Custom Information

This file was generated by fastlabel on December 14, 2024.

This summary was generated from the NIST CFReDS Data Leakage Case, using the “SANS Triage Collection” target provided with KAPE.

Summary

Target type	File count
$Boot	1
$J	1
$LogFile	1
$MFT	1
$Max	1
$SDS	1
$T	1
Application Event Log Win7+	1
Chrome Cookies	4
Chrome Current Session	2
Chrome Current Tabs	2
Chrome Extension Cookies	1
Chrome Favicons	4
Chrome History	6
Chrome Last Session	1
Chrome Last Tabs	1
Chrome Login Data	1
Chrome Network Action Predictor	2
Chrome Preferences	2
Chrome Quota Manager	2

Target type	File count
Chrome Shortcuts	4
Chrome Top Sites	4
Chrome Visited Links	2
Chrome Web Data	4
Event logs Win7+	46
Event logs Win7+	1
Event logs Win7+	1
GatherLogs	8
Google Drive Backup and Sync Metadata	6
IE 11 Metadata	12
IE 9/10 History	2
Index.dat Office	1
LNK Files	36
LNK Files from Recent	21
Local Internet Explorer folder	35
Local Service registry hive	1
Local Service registry transaction files	2
LocalSessionManager Event Logs	2
NTUSER.DAT DEFAULT registry hive	1
NTUSER.DAT DEFAULT transaction files	2
NTUSER.DAT registry hive	4
NTUSER.DAT registry transaction files	5
Network Service registry hive	1
Network Service registry transaction files	2
Prefetch	95
RecentFileCache	1
Roaming Internet Explorer folder	14

Target type	File count
SAM registry hive	1
SAM registry hive (RegBack)	1
SAM registry transaction files	2
SECURITY registry hive	1
SECURITY registry hive (RegBack)	1
SECURITY registry transaction files	2
SOFTWARE registry hive	1
SOFTWARE registry hive (RegBack)	1
SOFTWARE registry transaction files	2
SYSTEM registry hive	1
SYSTEM registry hive (RegBack)	1
SYSTEM registry transaction files	2
Setupapi.log Win7+	1
Syscache	1
Syscache transaction files	1
System Profile registry hive	1
System Profile registry transaction files	2
Thumbcache DB	13
UsrClass.dat registry hive	3
UsrClass.dat registry transaction files	3
WBEM	5
WDI Trace Logs 1	5
WDI Trace Logs 2	11
WMI Trace Logs	8
Windows Defender Event Logs	2
Windows Defender Logs	1
Windows Defender Logs	1

Target type	File count
Windows Protect Folder	6
WindowsIndexSearch	7
XML	85
at .job	2

Details

$Boot

1 files found:

- E:$Boot

$J

1 files found:

- E:$Extend$UsnJrnl:$J

$LogFile

1 files found:

- E:$LogFile

$MFT

1 files found:

- E:$MFT

$Max

1 files found:

- E:$Extend$UsnJrnl:$Max

$SDS

1 files found:

- E:$Secure:$SDS

$T

1 files found:

- E:$Extend$RmMetadata$TxfLog$Tops:$T

Application Event Log Win7+

1 files found:

- E:\Windows\System32\winevt\logs\Application.evtx

Chrome Cookies

4 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Cookies
- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Cookies
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal

Chrome Current Session

2 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Current Session
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Current Session

Chrome Current Tabs

2 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Current Tabs
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Current Tabs

Chrome Extension Cookies

1 files found:

- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies

Chrome Favicons

4 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Favicons
- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Favicons
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal

Chrome History

6 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\History
- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache
- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\History-journal
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\History
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\History-journal

Chrome Last Session

1 files found:

- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Last Session

Chrome Last Tabs

1 files found:

- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Last Tabs

Chrome Login Data

1 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Login Data

Chrome Network Action Predictor

2 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor

Chrome Preferences

2 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Preferences
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Preferences

Chrome Quota Manager

2 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\QuotaManager
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\QuotaManager

Chrome Shortcuts

4 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Shortcuts
- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Shortcuts-journal
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Shortcuts
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Shortcuts-journal

Chrome Top Sites

4 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Top Sites
- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Top Sites-journal
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Top Sites
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Top Sites-journal

Chrome Visited Links

2 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Visited Links
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Visited Links

Chrome Web Data

4 files found:

- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Web Data
- E:\Users\admin11\AppData\Local\Google\Chrome\User Data\Default\Web Data-journal
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Web Data
- E:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Web Data-journal

Event logs Win7+

46 files found:

- E:\Windows\System32\winevt\logs\HardwareEvents.evtx
- E:\Windows\System32\winevt\logs\Internet Explorer.evtx
- E:\Windows\System32\winevt\logs\Media Center.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Application-Experience%4Problem-Steps-Recorder.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Troubleshooter.evtx

