a-e3ef65729f3d}[precreate]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[stream]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[publishexpandedpath]

Queries value:

a03a-e3ef65729f3d}[attributes]

Oueries value:

a03a-e3ef65729f3d}[foldertypeid]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[initfolderhandler]

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

folders[appdata]

Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \footnote{1.5} \$ 

Oueries value:

Queries value:

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \folder\folder \folder \folder \folder \folder \folder \folder \folder \$ 

Queries value:

Queries value:

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \ensuremath{\mbox{\correntversion}\explorer \folder descriptions} \footnote{1.5e} \f$ 

Queries value:

 $\label{thm:local-problem} HKLM \software \windows \current version \explorer \folder descriptions \folder \f$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]

Queries value:

 $\label{thm:local-condition} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \footnote{1} \footnote{1} \footnote{2} \footnote$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]

Queries value:

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [roamable]$ 

Queries value:

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{5}e6c858f-0e22-4760-9afe-ea3317b67173\footnote{1}{5}e6c858f-0e22-4760-9afe-ea33170$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \folder\folder \folder \folder \folder \folder \folder \folder \folder \$ 

Queries value:

Queries value:

Queries value:

 $\label{thm:ham} HKLM \software \mbox{$^{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]}$ 

 $\label{lem:profile} Queries \ value: \\ HKLM\ software \ microsoft\ windows \ nt\ current version\ profile list\ s-1-5-21-2160590473-689474908-1361669368-1002 [profile image path]$ 

Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32[latestindex]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus index 145 [nius agemask]$ 

Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\index145[ilusagemask]

Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\181938c6\7950e2c5\89[displayname]
Oueries value:

 $\label{lem:hklmsoftware} HkLM \software \end{area} Hklm \software \end{area} A software \end{area} In $1938c6 \7950e2c5 \89 \end{area} Configstring Queries value:$ 

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\181938c6\7950e2c5\89[mvid]
Oueries value:

 $\label{lem:hklm} HKLM \software \microsoft \sinon \native images in dex \v2.0.50727\_32 \ni \native images in dex \v2.$ 

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\181938c6\7950e2c5\89[status] Queries value:

 $HKLM \label{eq:hkkm} Ksoftware \verb|\microsoft| fusion \verb|\nativeimagesindex| v2.0.50727\_32 \verb|\ni| 181938c6 \verb|\nativeimagesindex| v2.0.50727\_32 \verb|\nativeimagesindex| v2.0.5$ 

Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\181938c6\7950e2c5\89[missingdependencies]
Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\7950e2c5\183e33de\89[displayname]
Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\i1\7950e2c5\183e33de\89[status]
Oueries value:

 $\label{lem:hklm} HkLM \software \end{microsoft fusion \native images in dex $$v2.0.50727\_32\il\7950e2c5\183e33de\89[modules]$$ Oueries value:$ 

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\7950e2c5\183e33de\89[sig]
Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\7950e2c5\183e33de\89[lastmodtime]

HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,x86]
Oueries value:

 $\label{thm:hklm} HKL^{M} software \ensuremath{\mbox{\mbox{$1$}}} In the label{thm:hklm} which is a superior \ensuremath{\mbox{\mbox{$4$}}} In the label{thm:hklm} as the label{thm:hklm} has been descriptions \ensuremath{\mbox{$4$}}. The label{thm:hklm} as the label{thm:hklm} has been described \ensuremath{\mbox{$4$}}. The label{thm:hklm} as the label{thm:hklm} as the label{thm:hklm} as the label{thm:hklm} has been described \ensuremath{\mbox{$4$}}. The label{thm:hklm} as the l$ 

Queries value:

 $\label{lem:hklmsoftware} HkLM \software \ensuremath{\sc Nicrosoft \windows \current \version} \ensuremath{\sc Nicrosoft \windows \current \version \ensuremath{\sc Nicrosoft \windows \current \windows \ensuremath{\sc Nicrosoft \windows \current \windows \window$ 

Queries value:

 $\label{lem:hkklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cite{252481e8-33be-4251-ba85-6007} \cite{252481e8-33be-4251-ba$ 

