

Appendix 1 - Windows 10 Artifact Locations

Camera App		
Photos stored at		C:\Users\ <username>\Pictures\Camera Roll</username>
File Format		WIN_20151106_10_48_48_Pro.jpg - WIN / Date in YMD / Time HH_MM_SS / Pro.jpg
Shared photos	track to user at	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharingMFU
Registry	RecentDocs for .jpg at:	NTUSER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg
Registry	RecentDocs for .jpg at:	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg&ls=0&b=0

Cortana		
Contacts	contacts.json file	C:\Users\ <username>\AppData\Local\Packages\<cortana>\LocalState\Cortana\Upload\</cortana></username>
CortanaCoreDB.dat	Main page tracking	C:\Users\ <username>\AppData\Local\Packages\<cortana>\LocalState\ESEDatabase_CortanaCoreInstance</cortana></username>
IndexedDB.edb	Indexed search data	C:\Users\ <username>\AppData\Local\Packages\<cortana>\AppData\Indexed DB\IndexedDB.edb</cortana></username>
Local Speech	Saved WAV files	C:\Users\ <username>\AppData\Local\Packages\<cortana>\LocalState\LocalRecorder\Speech</cortana></username>
Main Cache	Main page storage	C:\Users\ <username>\AppData\Local\Packages\<cortana>\AC\AppCache\<#></cortana></username>
Searches	DestList (Jump Lists)	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9d1f905ce5044aee.automaticDestinations-ms</username>
Searches	.JSON Files	C:\Users\ <username>\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\IndexCache\<folder#></username>
Searches	Jump Lists	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9d1f905ce5044aee.automaticDestinations-ms</username>
Searches	Link Files	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent\https<bing-keyword></username>
Searches	Registry .com/search	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts / .com
Searches	Registry RecentDocs	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.&input=
Searches	Voice Recordings	C:\Users\ <username>\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\LocalRecorder\Speech</username>
Searches	WebCacheV01.dat	C:\Users\ <username>\AppData\Local\Microsoft\Windows\WebCache</username>

Defrag		
Registry	Last Defrag	SOFTWARE\Microsoft\Dfrg\Statistics\Volume<guid>

Appendix 1 - Windows 10 Artifact Locations

Edge	Main Application	C:\Users\ <username>\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe</username>
Downloads	File System storage	C:\Users\ <username>\Downloads</username>
Downloads	Edge Cache	C:\Users\ <username>\AppData\Local\Packages\<edge>\ac\#!001\microsoftedge\cache\<#>< td=""> </edge>\ac\#!001\microsoftedge\cache\<#><></username>
Downloads	WebCacheV01.dat	C:\Users\ <username>\AppData\Local\Microsoft\Windows\WebCache</username>
Event Logs		C:\Windows\System32\winevt\Logs
Favorites	Saved favorites	C:\Users\ <username>\AppData\Local\Packages\<edge>\ac\microsoftedge\user\default\favorites\< td=""> </edge>\ac\microsoftedge\user\default\favorites\<></username>
Favorites	Registry	UsrClass.dat\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\mic rosoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\FavOrder\<foldername>
IndexedDB.edb		C:\Users\ <username>\AppData\Local\Packages\<edge>\ac\microsoftedge\user\default\indexed </edge>\ac\microsoftedge\user\default\indexed DB\</username>
InPrivate Browsing	Recovery	C:\Users\ <username>\AppData\Local\Packages\<edge>\ac\microsoftedge\user\default\recovery\ </edge>\ac\microsoftedge\user\default\recovery\ Active</username>
InPrivate Browsing	WebCacheV01.dat	C:\Users\ <username>\AppData\Local\Microsoft\Windows\WebCache</username>
Internet Explorer	Cache	C:\Users\ <username>\AppData\Local\Microsoft\Windows\WebCache</username>
Jump Lists	File tracking	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent</username>
Link Files	File tracking	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent</username>
Local browsing	History - File Explorer	C:\Users\ <username>\AppData\Local\Microsoft\Windows\WebCache</username>
Log Files		C:\Users\ <username>\AppData\Local\Microsoft\OneDrive\logs\Common and Personal</username>
Main Cache	TIF Page storage	C:\Users\ <username>\AppData\Local\Packages\<edge>\ac\#!001\microsoftedge\cache\<#>< td=""> </edge>\ac\#!001\microsoftedge\cache\<#><></username>
Reading List	Files	C:\Users\ <username>\AppData\Local\Packages\<edge>\ac\#!001\microsoftedge\user\default\web </edge>\ac\#!001\microsoftedge\user\default\web Notes</username>
Reading List	Notes	C:\Users\ <username>\AppData\Local\Packages\<edge>\ac\microsoftedge\user\default\datastore\ </edge>\ac\microsoftedge\user\default\datastore\ Data\nouser1\<#>\ReadingList\</username>
Reading List	Recovery, last session	C:\Users\ <username>\AppData\Local\Packages\<edge>\ac\microsoftedge\user\default\recovery\ </edge>\ac\microsoftedge\user\default\recovery\ Active</username>
Reading List	Spartan.edb	C:\Users\ <username>\AppData\Local\Packages\<edge>\ac\microsoftedge\user\default\datastore\ </edge>\ac\microsoftedge\user\default\datastore\ Data\nouser1\<#>\DBStore\</username>