- E:\Windows\System32\winevt\logs\Microsoft-Windows-Application-Experience%4Program-Inventory.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Bits-Client%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-BranchCacheSMB%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Dhcp-Client%4Admin.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Dhcpv6-Client%4Admin.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Diagnosis-DPS%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Diagnosis-Scripted%4Admin.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Diagnosis-Scripted%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Diagnostics-Performance%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-GroupPolicy%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Kernel-Power%4Thermal-Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Kernel-WHEA%4Errors.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Kernel-WHEA%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Known Folders API Service.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-LanguagePackSetup%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-MUI%4Admin.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-MUI%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-NCSI%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-NetworkAccessProtection%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-NetworkAccessProtection%4WHC.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-NetworkLocationWizard%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-NetworkProfile%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-OfflineFiles%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-PrintService%4Admin.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-ReadyBoost%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-RestartManager%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-User Profile Service%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSecurity.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-WindowsBackup%4ActionCenter.evtx

- E:\Windows\System32\winevt\logs\Microsoft-Windows-WindowsSystemAssessmentTool%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-WindowsUpdateClient%4Operational.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-Winlogon%4Operational.evtx
- E:\Windows\System32\winevt\logs\OAlerts.evtx
- E:\Windows\System32\winevt\logs\Setup.evtx
- E:\Windows\System32\winevt\logs\Windows PowerShell.evtx

Event logs Win7+

1 files found:

- E:\Windows\System32\winevt\logs\System.evtx

Event logs Win7+

1 files found:

- E:\Windows\System32\winevt\logs\Security.evtx

GatherLogs

8 files found:

- E:\programdata\microsoft\search\data\applications\windows\GatherLogs\SystemIndex\SystemIndex.1.Crwl
- E:\programdata\microsoft\search\data\applications\windows\GatherLogs\SystemIndex\SystemIndex.1.gthr
- E:\programdata\microsoft\search\data\applications\windows\GatherLogs\SystemIndex\SystemIndex.2.Crwl
- E:\programdata\microsoft\search\data\applications\windows\GatherLogs\SystemIndex\SystemIndex.2.gthr
- E:\programdata\microsoft\search\data\applications\windows\GatherLogs\SystemIndex\SystemIndex.3.Crwl
- E:\programdata\microsoft\search\data\applications\windows\GatherLogs\SystemIndex\SystemIndex.3.gthr
- E:\programdata\microsoft\search\data\applications\windows\GatherLogs\SystemIndex\SystemIndex.4.Crwl
- E:\programdata\microsoft\search\data\applications\windows\GatherLogs\SystemIndex\SystemIndex.4.gthr

Google Drive Backup and Sync Metadata

6 files found:

- E:\Users\informant\AppData\Local\Google\Drive\lockfile
- E:\Users\informant\AppData\Local\Google\Drive\user_default\com.google.drive.nativeproxy.json
- E:\Users\informant\AppData\Local\Google\Drive\user_default\pid

- E:\Users\informant\AppData\Local\Google\Drive\user_default\run_dir
- E:\Users\informant\AppData\Local\Google\Drive\user_default\sync_log.log
- E:\Users\informant\AppData\Local\Google\Drive\user_default\cloud_graph\dict_2.db

IE 11 Metadata

12 files found:

- E:\Users\admin11\AppData\Local\Microsoft\Windows\WebCache\V01.chk
- E:\Users\admin11\AppData\Local\Microsoft\Windows\WebCache\V01.log
- E:\Users\admin11\AppData\Local\Microsoft\Windows\WebCache\V01res00001.jrs
- E:\Users\admin11\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
- E:\Users\informant\AppData\Local\Microsoft\Windows\WebCache\V01.chk
- E:\Users\informant\AppData\Local\Microsoft\Windows\WebCache\V01.log
- E:\Users\informant\AppData\Local\Microsoft\Windows\WebCache\V0100024.log
- E:\Users\informant\AppData\Local\Microsoft\Windows\WebCache\V0100025.log
- E:\Users\informant\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
- E:\Users\temporary\AppData\Local\Microsoft\Windows\WebCache\V01.chk
- E:\Users\temporary\AppData\Local\Microsoft\Windows\WebCache\V01.log
- E:\Users\temporary\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

IE 9/10 History

2 files found:

- E:\Users\admin11\AppData\Local\Microsoft\Windows\History\desktop.ini
- E:\Users\informant\AppData\Local\Microsoft\Windows\History\desktop.ini

Index.dat Office

1 files found:

- E:\Users\informant\AppData\Roaming\Microsoft\Office\Recent\index.dat

LNK Files

36 files found:

- E:\Users\admin11\AppData\Roaming\Microsoft\Windows\Recent\inf.lnk

- E:\Users\admin11\AppData\Roaming\Microsoft\Windows\Recent\setupapi.dev.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent(secret_project)_pricing_decision.xlsx.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\CD Drive (2).lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\CD Drive.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\final.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\Koala.jpg.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\Penguins.jpg.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\pricing decision.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\Resignation_Letter_(Iaman_Informant).docx
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\Resignation_Letter_(Iaman_Informant).xps.l
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\secret.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\Tulips.jpg.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\winter_whether_advisory.zip.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent[secret_project]_design_concept.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent[secret_project]_final_meeting.pptx.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent[secret_project]_proposal.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Office\Recent(secret_project)_pricing_decision.xlsx.LNK
- E:\Users\informant\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK
- E:\Users\informant\AppData\Roaming\Microsoft\Office\Recent\Resignation_Letter_(Iaman_Informant).docx.LN
- E:\Users\informant\AppData\Roaming\Microsoft\Office\Recent\Templates.LNK
- E:\Users\informant\AppData\Roaming\Microsoft\Office\Recent[secret_project]_design_concept.LNK
- E:\Users\informant\AppData\Roaming\Microsoft\Office\Recent[secret_project]_final_meeting.pptx.LNK
- E:\Users\informant\AppData\Roaming\Microsoft\Office\Recent[secret_project]_proposal.LNK
- E:\Users\admin11\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer.lnk
- E:\Users\temporary\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer.lnk
- E:\Users\Public\Desktop\Google Chrome.lnk
- E:\ProgramData\Microsoft\Windows\Start Menu\Programs\Apple Software Update.lnk
- E:\ProgramData\Microsoft\Windows\Start Menu\Programs\Eraser.lnk
- E:\ProgramData\Microsoft\Windows\Start Menu\Programs\Media Center.lnk
- E:\ProgramData\Microsoft\Windows\Start Menu\Programs\Sidebar.lnk
- E:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows DVD Maker.lnk
- E:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows Fax and Scan.lnk
- E:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows Media Player.lnk
- E:\ProgramData\Microsoft\Windows\Start Menu\Programs\XPS Viewer.lnk

LNK Files from Recent

21 files found:

- E:\Users\admin11\AppData\Roaming\Microsoft\Windows\Recent\desktop.ini
- E:\Users\admin11\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.au
  ms
- E:\Users\admin11\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b9cdc69c1c24e2b.au
  ms
- E:\Users\admin11\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1b4dd67f29cb1962.custo
  ms
- E:\Users\admin11\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5afe4de1b92fc382.custom
  ms
- E:\Users\admin11\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5d696d521de238c3.custo
  ms
- E:\Users\admin11\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7e4dca80246863e3.custo
  ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.a
  ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\47bb2136fda3f1ed.au
  ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\4cc9bcff1a772a63.au
  ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\69bacc0499d41c4.au
  ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\7e4dca80246863e3.a
  ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\e36bfc8972e5ab1d.au
  ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\28c8b86deab549a1.cust
  ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\337ed59af273c758.custo
  ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5afe4de1b92fc382.custo
  ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5d696d521de238c3.cust
  ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6d2bac8f1edf6668.custo

ms
- E:\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ccc0fa1b9f86f7b3.custo
ms
- E:\Users\temporary\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.a
ms
- E:\Users\temporary\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\7e4dca80246863e3.a
ms

Local Internet Explorer folder

35 files found:

- E:\Users\admin11\AppData\Local\Microsoft\Internet Explorer\brndlog.txt
- E:\Users\admin11\AppData\Local\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml
- E:\Users\admin11\AppData\Local\Microsoft\Internet Explorer\Tiles\pin9728060290\msapplication.xml
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\brndlog.bak
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\brndlog.txt
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\frameiconcache.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions\en-US.1
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\VersionManager\versionlist.xml
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\DOMStore\AB94QIIA\drive.google[1].xml
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\imagestore\m1pfyb8\imagestore.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active\RecoveryStore.{5BEC2B2D-D0A5-11E4-B985-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active\RecoveryStore.{AA15C628-D2FD-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{03C17667-D2FE-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{22546D87-D2FE-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{5BEC2B2E-D0A5-11E4-B985-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{62B37659-D0A5-11E4-B985-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{7BFFEA36-D0A5-11E4-B985-000C29FF2429}.dat

- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{7BFFEA53-D0A5-11E4-B985-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{A68678CE-D0A5-11E4-B985-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{AA15C62A-D2FD-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{AA15C62B-D2FD-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{AA15C62C-D2FD-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{C479407F-D2FD-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{C4794080-D2FD-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{D10B9AEF-D2FD-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{E34CBB3F-D2FD-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{E34CBB40-D2FD-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Active{F8BC20AF-D2FD-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{22546D88-D2FE-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active{B24921CB-D302-11E4-B734-000C29FF2429}.dat
- E:\Users\informant\AppData\Local\Microsoft\Internet Explorer\Tiles\pin9728060290\msapplication.xml
- E:\Users\temporary\AppData\Local\Microsoft\Internet Explorer\brndlog.txt
- E:\Users\temporary\AppData\Local\Microsoft\Internet Explorer\Tiles\pin9728060290\msapplication.xml

Local Service registry hive

1 files found:

- E:\Windows\ServiceProfiles\LocalService\NTUSER.DAT

Local Service registry transaction files

2 files found:

- E:\Windows\ServiceProfiles\LocalService\NTUSER.DAT.LOG
- E:\Windows\ServiceProfiles\LocalService\NTUSER.DAT.LOG1

LocalSessionManager Event Logs

2 files found:

- E:\Windows\System32\winevt\logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx
- E:\Windows\System32\winevt\logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.e

NTUSER.DAT DEFAULT registry hive

1 files found:

- E:\Windows\System32\config\DEFAULT

NTUSER.DAT DEFAULT transaction files

2 files found:

- E:\Windows\System32\config\DEFAULT.LOG
- E:\Windows\System32\config\DEFAULT.LOG1

NTUSER.DAT registry hive

4 files found:

- E:\Users\admin11\NTUSER.DAT
- E:\Users\Default\NTUSER.DAT
- E:\Users\informant\NTUSER.DAT
- E:\Users\temporary\NTUSER.DAT

NTUSER.DAT registry transaction files

5 files found:

- E:\Users\admin11\ntuser.dat.LOG1
- E:\Users\Default\NTUSER.DAT.LOG
- E:\Users\Default\NTUSER.DAT.LOG1
- E:\Users\informant\ntuser.dat.LOG1
- E:\Users\temporary\ntuser.dat.LOG1

Network Service registry hive

1 files found:

- E:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT

Network Service registry transaction files

2 files found:

- E:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT.LOG
- E:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT.LOG1

Prefetch

95 files found:

- E:\Windows\prefetch\ASPNET_REGIIS.EXE-75651A3C.pf
- E:\Windows\prefetch\ASPNET_REGIIS.EXE-86915B5A.pf
- E:\Windows\prefetch\AUDIODG.EXE-BDFD3029.pf
- E:\Windows\prefetch\AU_.EXE-506726E7.pf
- E:\Windows\prefetch\BFSVC.EXE-9C7A4DEE.pf
- E:\Windows\prefetch\CCLEANER64.EXE-779BD542.pf
- E:\Windows\prefetch\CCSETUP504.EXE-6BA2F6A1.pf
- E:\Windows\prefetch\CHROME.EXE-D999B1BA.pf
- E:\Windows\prefetch\CLRGC.EXE-5D5B90F5.pf
- E:\Windows\prefetch\CONHOST.EXE-1F3E9D7E.pf
- E:\Windows\prefetch\CONSENT.EXE-531BD9EA.pf
- E:\Windows\prefetch\CONTROL.EXE-817F8F1D.pf

- E:\Windows\prefetch\DEVICEDISPLAYOBJECTPROVIDER.E-17410B90.pf
- E:\Windows\prefetch\DLLHOST.EXE-4F28A26F.pf
- E:\Windows\prefetch\DLLHOST.EXE-5E46FA0D.pf
- E:\Windows\prefetch\DLLHOST.EXE-766398D2.pf
- E:\Windows\prefetch\DLLHOST.EXE-7FAA2E4C.pf
- E:\Windows\prefetch\DLLHOST.EXE-A8DE6D5B.pf
- E:\Windows\prefetch\DLLHOST.EXE-C373C89E.pf
- E:\Windows\prefetch\DLLHOST.EXE-E129DEF0.pf
- E:\Windows\prefetch\DLLHOST.EXE-ECB71776.pf
- E:\Windows\prefetch\DOTNETFX40_FULL_SETUP.EXE-5EFD2BFF.pf
- E:\Windows\prefetch\DRVINST.EXE-4CB4314A.pf
- E:\Windows\prefetch\ERASER 6.2.0.2962.EXE-BE552234.pf
- E:\Windows\prefetch\ERASER.EXE-CE61944A.pf
- E:\Windows\prefetch\GOOGLEDRIVESYNC.EXE-841A0D94.pf
- E:\Windows\prefetch\GOOGLEUPDATE.EXE-B95715F5.pf
- E:\Windows\prefetch\IEXPLORE.EXE-4B6C9213.pf
- E:\Windows\prefetch\IEXPLORE.EXE-908C99F8.pf
- E:\Windows\prefetch\LODCTR.EXE-3CCE0534.pf
- E:\Windows\prefetch\LODCTR.EXE-72CD50D0.pf
- E:\Windows\prefetch\LOGONUI.EXE-09140401.pf
- E:\Windows\prefetch\MCBUILDER.EXE-7F26B913.pf
- E:\Windows\prefetch\MOBSYNC.EXE-C5E2284F.pf
- E:\Windows\prefetch\MOFCOMP.EXE-8FE3D558.pf
- E:\Windows\prefetch\MOFCOMP.EXE-FDE76EFC.pf
- E:\Windows\prefetch\MSCORSVW.EXE-245ED79E.pf
- E:\Windows\prefetch\MSCORSVW.EXE-57D17DAF.pf
- E:\Windows\prefetch\MSCORSVW.EXE-90526FAC.pf
- E:\Windows\prefetch\MSCORSVW.EXE-C3C515BD.pf
- E:\Windows\prefetch\MSIEXEC.EXE-A2D55CB6.pf
- E:\Windows\prefetch\MSIEXEC.EXE-E09A077A.pf
- E:\Windows\prefetch\MSOSYNC.EXE-6051F98A.pf
- E:\Windows\prefetch\NETSH.EXE-F1B6DA12.pf
- E:\Windows\prefetch\NGEN.EXE-AE594A6B.pf
- E:\Windows\prefetch\NGEN.EXE-EC3F9239.pf
- E:\Windows\prefetch\NTOSBOOT-B00DFAAD.pf
- E:\Windows\prefetch\OSPPSVC.EXE-E53D3CC0.pf
- E:\Windows\prefetch\OUTLOOK.EXE-1DF422BF.pf
- E:\Windows\prefetch\PING.EXE-371F41E2.pf