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{352481e8-33be-4251-ba85-6007 \ caed \ cf9d\} \ [description]$ 

Queries value:

Queries value:

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} \end{subarray} $$4352481e8-33be-4251-ba85-6007 \caedcf9d \cal{lem:hklmsoftware} \label{lem:hklmsoftware} $$$15007 \caedcf9d \cal{lem:hklmsoftware} $$$15007 \caedcf9d \cal{lem:hklmsoftware} $$$15007 \caedcf9d \caed$ 

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\{352481e8-33be-4251-ba85-6007 \ caedcf9d\} \ 'flocalized name' \ |$ 

Oueries value:

 $\label{lem:hkkm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hkkm} \footnote{1.000} \cite{1.000} \$ 

Queries value:

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} If the label{lem:hklm} If the label{lem:hklm} HKLM \label{lem:hklm} If the label{lem:hklm} If the label{lem:hklm} If the label{lem:hklm} HKLM \label{lem:hklm} If the label{lem:hklm} If$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]

Queries value:

 $\label{thm:local_ham} HKLM \software \ensuremath{\mbox{\mbox{$152481e8-33be-4251-ba85-6007}} \ensuremath{\mbox{\mbox{$152481e8-33be-4251-ba85-6007}} \ensuremath{\mbox{\mbox{$1607$}} \ensuremath{\mbox{$1607$}} \ensuremath{\mbox{$1607$}}$ 

Queries value:

Oueries value:

 $\label{thm:hklm} HKL^{M} software \ensuremath{\text{\sc higher}} as 52481e8-33be-4251-ba85-6007 caedcf9d \ensuremath{\text{\sc higher}} [precreate]$ 

Oueries value

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 \ caedcf9d\} \ [stream]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cite{252481e8-33be-4251-ba85-6007} \cite{252481e8-33be-4251-ba85-$ 

Oueries value

 $HKLM\software\mbox{\tt hkLM}\software\mbox{\tt hkLM}\software\mbox{\tt hicrosoft\windows\currentversion}\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007\caedcf9d}\ [attributes]$ 

Queries value:

 $HKLM\software\mbox{\tt hkLM}\software\mbox{\tt hkLM}\software\mbox{\tt$ 

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\{352481e8-33be-4251-ba85-6007 \ caedcf9d\}[initfolder \ handler]$ 

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

folders[cache]

Queries value: HKLM\software\microsoft\fusion\publisherpolicy\default[latest]
Queries value: HKLM\software\microsoft\fusion\publisherpolicy\default[index4]
Queries value:

 $HKLM \verb|\software\microsoft\fusion\publisherpolicy\default[legacypolicytimestamp]|$ 

Queries value:

 $\label{local-bound} HKLM \software \microsoft \sion \native images in dex \v2.0.50727\_32 \ni\61e7e666 \c991064 \82[display name] \\ Oueries \value:$ 

 $\label{lem:hklmsoftware} HKLM \software \mbox{$\sim 1.50727\_32\ni\61e7e666\c991064\82[configmask] Queries value:}$ 

 $\label{lem:hklmsoftware} HKLM \software \mbox{$\sim$ 1.50727\_32\ni\61e7e666\c991064\82[configstring] Queries value:}$ 

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus ni \setminus 61e7e666 \setminus c991064 \setminus 82 [mvid]$ 