Appendix 1 - Windows 10 Artifact Locations

Recovery	Last open pages	C:\Users\ <username>\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\Recovery\Active\<guid>.dat< td=""> </guid>.dat<></username>
Registry	App Information	UsrClass.dat\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\Microsoft.Microsoftedge\Microsoft.MicrosoftEdge_20.10240.16384.0_neutral__8wekyb3d8bbwe\MicrosoftEdge\Capabilities\FileAssociations
Registry	App Install Date/Time	UsrClass.dat\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Families\Microsoft.Microsoftedge_8wekyb3d8bbwe\Microsoft.MicrosoftEdge_20.10240.16384.0_neutral__8wekyb3d8bbwe / InstallTime
Registry	History - Days to Keep	UsrClass.dat\SOFTWARE\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\InternetSettings\Url History / DaysToKeep
Registry	TypedURLs	UsrClass.dat\SOFTWARE\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLs
Registry	TypedURLs Hyperlink	NTUSER.DAT\SOFTWARE\Microsoft\Internet Explorer\TypedURLs
Registry	TypedURLsTime	UsrClass.dat\SOFTWARE\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLs
Registry	TypedURLsVisitCount	UsrClass.dat\SOFTWARE\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLsVisitCount

File Explorer		
Local Browsing	History	C:\Users\ <username>\AppData\Local\Microsoft\Windows\WebCache</username>
Registry	RecentDocs	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Internet Explorer		
Version 11		
Registry	History - Days to Keep	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Url History / DaysToKeep
Registry	TypedURLs	NTUSER.DAT\SOFTWARE\Microsoft\Internet Explorer\TypedURLs
Registry	TypedURLsTime	NTUSER.DAT\SOFTWARE\Microsoft\Internet Explorer\TypedURLsTime
TIF	Storage	C:\Users\ <username>\AppData\Microsoft\Windows\INetCache</username>
WebCacheV01.dat	Tracking History	C:\Users\ <username>\AppData\Local\Microsoft\Windows\WebCache</username>

Appendix 1 - Windows 10 Artifact Locations

ISO Mounting		
Jump Lists	File Explorer Virtual	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms</username>
Registry	RecentDocs	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.iso

