Chrome Common artifact collection path

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Bookmarks*

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Cookies*

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Current Session

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Current Tabs

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Favicons*

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\History*

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Last Session

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\Usey

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\Usea\Default\Preferences

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Shortcuts*

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Top Sites*

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Bookmarks*

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Visited Links

Chrome: Path: C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Web Data*

Event Logs Common artifact collection path

EventLogs: Path: C:\Windows\system32\config\\ *. evt

EventLogs: Path: C:\Windows\system32\winevt\logs\\ *. Evtx

Event Trace Logs Common artifact collection path

EventTraceLogs: Path: C:\Windows\System32\WDI\LogFiles\\ *. etl*

EventTraceLogs: Path: C:\Windows\System32\WDI*

EventTraceLogs: Path: C:\Windows\System32\LogFiles\WMI*

EventTraceLogs: Path: C:\Windows\System32\SleepStudy*

EventTraceLogs: Path: C:\ProgramData\Microsoft\Windows\PowerEfficiency Diagnostics\energy-ntkl.etl

Evidence of execution Common artifact collection path

EvidenceOfExecution: Path: C:\Windows\prefetch

EvidenceOfExecution: Path: C:\Windows\AppCompat\Programs\RecentFileCache.bcf

EvidenceOfExecution: Path: C:\Windows\AppCompat\Programs\Amcache.hve

EvidenceOfExecution: Path: C:\Windows\AppCompat\Programs\Amcache.hve.LOG*

File System Common artifact collection path

FileSystem: Path: C:\\$MFT

FileSystem: Path: C:\\$LogFile

FileSystem: Path: c:\\$Extend\\$UsnJrnl:\$J

Firefox Common artifact collection path

FireFox: Path: C:\Users*\AppData\Roaming\Mozilla\Firefox\Profiles\\ *. default\places.sqlite*

FireFox: Path: C:\Users*\AppData\Roaming\Mozilla\Firefox\Profiles\\ *. default\downloads.sqlite*

FireFox: Path: C:\Users*\AppData\Roaming\Mozilla\Firefox\Profiles\\ *. default\formhistory.sqlite*

FireFox: Path: C:\Users*\AppData\Roaming\Mozilla\Firefox\Profiles\\ *. default\cookies.sqlite*

FireFox: Path: C:\Users*\AppData\Roaming\Mozilla\Firefox\Profiles\\ *. default\signons.sqlite*

FireFox: Path: C:\Users*\AppData\Roaming\Mozilla\Firefox\Profiles\\ *. default\webappstore.sqlite*

FireFox: Path: C:\Users*\AppData\Roaming\Mozilla\Firefox\Profiles\\ *. default\favicons.sqlite*

FireFox: Path: C:\Users*\AppData\Roaming\Mozilla\Firefox\Profiles\\ *. default\addons.sqlite*

FireFox: Path: C:\Users*\AppData\Roaming\Mozilla\Firefox\Profiles\\ *. default\search.sqlite*

Internet explorer Common artifact collection path

InternetExplorer: Path: C:\Users*\AppData\Roaming\Microsoft\Office\Recent\index.dat

InternetExplorer: Path: C:\Users*\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

InternetExplorer: Path: C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Internet Explorer\Recovery

InternetExplorer: Path: C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\History\

InternetExplorer: Path: C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\Windows\Cookies\

InternetExplorer: Path:C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\Windows\Web Cache\

InternetExplorer: Path: C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\

InternetExplorer: Path: C:\Users\

*\AppData\Local\Packages\Microsoft.MicrosoftEdge_*\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\120712-049\DBStore

InternetExplorer: Path: C:\Users*\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup*\DatastoreBackup\spartan.edb

Live user files Common artifact collection path

LiveUserFiles: Path: C:\Users*\Desktop*

LiveUserFiles: Path: C:\Users*\Documents*

LiveUserFiles: Path: C:\Users*\Downloads*

LiveUserFiles: Path: C:\Users*\Dropbox**

Lnk and Jumplists Common artifact collection path

LnkFilesAndJumpLists: Path: C:\Users*\AppData\Roaming\Microsoft\Windows\Recent

LnkFilesAndJumpLists: Path: C:\Documents and Settings*\Recent

LnkFilesAndJumpLists: Path: C:\Documents and Settings*\Desktop\\ *. lnk

LnkFilesAndJumpLists: Path: C:\Users*\Desktop\\ *. lnk

LnkFilesAndJumpLists: Path: C:\Users*\AppData\Local\ConnectedDevicesPlatform*\\ *. db