- Queries value:
- $\label{local-ham} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727\_32 \ni\61e7e666 \c991064 \82 \end{2} evaluation data Queries value:}$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\61e7e666\c991064\82[ildependencies]
   Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ ni \ 61e7e666 \ c991064 \ 82 \ [missing dependencies] \\ Oueries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\475dce40\2d382ce6\8c[displayname]
  Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\i1\475dce40\2d382ce6\8c[status]
  Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\475dce40\2d382ce6\8c[modules]
  Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\475dce40\2d382ce6\8c[sig] Oueries value:
- $\label{local-equation} HKLM software \mbox{\cosoft} \sl ware \mbox{\cosoft}$
- $\label{lem:hklmsoftware} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727\_32\mbox{\sc il}\19ab8d57\1bd7b0d8\8e[displayname] Queries\ value:$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sion \native images in dex \normalized 2.0.50727\_32 \normalized 19ab8d57 \normali$
- $\label{lem:hklmsoftware} HKLM \software \sinces index \sinces 2.0.50727\_32 \sinces 2.0.5072$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\19ab8d57\1bd7b0d8\8e[sig]
  Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\19ab8d57\1bd7b0d8\8e[lastmodtime]
   Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\2dd6ac50\163e1f5e\88[displayname]
  Oueries value:
- $\label{local-equation} HKLM \software \mbox{$\le$ index$} \scale{local-equation} A simple \sca$
- $\label{local-equation} HKLM\software\microsoft\fusion\native images in dex $$v2.0.50727\_32\il\2dd6ac50\163e1f5e\88[modules]$$ Queries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\2dd6ac50\163e1f5e\88[sig] Oueries value:
- $\label{local-equation} HKLM \software \mbox{$\mbox{$\mbox{$\sim$}}$} It \some \software \mbox{$\mbox{$\sim$}} Ali \some \som$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\424bd4d8\1c83327b\8d[status]
  Oueries value:
- $\label{lem:hklm} $$HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\424bd4d8\1c83327b\8d[sig] $$Oueries\ value:$
- $\label{local-bound} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727\_32\il\424bd4d8\lc83327b\8d[lastmodtime] Queries value:$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{local-equation} $HKL^M\software\microsoft\fusion\native images index \v2.0.50727\_32\il\41c04c7e\7f3b6ac4\80[status] Oueries value:$
- $\label{lem:hklmsoftware} HkLM \software \end{area} Hklm \software \end{area} Nuclear \software \end{area} Nuclear \software \end{area} Oueries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\41c04c7e\7f3b6ac4\80[sig] Oueries value:
- $\label{local-equation} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727\_32\il\41c04c7e\7f3b6ac4\80[last mod time] \\ Queries\ value:$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{local-prop} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727\_32 \il\aced 59c5 \label{local-prop} 1b2590b1 \sales \fusion \native images in dex \v2.0.50727\_32 \il\aced 59c5 \label{local-prop} 1b2590b1 \sales \fusion \native images in dex \v2.0.50727\_32 \il\aced 59c5 \label{local-prop} 1b2590b1 \sales \fusion \native images \fusion \native images \fusion \native images \fusion \native images \fusion \native \$
- $\label{local-bound} HKLM software \microsoft \sion \native images in dex \v2.0.50727\_32 \sin \side \$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\3ced59c5\1b2590b1\84[sig]
  Oueries value:
- $\label{local-equation} HKLM \software \mbox{$\mbox{$\mbox{$\sim$}}$ il \scd59c5\lb2590b1\84[last mod time]} \\ Queries value:$
- $\label{local-bound} HKLM\software\microsoft\fusion\native\magesindex\v2.0.50727\_32\il\c991064\2bd33e1c\81[displayname] \\ Oueries\ value:$
- $\label{local-prop} HKLM \software \mbox{$\mbox{$\mbox{$\sim$}} 1.059727\_32\il\c991064\2bd33e1c\81[status]$ Queries value:}$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sinon \native images in dex \normalized 2.0.50727\_32 \sinon \n$
- $\label{thm:local-bound} HKLM\software\mbox{\cosoft\fusion\native} images index \cosoft\coso$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\c991064\2bd33e1c\81[lastmodtime]
  Queries value:
- $\label{lem:hklmsoftware} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\sl 2.0.50727\_32\mbox{ni}\30bc7c4f\3f50fe4f\8f[displayname] Queries\ value:$
- $\label{local-equation} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727\_32\ni\30bc7c4f\3f50fe4f\8f[configmask]\ Queries\ value:$
- $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 8f[configstring] \ Oueries \ value:$
- $HKLM\software\mbox{\tt hicrosoft\fusion\native} images in dex\v2.0.50727\_32\mbox{\tt ni\30bc7c4f\3f50fe4f\8f[mvid]}$

```
Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus ni \setminus 30bc7c4f \setminus 3f50fe4f \setminus 8f[evalation data]
      Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 8f[status]
      Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus ni \setminus 30bc7c4f \setminus 3f50fe4f \setminus 8f[ildependencies]
      Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 30bc7c4f \ 8f[nidependencies]
      Queries value:
HKLM \label{lem:hklm} Software \mbox{\cosft} fusion \mbox{\cosftware} \mbox{\cosft
      Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 3f50fe4f \ 6f1da7aa\ 8f[displayname]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus i1 \setminus 3f50 fe4f \setminus 6f1 da7aa \setminus 8f[status]
     Queries value:
Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 3f50fe4f \ 6f1da7aa \ 8f[sig]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i1 \setminus 3f50 fe4f \setminus 6f1 da7aa \setminus 8f[last mod time]
     Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 32\ni\3cca06a0\6dc7d4c0\83[displayname]
      Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus ni \setminus 3cca06a0 \setminus 6dc7d4c0 \setminus 83[configmask]
Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 32\ni\3cca06a0\6dc7d4c0\83[mvid]
      Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[evalationdata]
      Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni\ 3cca06a0\ 6dc7d4c0\ 83[status]
      Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 3cca 06a0 \ 6dc 7d4c0 \ 83[ildependencies]
      Queries value:
HKLM \label{lem:hklm} Software \mbox{\sca06a0\6dc7d4c0\83[nidependencies]} \\
      Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 83 \ [missing dependencies]
     Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\86[displayname]
      Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ i1 \ 6dc7d4c0 \ a5cd4db \ 86[status]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i1 \setminus 6dc7d4c0 \setminus a5cd4db \setminus 86 [modules]
     Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ i1 \ 6dc7d4c0 \ a5cd4db \ 86 \ [sig] \ for the software \ microsoft \ fusion \ native images index \ native \ nat
      Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 6dc7d4c0\ a5cd4db\ 86[last mod time]
      Oueries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.windows.forms,2.0.0.0,,b77a5c561934e089,msil]
      Queries value:
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \
      Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system,2.0.0.0,,b77a5c561934e089,msil]
      Oueries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.xml,2.0.0.0,,b77a5c561934e089,msil]
      Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default[system.configuration, 2.0.0.0, , b03f5f7f11d50a3a, msil] + (b1) + (b2) + (b
      Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchangenotification \setminus default[system.deployment, 2.0.0.0, , b03f5f7f11d50a3a, msil] + (b1) + (b2) + (b2) + (b3) +
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchangenotification \setminus default[system.runtime.serialization.formatters.soap, 2.0.0.0, ,b03f5f7f11d50a3a, msil]
      Oueries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[accessibility,2.0.0.0,,b03f5f7f11d50a3a,msil]
      Queries value:
HKLM \label{lem:hklm} Software \verb|\microsoft| fusion \| gacchange notification \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the lemma security and the lemma secur
      Queries value:
                                                                                         HKLM\software\microsoft\.netframework[dbgjitdebuglaunchsetting]
      Queries value:
                                                                                          HKLM\software\microsoft\.netframework[dbgmanageddebugger]
                                                                                         HKLM\hardware\devicemap\video[maxobjectnumber]
      Oueries value:
      Oueries value:
                                                                                         HKLM\hardware\devicemap\video[\device\video3]
      Oueries value:
                                                                                         HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
 fd27e3774e32}\0000[pruningmode]
      Queries value:
                                                                                         HKCU\software\microsoft\gdiplus[fontcachepath]
                                                                                         HKLM\system\currentcontrolset\control\nls\locale[00000409]
      Queries value:
                                                                                         HKLM \verb|\system| current controlset| control \verb|\nls| language groups[1]
      Oueries value:
      Oueries value:
                                                                                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
                                                                                         HKLM\software\microsoft\windows
      Queries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                                                                                         HKLM\software\microsoft\windows
      Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane1]|
      Oueries value:
                                                                                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
      Queries value:
                                                                                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
```