- E:\Windows\prefetch\REGTLIBV12.EXE-B7C4F383.pf
- E:\Windows\prefetch\REGTLIBV12.EXE-D3A27E55.pf
- E:\Windows\prefetch\RUNDLL32.EXE-411A328D.pf
- E:\Windows\prefetch\RUNDLL32.EXE-89545801.pf
- E:\Windows\prefetch\RUNDLL32.EXE-AF74762C.pf
- E:\Windows\prefetch\RUNDLL32.EXE-FE9FC6E1.pf
- E:\Windows\prefetch\SC.EXE-945D79AE.pf
- E:\Windows\prefetch\SCHTASKS.EXE-AD598958.pf
- E:\Windows\prefetch\SEARCHFILTERHOST.EXE-77482212.pf
- E:\Windows\prefetch\SEARCHINDEXER.EXE-4A6353B9.pf
- E:\Windows\prefetch\SEARCHPROTOCOLHOST.EXE-0CB8CADE.pf
- E:\Windows\prefetch\SERVICEMODELREG.EXE-1F42B3E3.pf
- E:\Windows\prefetch\SERVICEMODELREG.EXE-AFDDD121.pf
- E:\Windows\prefetch\SETUP.EXE-9FA85C1C.pf
- E:\Windows\prefetch\SETUPUTILITY.EXE-3393AB00.pf
- E:\Windows\prefetch\SETUP_WM.EXE-D33FD27D.pf
- E:\Windows\prefetch\SOLITAIRE.EXE-906D7E29.pf
- E:\Windows\prefetch\SPPSVC.EXE-B0F8131B.pf
- E:\Windows\prefetch\STIKYNOT.EXE-AD181651.pf
- E:\Windows\prefetch\SVCHOST.EXE-007FEA55.pf
- E:\Windows\prefetch\SVCHOST.EXE-05F624AB.pf
- E:\Windows\prefetch\SVCHOST.EXE-7AC6742A.pf
- E:\Windows\prefetch\SVCHOST.EXE-7CFEDEA3.pf
- E:\Windows\prefetch\SVCHOST.EXE-80F4A784.pf
- E:\Windows\prefetch\TASKENG.EXE-48D4E289.pf
- E:\Windows\prefetch\TASKHOST.EXE-7238F31D.pf
- E:\Windows\prefetch\TMP5B99.TMP.EXE-6E86E5DD.pf
- E:\Windows\prefetch\TMPFF8D.TMP.EXE-E479EE08.pf
- E:\Windows\prefetch\TRUSTEDINSTALLER.EXE-3CC531E5.pf
- E:\Windows\prefetch\UNINST.EXE-0867DC84.pf
- E:\Windows\prefetch\UNLODCTR.EXE-531FACC7.pf
- E:\Windows\prefetch\UNLODCTR.EXE-A3D4DEEB.pf
- E:\Windows\prefetch\VSSVC.EXE-B8AFC319.pf
- E:\Windows\prefetch\WERMGR.EXE-0F2AC88C.pf
- E:\Windows\prefetch\WEVTUTIL.EXE-400D93E8.pf
- E:\Windows\prefetch\WEVTUTIL.EXE-EF5861C4.pf
- E:\Windows\prefetch\WINWORD.EXE-CECBA770.pf
- E:\Windows\prefetch\WMIADAP.EXE-F8DFDFA2.pf

- E:\Windows\prefetch\WMIPRVSE.EXE-1628051C.pf
- E:\Windows\prefetch\WMPLAYER.EXE-26C72A86.pf
- E:\Windows\prefetch\WMPNSCFG.EXE-FC0D39BF.pf
- E:\Windows\prefetch\WSQMCONS.EXE-118B52B7.pf
- E:\Windows\prefetch\WUAUCLT.EXE-70318591.pf
- E:\Windows\prefetch\WUSA.EXE-A8D5906C.pf
- E:\Windows\prefetch\XPSRCHVW.EXE-FEB3BF01.pf

RecentFileCache

1 files found:

- E:\Windows\AppCompat\Programs\RecentFileCache.bcf

Roaming Internet Explorer folder

14 files found:

- E:\Users\admin11\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
- E:\Users\admin11\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Google Chrome.lnk
- E:\Users\admin11\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk
- E:\Users\admin11\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk
- E:\Users\admin11\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\desktop.ini
- E:\Users\admin11\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Google Chrome.lnk
- E:\Users\admin11\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Explorer.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
- E:\Users\informant\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Google Chrome.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
- E:\Users\informant\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Microsoft Outlook.lnk

- E:\Users\informant\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\desktop.ini
- E:\Users\informant\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explorer.lnk
- E:\Users\temporary\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Google Chrome.lnk

SAM registry hive

1 files found:

- E:\Windows\System32\config\SAM

SAM registry hive (RegBack)

1 files found:

- E:\Windows\System32\config\RegBack\SAM

SAM registry transaction files

2 files found:

- E:\Windows\System32\config\SAM.LOG
- E:\Windows\System32\config\SAM.LOG1

SECURITY registry hive

1 files found:

- E:\Windows\System32\config\SECURITY

SECURITY registry hive (RegBack)

1 files found:

- E:\Windows\System32\config\RegBack\SECURITY

SECURITY registry transaction files

2 files found:

- E:\Windows\System32\config\SECURITY.LOG
- E:\Windows\System32\config\SECURITY.LOG1

SOFTWARE registry hive

1 files found:

- E:\Windows\System32\config\SOFTWARE

SOFTWARE registry hive (RegBack)

1 files found:

- E:\Windows\System32\config\RegBack\SOFTWARE

SOFTWARE registry transaction files

2 files found:

- E:\Windows\System32\config\SOFTWARE.LOG
- E:\Windows\System32\config\SOFTWARE.LOG1

SYSTEM registry hive

1 files found:

- E:\Windows\System32\config\SYSTEM

SYSTEM registry hive (RegBack)

1 files found:

- E:\Windows\System32\config\RegBack\SYSTEM

SYSTEM registry transaction files

2 files found:

- E:\Windows\System32\config\SYSTEM.LOG
- E:\Windows\System32\config\SYSTEM.LOG1

Setupapi.log Win7+

1 files found:

- E:\Windows\inf\setupapi.dev.log

Syscache

1 files found:

- E:\System Volume Information\Syscache.hve

Syscache transaction files

1 files found:

- E:\System Volume Information\Syscache.hve.LOG1

System Profile registry hive

1 files found:

- E:\Windows\System32\config\systemprofile\ntuser.dat

System Profile registry transaction files

2 files found:

- E:\Windows\System32\config\systemprofile\ntuser.dat.LOG
- E:\Windows\System32\config\systemprofile\ntuser.dat.LOG1

Thumbcache DB

13 files found:

- E:\Users\admin11\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1024.db
- E:\Users\admin11\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
- E:\Users\admin11\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db
- E:\Users\admin11\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db
- E:\Users\admin11\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db
- E:\Users\admin11\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db
- E:\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
- E:\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db
- E:\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db
- E:\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db
- E:\Users\temporary\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
- E:\Users\temporary\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db
- E:\Users\temporary\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db

UsrClass.dat registry hive

3 files found:

- E:\Users\admin11\AppData\Local\Microsoft\Windows\UsrClass.dat
- E:\Users\informant\AppData\Local\Microsoft\Windows\UsrClass.dat
- E:\Users\temporary\AppData\Local\Microsoft\Windows\UsrClass.dat

UsrClass.dat registry transaction files

3 files found:

- E:\Users\admin11\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
- E:\Users\informant\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
- E:\Users\temporary\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1

WBEM

5 files found:

- E:\Windows\System32\wbem\Repository\INDEX.BTR

- E:\Windows\System32\wbem\Repository\MAPPING1.MAP
- E:\Windows\System32\wbem\Repository\MAPPING2.MAP
- E:\Windows\System32\wbem\Repository\MAPPING3.MAP
- E:\Windows\System32\wbem\Repository\OBJECTS.DATA

WDI Trace Logs 1

5 files found:

- E:\Windows\System32\WDI\LogFiles\BootCKCL.etl
- E:\Windows\System32\WDI\LogFiles\ShutdownCKCL.etl
- E:\Windows\System32\WDI\LogFiles\WdiContextLog.etl.001
- E:\Windows\System32\WDI\LogFiles\WdiContextLog.etl.002
- E:\Windows\System32\WDI\LogFiles\WdiContextLog.etl.003

WDI Trace Logs 2

11 files found:

- E:\Windows\System32\WDI{67144949-5132-4859-8036-a737b43825d8}{9a3d7e9e-7fc6-43a4-a74e-8d50303fcdae}\snapshot.etl
- E:\Windows\System32\WDI{67144949-5132-4859-8036-a737b43825d8}{ac1aa789-a259-4e50-be32-58447f92b714}\snapshot.etl
- E:\Windows\System32\WDI{86432a0b-3c7d-4ddf-a89c-172faa90485d}\S-1-5-21-2425377081-3129163575-2985601102-1000_UserData.bin
- E:\Windows\System32\WDI{86432a0b-3c7d-4ddf-a89c-172faa90485d}\S-1-5-21-3111613574-2524581245-2586426736-500_UserData.bin
- E:\Windows\System32\WDI{86432a0b-3c7d-4ddf-a89c-172faa90485d}{2c5f5048-4e9b-487e-b245-7e0e9b604606}\snapshot.etl
- E:\Windows\System32\WDI{86432a0b-3c7d-4ddf-a89c-172faa90485d}{336c8a0e-f419-4df4-b3fe-52de057e5cae}\snapshot.etl
- E:\Windows\System32\WDI{86432a0b-3c7d-4ddf-a89c-172faa90485d}{3aaf5c18-c3df-412f-921f-a7c03ea7e145}\snapshot.etl
- E:\Windows\System32\WDI{86432a0b-3c7d-4ddf-a89c-172faa90485d}{8c8a5498-1428-4a4f-9a52-aa2105754f70}\snapshot.etl
- E:\Windows\System32\WDI{86432a0b-3c7d-4ddf-a89c-172faa90485d}{9e840662-7805-40ea-abbc-2666b58e80f3}\snapshot.etl
- E:\Windows\System32\WDI{86432a0b-3c7d-4ddf-a89c-172faa90485d}{d3f5594e-34ec-4579-b2ed-9b3aa4a561f9}\snapshot.etl