Memory Common artifact collection path

MemoryArtifacts: Path: C:\hiberfil.sys

MemoryArtifacts: Path: C:\pagefile.sys

MemoryArtifacts: Path: C:\swapfile.sys

MemoryArtifacts: Path: C:\Windows\memory.dmp

Outlook Common artifact collection path

OutlookPSTOST: Path: C:\Documents and Settings*\Local Settings\Application Data\Microsoft\Outlook\\ *. pst

OutlookPSTOST: Path: C:\Documents and Settings*\Local Settings\Application Data\Microsoft\Outlook\\ *. ost

OutlookPSTOST: Path: C:\Users*\AppData\Local\Microsoft\Outlook\\ *. pst

OutlookPSTOST: Path: C:\Users*\AppData\Local\Microsoft\Outlook\\ *. Ost

Recycle Bin Common artifact collection path

Recycle: Path: C:\\$Recycle.Bin*

Recycle: Path: C:\RECYCLER*

Registry Hives Common artifact collection path

RegistryHives: Path: C:\Documents and Settings*\ntuser.dat

RegistryHives: Path: C:\Users*\ntuser.dat

RegistryHives: Path: C:\Users*\ntuser.dat.LOG*

RegistryHives: Path: C:\Users*\AppData\Local\Microsoft\Windows\UsrClass.dat

RegistryHives: Path: C:\Users*\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG*

RegistryHives: Path: C:\Windows\System32\config\SAM.LOG*

RegistryHives: Path: C:\Windows\System32\config\SECURITY.LOG*

RegistryHives: Path: C:\Windows\System32\config\SOFTWARE.LOG*

RegistryHives: Path: C:\Windows\System32\config\SYSTEM.LOG*

RegistryHives: Path: C:\Windows\System32\config\SAM

RegistryHives: Path: C:\Windows\System32\config\SECURITY

RegistryHives: Path: C:\Windows\System32\config\SOFTWARE

RegistryHives: Path: C:\Windows\System32\config\SYSTEM

RegistryHives: Path: C:\Windows\System32\config\RegBack\\ *. LOG*

RegistryHives: Path: C:\Windows\System32\config\RegBack\SAM

RegistryHives: Path: C:\Windows\System32\config\RegBack\SECURITY

RegistryHives: Path: C:\Windows\System32\config\RegBack\SOFTWARE

RegistryHives: Path: C:\Windows\System32\config\RegBack\SYSTEM

RegistryHives: Path: C:\Windows\System32\config\RegBack\SYSTEM1

Scheduled Tasks Common artifact collection path

ScheduledTasks: Path: C:\Windows\Tasks\\ *. job

ScheduledTasks: Path: C:\Windows\SchedLgU.txt

ScheduledTasks: Path: C:\Windows\system32\Tasks

Skype Common artifact collection path

Skype: Path: C:\Users*\AppData\Local\Packages\Microsoft.SkypeApp_*\LocalState*\main.db

Skype: Path: C:\Documents and Settings*\Application Data\Skype*\main.db

SRUM Common artifact collection path

SRUM: Path: C:\Windows\System32\SRU

Thumb Cache Common artifact collection path

ThumbCache: Path: C:\Users*\AppData\Local\Microsoft\Windows\Explorer\thumbcache_\ *. db

USB Common artifact collection path

USBDevicesLogs: Path: C:\Windows\setupapi.log

USBDevicesLogs: Path: C:\Windows\inf\setupapi.dev.log

WBEM Common artifact collection path

WBEM: Path: C:\Windows\System32\wbem\Repository*

Webbrowsers Common artifact collection path

WebBrowsers: Path: InternetExplorer

WebBrowsers: Path: Chrome

WebBrowsers: Path: FireFox

Index Searches Common artifact collection path

WlindowsIndexSearch: Path: C:\programdata\microsoft\search\data\applications\windows\Windows.edb