Oueries value:

Queries value:

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

 $\verb| nt\currentversion \ | \ anguage pack \ | \ surrogatefall \ back[plane 4]|$ 

```
Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                          HKLM\software\microsoft\windows
 Oueries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane7]|
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
 Queries value:
                          HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane9]|
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                          HKLM\software\microsoft\windows
  Oueries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane11]|
 Queries value:
                          HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane12]|
 Oueries value:
                          HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane13]|
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
                          HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:
HKLM \verb|\software\policies\microsoft| windows \verb|\safer\codeidentifiers[authenticodeenabled]|
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
  Queries value:
                          HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
Oueries value:
                          HKLM\system\setup[oobeinprogress]
  Oueries value:
                          HKLM\svstem\setup[svstemsetupinprogress]
                          HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
  Queries value:
                          HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:
                          HKLM \verb|\system| current control \verb|\sa[everyoneincludes an ony mous]|
 Queries value:
                          HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
                          HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
 Oueries value:
cryptographic provider[image path]
                          HKLM\system\currentcontrolset\control\session
  Queries value:
manager[safeprocesssearchmode]
                          HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Oueries value:
  Oueries value:
                          HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
 Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography[privkeycachepurgeinterval seconds]
  Oueries value:
                          HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:
                          HKLM\software\microsoft\cryptography[machineguid]
                          HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:
                          HKLM\software\microsoft\rpc\extensions[remoterpcdll]
  Queries value:
                          HKLM\software\microsoft\sqmclient\windows\disabledprocesses[76c7ff28]
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
 Oueries value:
HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabledsessions [global session]
  Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
                          HKLM\software\microsoft\command processor[disableunccheck]
  Queries value:
  Oueries value:
                          HKLM\software\microsoft\command processor[enableextensions]
  Queries value:
                          HKLM\software\microsoft\command processor[delayedexpansion]
                          HKLM\software\microsoft\command processor[defaultcolor]
  Oueries value:
 Oueries value:
                          HKLM\software\microsoft\command processor[completionchar]
  Queries value:
                          HKLM\software\microsoft\command processor[pathcompletionchar]
                          HKLM\software\microsoft\command processor[autorun]
  Queries value:
  Queries value:
                          HKCU\software\microsoft\command processor[disableunccheck]
  Queries value:
                          HKCU\software\microsoft\command processor[enableextensions]
  Oueries value:
                          HKCU\software\microsoft\command processor[delayedexpansion]
  Oueries value:
                          HKCU\software\microsoft\command processor[defaultcolor]
  Oueries value:
                          HKCU\software\microsoft\command processor[completionchar]
                          HKCU\software\microsoft\command processor[pathcompletionchar]
  Queries value:
  Queries value:
                          HKCU\software\microsoft\command processor[autorun]
 Queries value:
                          HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Oueries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\layers[c:\windows\system32\nslookup.exe]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\compatibility32[nslookup]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
```

nt\currentversion\languagepack\surrogatefallback[plane5]

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[num\_catalog\_entries]
- Queries value:
- Oueries value:
- Queries value:
- Queries value:
- Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000006 \ [packed catalog item]$ Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000007 \ [packed catalog item]$ Oueries value:
- Queries value:
- Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000012 \ [packed catalog item]$ Oueries value:
- Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000014 \ [packed catalog item]$ Queries value:
- Oueries value:
- Queries value:
- Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000018[packedcatalogitem] Oueries value:
- Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries]
- Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 000000000001 \ [displaystring]$ Queries value:
- Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[addressfamily] Queries value:
- Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[enabled] Oueries value:
- Oueries value:
- $HKLM \ system \ \ current control set \ services \ \ winsock 2 \ parameters \ \ namespace\_catalog5 \ \ catalog\_entries \ \ \ 000000000001[storesserviceclassinfo]$ Queries value:
- Oueries value:
- Oueries value:
- Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog5 \ catalog\_entries \ 0000000000002 \ [providerid]$ Queries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 0000000000002 \ [address family]$ Oueries value:
- Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000002[enabled] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 0000000000002 \ [version]$ Oueries value:
- Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 0000000000002 \ [providerinfo]$ Queries value:
- Oueries value:
- Oueries value:
- Queries value:
- Oueries value:

Queries value:

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[librarypath]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerid]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily]
Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ supported namespace\_Queries \ value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[enabled]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[displaystring]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[enabled]
Oueries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[storesserviceclassinfo]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerinfo]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerid]
 Queries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 0000000000006 [address family] \\ Oueries \ value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[supportednamespace]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[enabled]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[storesserviceclassinfo]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerinfo]
Oueries value:

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

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2\_32 spin count]$ 

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

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \setminus parameters \setminus winsock[mapping]$ 

Queries value:

HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\psched[winsock 2.0 provider id]

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

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip[winsock 2.0 provider id]

Oueries value:

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

Queries value:

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

Queries value:

 $\label{local-parameters-winsock} $$HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] $$$ 

Queries value:

 $\label{thm:local_hammel} \begin{tabular}{ll} HKLM \end{tabular} winsock [helperdlname] \\$ 

Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[dnslookuporder]Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[domain]Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpdomain]Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]

HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpsearchlist] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel] HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [direct access query order]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Queries value:  $HKLM \verb|\system| current controlset \verb|\services| dns cache \verb|\parameters[register primary name]|$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register reverse lookup]$ Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value:  $\label{lem:hklm} \verb|HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]| \\$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: Oueries value:  ${\tt HKLM \normalfoot} \\ {\tt HKLM \normalfoot} \\ {\tt HKLM \normalfoot} \\ {\tt Idwn \normalfoot} \\ {\tt HKLM \normalfoot}$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]

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

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

Queries value: Queries value:

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] Oueries value: Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [resolver registration]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonlv] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[dnsquickquervtimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Queries value:

c19ce8a73253}[searchlist]

Oueries value:

c19ce8a73253}[enabledhcp]

Queries value:

c19ce8a73253}[registrationenabled]

Oueries value:

c19ce8a73253}[registeradaptername] Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[domain]

Queries value:

c19ce8a73253}[dhcpdomain]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[dhcpv6domain]

Oueries value:

c19ce8a73253}[nameserver]

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{128919e8-8a5e-41d1-ac17-428919e8-8a5e-4289196-8a5e-428919e8-8a5e-4289196-869196-869196-869196-869196-869196-869196-869196-869196-869196$ c19ce8a73253}[nameserver]

Oueries value:

c19ce8a73253}[dhcpnameserver]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enabledhcp]

Oueries value:

806e6f6e6963}[registrationenabled]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registeradaptername]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[domain]

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[dhcpdomain]

Oueries value:

806e6f6e6963}[nameserver]

806e6f6e6963}[dhcpnameserver]

Oueries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \true faces \{128919e8-8a5e-41d1-ac17-c19ce8a73253\} [queryadaptername]$ 

Queries value:

 $\label{thm:hklm} HKLM \system \current controls et \services \tcpip \parameters \traces \{128919e8-8a5e-41d1-ac17-c19ce8a73253\} [disable adapter domain name]$ 

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \time faces \{128919e8-8a5e-41d1-ac17-c19ce8a73253\} \[registration max address count]\]$ 

Queries value:

 $\label{lem:hkklmsystem} HKLM \system \current controls et \services \tcpip \parameters \ interfaces \ \{128919e8-8a5e-41d1-ac17-c19ce8a73253\} \ [maxnumber of addresses to register]$ 

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \time faces \{128919e8-8a5e-41d1-ac17-c19ce8a73253\} [enable multicast]$ 

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \true \equiv except \equiv$ 

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \time faces \equiv except for the substantial of the substantial except for the substantial exc$ 

Queries value:

 $\label{thm:local-substance} HKLM \system \current controls et \services \tcpip \parameters \time faces \equiv each current controls et \services \time faces \equiv except exce$ 

Queries value:

 $HKLM \ system \ \ current control set \ services \ \ tcpip \ parameters \ \ interfaces \ \ \ \{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [enable adapter domain name registration]$ 

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{e29ac6c2-7037-11de-816d-806e6f6e6963\}[registration maxaddress count]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{e29ac6c2-7037-11de-816d-806e6f6e6963\}[max number of addresses to register]$ 

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \time faces \equiv 29ac6c2-7037-11de-816d-806e6f6e6963 \cite{lem:hklmsystem} \equiv 29ac6c2-7037-11de-816d-806e6f6e6963 \cite{lem:hklmsyst$ 

 $\label{lem:problem:p$ 

Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]