Jump Lists		
Jump Lists	AutomaticDestinations	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations</username>
Common App IDs	MSPaint	12dc1ea8e34b5a6.automaticDestinations-ms
Common App IDs	File Explorer-Virtual	1b4dd67f29cb1962.automaticDestinations-ms
Common App IDs	IE Version 11	28c8b86deab549a1.automaticDestinations-ms
Common App IDs	Microsoft Access	319f01bf9fe00f2d.automaticDestinations-ms
Common App IDs	Wordpad	469e4a7982cea4d4.automaticDestinations-ms
Common App IDs	File Explorer	5f7b5f1e01b83767.automaticDestinations-ms
Common App IDs	Control Panel	7e4dca80246863e3.automaticDestinations-ms
Common App IDs	Windows Store	9a165f62edbf161.automaticDestinations-ms
Common App IDs	Notepad	9b9cdc69c1c24e2b.automaticDestinations-ms
Common App IDs	Edge Browser	9d1f905ce5044aee.automaticDestinations-ms
Common App IDs	Windows Photo	a52b0784bd667468.automaticDestinations-ms
Common App IDs	Zune Music App	ae6df75df512bd06.automaticDestinations-ms
Common App IDs	Excel 2013	b8ab77100df80ab2.automaticDestinations-ms
Common App IDs	PowerPoint 2013	d00655d2aa12ff6d.automaticDestinations-ms
Common App IDs	Adobe Acrobat Reader	de48a32edcbe79e4.automaticDestinations-ms
Common App IDs	File Explorer	f01b4d95cf55d32a.automaticDestinations-ms
Common App IDs	Word 2013	fb3b0dbfee58fac8.automaticDestinations-ms
DestList	AutomaticDestinations	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations</username>
Jump Lists	CustomDestinations	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations</username>
Registry	TaskBar Application List	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Taskband / FavoritesResolve
User Pinned Apps	Link File at:	C:\Users\ <username>\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar</username>

Appendix 1 - Windows 10 Artifact Locations

Link Files		
Link Files	Recent folder	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent</username>
Link Files	Office only	C:\Users\ <username>\AppData\Roaming\Microsoft\Office\15.0\Recent (or 16.0)</username>
Cortana	Searches	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent\https<bing-keyword></username>
Jump Lists	AutomaticDestinations	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations</username>
Link Files	Office only	C:\Users\ <username>\AppData\Roaming\Microsoft\Office\15.0\Recent (or 16.0)</username>
TaskBar	User Pinned	C:\Users\ <username>\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar</username>

Mail		
_sessionState.xml	tmp contact information	C:\Users\ <username>\AppData\Local\Packages\<peopleapp>\</peopleapp></username>
Contacts.txt	Contact information	C:\Users\ <username>\AppData\Local\Packages\<peopleapp>\</peopleapp></username>
Pcontacts.txt	Contact information	C:\Users\ <username>\AppData\Local\Packages\<peopleapp>\</peopleapp></username>
Storage	Mail location; 0=Windows Phone Mail, 2=Contact Data, 3=Mail, 5=Calendar, 7=Attachments	C:\Users\ <username>\AppData\Local\Comms\Unistore\Data<#></username>
store.vol	Full mail storage	C:\Users\ <username>\AppData\Local\Comms\Unistore\</username>
UserDataTempFiles	Temporary mail	C:\Users\ <username>\AppData\Local\Comms\UserDataTempFiles\</username>

Notifications		
	News, tiles, graphics	C:\Users\ <username>\AppData\Local\Microsoft\Windows\Notifications\wpsnidm</username>

Office Applications		
CentralTable.accdb	Using Word as example DB tracking Office docs	C:\Users\ <username>\AppData\Local\Microsoft\Office\15.0\OfficeFileCache (or 16.0)</username>
Graphics	In Word document	\word\media\image<#>.jpg
Link Files	Office only	C:\Users\ <username>\AppData\Roaming\Microsoft\Office\15.0\Recent (or 16.0)</username>
Log File Information	Microsoft Office Alerts	C:\Users\Windows\System32\winevt\Logs\OAlerts.evtx
Metadata	Actual data in Word	\word\document.xml
Metadata	Document Info	docProps\core.xml
Registry	Identity Live Account	NTUSER\SOFTWARE\Microsoft\15.0\Common\Identity\Identities\<ID#>
Registry	MRU Non Live Account	NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\File MRU