- E:\Windows\System32\WDI{86432a0b-3c7d-4ddf-a89c-172faa90485d}{dc425e1a-3399-4a2e-9a96-e67a64c9ffd2}\snapshot.etl

WMI Trace Logs

8 files found:

- E:\Windows\System32\LogFiles\WMI\Terminal-Services-Core.etl
- E:\Windows\System32\LogFiles\WMI\Terminal-Services-IP-Virtualization.etl
- E:\Windows\System32\LogFiles\WMI\Terminal-Services-RPC-Client.etl
- E:\Windows\System32\LogFiles\WMI\Terminal-Services-SessionEnv.etl
- E:\Windows\System32\LogFiles\WMI\Terminal-Services-Unified-APIs.etl
- E:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTDiagLog.etl
- E:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTEventLog-Application.etl
- E:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTEventLog-System.etl

Windows Defender Event Logs

2 files found:

- E:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4Operational.evtx
- E:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4WHC.evtx

Windows Defender Logs

1 files found:

- E:\ProgramData\Microsoft\Windows Defender\Support\MPLog-07132009-221054.log

Windows Defender Logs

1 files found:

- E:\Windows\Temp\MpCmdRun.log

Windows Protect Folder

6 files found:

- E:\Users\admin11\AppData\Roaming\Microsoft\Protect\S-1-5-21-2425377081-3129163575-2985601102-1001\38e42213-4f50-4230-aebe-bfbdefeba478
- E:\Users\admin11\AppData\Roaming\Microsoft\Protect\S-1-5-21-2425377081-3129163575-2985601102-1001\Preferred
- E:\Users\informant\AppData\Roaming\Microsoft\Protect\S-1-5-21-2425377081-3129163575-2985601102-1000\daf02181-b35a-4965-bf54-90704762f8bb
- E:\Users\informant\AppData\Roaming\Microsoft\Protect\S-1-5-21-2425377081-3129163575-2985601102-1000\Preferred
- E:\Users\temporary\AppData\Roaming\Microsoft\Protect\S-1-5-21-2425377081-3129163575-2985601102-1003\f06b6be8-1d9a-4955-86c3-5bf9b13948ed
- E:\Users\temporary\AppData\Roaming\Microsoft\Protect\S-1-5-21-2425377081-3129163575-2985601102-1003\Preferred

WindowsIndexSearch

7 files found:

- E:\programdata\microsoft\search\data\applications\windows\MSS.chk
- E:\programdata\microsoft\search\data\applications\windows\MSS.log
- E:\programdata\microsoft\search\data\applications\windows\MSS0000B.log
- E:\programdata\microsoft\search\data\applications\windows\MSS0000C.log
- E:\programdata\microsoft\search\data\applications\windows\MSS0000D.log
- E:\programdata\microsoft\search\data\applications\windows\MSSres00001.jrs
- E:\programdata\microsoft\search\data\applications\windows\Windows.edb

XML

85 files found:

- E:\Windows\System32\Tasks\GoogleUpdateTaskMachineCore
- E:\Windows\System32\Tasks\GoogleUpdateTaskMachineUA
- E:\Windows\System32\Tasks\Microsoft Office 15 Sync Maintenance for informant-PC-informant informant-PC
- E:\Windows\System32\Tasks\OfficeSoftwareProtectionPlatform\SvcRestartTask
- E:\Windows\System32\Tasks\Microsoft\Office\Office 15 Subscription Heartbeat
- E:\Windows\System32\Tasks\Microsoft\Office\OfficeTelemetryAgentFallBack
- E:\Windows\System32\Tasks\Microsoft\Office\OfficeTelemetryAgentLogOn
- E:\Windows\System32\Tasks\Microsoft\Windows Defender\MP Scheduled Scan