Appendix 1 - Windows 10 Artifact Locations

Registry	MRU Live Account	NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\User MRU\LiveId<#>\File MRU
Registry	Place MRU	NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\User MRU\LiveId<#>\Place MRU
Registry	Reading Locations	NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\Reading Locations
Registry	Roaming Identities	NTUSER.DAT\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\Identities\<liveID\Settings\<#>\<guid> (Where <#> is: 1125 PowerPoint, 1133 Word, 1141 Excel
Registry	Trusted Locations	NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\Security\Trusted Locations
Registry	Trusted Documents	NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\Security\Trusted Documents\TrustRecords

OneDrive		
Cache Files	Storage	C:\Users\<username>\AppData\Local\Packages\Microsoft.MicrosoftEdge\8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cache\<#value>
File System	Locally stored files	C:\Users\<username>\OneDrive
LastUpload/Sync	<guid>.ini	C:\Users\<username>\AppData\Local\Microsoft\OneDrive\settings\Personal
Log Files	<liveID#>.dat	C:\Users\<username>\AppData\Local\Microsoft\OneDrive\settings\Personal
Log Files	SyncDiagnostics.log	C:\Users\<username>\AppData\Local\Microsoft\OneDrive\logs\Personal
Log Files	SyncEngine<date>.odl	C:\Users\<username>\AppData\Local\Microsoft\OneDrive\logs\Personal
Log Files	TraceArchive.#.#.#.etl	C:\Users\<username>\AppData\Local\Microsoft\OneDrive\logs\Personal
Log Files	TraceCurrent.#.#.#.etl	C:\Users\<username>\AppData\Local\Microsoft\OneDrive\logs\Personal
Office Docs	Tracking	C:\Users\<username>\AppData\Local\Microsoft\Office\15.0\OfficeFileCache
Online Docs	Tracking - .JSON	C:\Users\<username>\AppData\Local\Microsoft\Windows\WebCache
Online Docs	Tracking - Web Cache	C:\Users\<username>\AppData\Local\Microsoft\Windows\WebCache
Registry	Live Account ID	NTUSER.DAT\SOFTWARE\Microsoft\Office\15.0\Common\Identity\Identities\<liveid>_LiveId
Registry	Live Account ID	NTUSER.DAT\SOFTWARE\Microsoft\IdentityCRL\UserExtendedProperties\<user-email> / cid
Registry	Live Account ID	NTUSER.DAT\SOFTWARE\Microsoft\AuthCookies\Live\Default\CAW / Id
Registry	Run subkey - Active	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Run / OneDrive

OneNote		
BIN Files	Storage of notes	C:\Users\<username>\AppData\Local\Packages\<onenote>\LocalState\AppData\Local\OneNote\16.0\cache
Registry	Identity	settings.dat\LocalState\HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Identity\Identities\<liveID>

Appendix 1 - Windows 10 Artifact Locations

Sharing	Shared data to: e-mail	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharingMFU
Temp Files	Tmp files stored as BIN	C:\Users\ <username>\AppData\Local\Packages\<onenote>\LocalState\AppData\Local\OneNote\16.0\cache\tmp</onenote></username>

Photos App	MediaDB.v1.sqlite	C:\Users\ <username>\AppData\Local\Packages\<winphotos>\LocalState</winphotos></username>
-------------------	-------------------	---

Prefetch		
Prefetch	File System	C:\Windows\Prefetch
Prefetch	Layout.ini	C:\Windows\Prefetch\Layout.ini
Prefetch	Registry Controls	SYSTEM\ControlSet###\Control\Session Manager\Memory Management\PrefetchParameters