- E:\Windows\System32\Tasks\Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS Rights Policy Template Management (Automated)
- E:\Windows\System32\Tasks\Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS Rights Policy Template Management (Manual)
- E:\Windows\System32\Tasks\Microsoft\Windows\AppID\PolicyConverter
- E:\Windows\System32\Tasks\Microsoft\Windows\AppID\VerifiedPublisherCertStoreCheck
- E:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\AitAgent
- E:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramDataUpdater
- E:\Windows\System32\Tasks\Microsoft\Windows\Autochk\Proxy
- E:\Windows\System32\Tasks\Microsoft\Windows\Bluetooth\UninstallDeviceTask
- E:\Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient\SystemTask
- E:\Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient\UserTask
- E:\Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient\UserTask-Roam
- E:\Windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program\Consolidator
- E:\Windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program\KernelCeipTask
- E:\Windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program\UsbCeip
- E:\Windows\System32\Tasks\Microsoft\Windows\Defrag\ScheduledDefrag
- E:\Windows\System32\Tasks\Microsoft\Windows\Diagnosis\Scheduled
- E:\Windows\System32\Tasks\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector
- E:\Windows\System32\Tasks\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver
- E:\Windows\System32\Tasks\Microsoft\Windows\Location\Notifications
- E:\Windows\System32\Tasks\Microsoft\Windows\Maintenance\WinSAT
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\ActivateWindowsSearch
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\ConfigureInternetTimeService
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\DispatchRecoveryTasks
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\ehDRMInit
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\InstallPlayReady
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\mcupdate
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\MediaCenterRecoveryTask
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\ObjectStoreRecoveryTask
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\OCURActivate
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\OCURDiscovery
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\PBDADiscovery

- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\PBDADiscoveryW1
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\PBDADiscoveryW2
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\PeriodicScanRetry
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\PvrRecoveryTask
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\PvrScheduleTask
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\RecordingRestart
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\RegisterSearch
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\ReindexSearchRoot
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\SqlLiteRecoveryTask
- E:\Windows\System32\Tasks\Microsoft\Windows\Media Center\UpdateRecordPath
- E:\Windows\System32\Tasks\Microsoft\Windows\MemoryDiagnostic\CorruptionDetector
- E:\Windows\System32\Tasks\Microsoft\Windows\MemoryDiagnostic\DecompressionFailureDetector
- E:\Windows\System32\Tasks\Microsoft\Windows\MobilePC\HotStart
- E:\Windows\System32\Tasks\Microsoft\Windows\MUI\LPRemove
- E:\Windows\System32\Tasks\Microsoft\Windows\Multimedia\SystemSoundsService
- E:\Windows\System32\Tasks\Microsoft\Windows\NetTrace\GatherNetworkInfo
- E:\Windows\System32\Tasks\Microsoft\Windows\Offline Files\Background Synchronization
- E:\Windows\System32\Tasks\Microsoft\Windows\Offline Files\Logon Synchronization
- E:\Windows\System32\Tasks\Microsoft\Windows\PerfTrack\BackgroundConfigSurveyor
- E:\Windows\System32\Tasks\Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem
- E:\Windows\System32\Tasks\Microsoft\Windows\RAC\RacTask
- E:\Windows\System32\Tasks\Microsoft\Windows\Ras\MobilityManager
- E:\Windows\System32\Tasks\Microsoft\Windows\Registry\RegIdleBackup
- E:\Windows\System32\Tasks\Microsoft\Windows\RemoteAssistance\RemoteAssistanceTask
- E:\Windows\System32\Tasks\Microsoft\Windows\Shell\WindowsParentalControls
- E:\Windows\System32\Tasks\Microsoft\Windows\Shell\WindowsParentalControlsMigration
- E:\Windows\System32\Tasks\Microsoft\Windows\SideShow\AutoWake
- E:\Windows\System32\Tasks\Microsoft\Windows\SideShow\GadgetManager
- E:\Windows\System32\Tasks\Microsoft\Windows\SideShow\SessionAgent
- E:\Windows\System32\Tasks\Microsoft\Windows\SideShow\SystemDataProviders
- E:\Windows\System32\Tasks\Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTask
- E:\Windows\System32\Tasks\Microsoft\Windows\SystemRestore\SR
- E:\Windows\System32\Tasks\Microsoft\Windows\Task Manager\Interactive
- E:\Windows\System32\Tasks\Microsoft\Windows\Tcpip\IpAddressConflict1
- E:\Windows\System32\Tasks\Microsoft\Windows\Tcpip\IpAddressConflict2
- E:\Windows\System32\Tasks\Microsoft\Windows\TextServicesFramework\MsCtfMonitor
- E:\Windows\System32\Tasks\Microsoft\Windows\Time Synchronization\SynchronizeTime
- E:\Windows\System32\Tasks\Microsoft\Windows\UPnP\UPnPHostConfig

- E:\Windows\System32\Tasks\Microsoft\Windows\User Profile Service\HiveUploadTask
- E:\Windows\System32\Tasks\Microsoft\Windows\WDI\ResolutionHost
- E:\Windows\System32\Tasks\Microsoft\Windows\Windows Error Reporting\QueueReporting
- E:\Windows\System32\Tasks\Microsoft\Windows\Windows Filtering Platform\BfeOnServiceStartTypeChange
- E:\Windows\System32\Tasks\Microsoft\Windows\Windows Media Sharing\UpdateLibrary
- E:\Windows\System32\Tasks\Microsoft\Windows\WindowsBackup\ConfigNotification
- E:\Windows\System32\Tasks\Microsoft\Windows\WindowsColorSystem\Calibration Loader
- E:\Windows\System32\Tasks\Microsoft\Windows\Wininet\CacheTask

at .job

2 files found:

- E:\Windows\Tasks\GoogleUpdateTaskMachineCore.job
- E:\Windows\Tasks\GoogleUpdateTaskMachineUA.job