Print Spool Files	Word as example app	
File System	Created at time of Print	C:\Windows\System32\spool\PRINTERS\0000#.SPL (data) .SHD (admin info on print job)
Graphics	Inserted #.JPG (folder)	C:\Windows\System32\spool\PRINTERS\0000#.SPL\Documents\1\Resources\Images\#.JPG\[#].piece
Graphics	Pasted #.JPG (file)	C:\Windows\System32\spool\PRINTERS\0000#.SPL\Documents\1\Resources\Images\#.JPG
Printed Pages		C:\Windows\System32\spool\PRINTERS\0000#.SPL\Documents\1\Pages_rels\#.fpage.rels

Recycle Bin		
\$Recycle.Bin	File System	C:\\$Recycle.Bin\ <usersid>< td=""> </usersid><>

Registry Files		
ActivationStore.dat		Individual application folder, usually under folder called ActivationStore
Amcache.hve	Executable tracking	C:\Windows\appcompat\Programs
NTUSER.DAT	User behavior tracking	C:\Users\ <username>< td=""> </username><>
SAM	Security Account Mgr	C:\Windows\System32\config
SECURITY	Local security acct info	C:\Windows\System32\config
settings.dat	App settings	C:\Users\ <username>\AppData\Local\Packages\<individualappname>\Settings</individualappname></username>
SOFTWARE	Global software settings	C:\Windows\System32\config
SYSTEM	System settings	C:\Windows\System32\config

Appendix 1 - Windows 10 Artifact Locations

Thumbnail Cache		
Thumbnail Cache	Centralized thumb cache	C:\Users\ <username>\AppData\Local\Microsoft\Windows\Explorer</username>
thumbs.db	Network browsing	In folder that was browsed with some form of View Icons

Tiles		
	vedatamodel.edb	C:\Users\ <username>\AppData\Local\TileDataLayer\Database</username>
Notifications	News, tiles, graphics	C:\Users\ <username>\AppData\Local\Microsoft\Windows\Notifications\wpidm</username>
Start - Tiles, Office	vedatamodel.edb	C:\Users\ <username>\AppData\Local\TileDataLayer\Database</username>
Detection	Header to search for	0x 33 C0 8E D0 BC 00 7C 8E
Event Logs	VHDMP Operational Log	C:\Windows\System32\winevt\Logs\Microsoft-Windows-VHDMP%4Operational.evtx
Registry	Common Dialog	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU.vhd
Registry	RecentDocs	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs.vhd
Registry	Shell Bags	NTUSER.DAT\SOFTWARE\Microsoft\Windows\Shell\Bags\1\Desktop (if it is on the Desktop)

Windows		
User Logon Icon	<guid>.accountpicture-ms	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\AccountPictures</username>

Xbox		
Blocked.xml	Log of blocked users	C:\Users\ <username>\AppData\Local\Packages\<xboxapp>\LocalState\ModelManager</xboxapp></username>
Messages.xml	Tracks msgs sent/rcvd	C:\Users\ <username>\AppData\Local\Packages\<xboxapp>\LocalState\ModelManager</xboxapp></username>
Livetiledata.xml	Activity and msg alerts	C:\Users\ <username>\AppData\Local\Packages\<xboxapp>\LocalState\ModelManager</xboxapp></username>
LocalState	Friend, Game Info, Msg data and Settings	C:\Users\ <username>\AppData\Local\Packages\<xboxapp>\LocalState\</xboxapp></username>
ModelManager	Social Activity	C:\Users\ <username>\AppData\Local\Packages\<xboxapp>\LocalState\ModelManager</xboxapp></username>
People	Friend List	C:\Users\ <username>\AppData\Local\Packages\<xboxapp>\LocalState\ModelManager\People\Following</xboxapp></username>
Pins.xml	List of pinned apps	C:\Users\ <username>\AppData\Local\Packages\<xboxglassapp>\LocalState\</xboxglassapp></username>
ProfileActivity	Activity between users	C:\Users\ <username>\AppData\Local\Packages\<xboxapp>\LocalState\ModelManager\ProfileActivity</xboxapp></username>
SmartGlass App	Connection app for Xbox	C:\Users\ <username>\AppData\Local\Packages\<xboxglassapp>\LocalState\</xboxglassapp></username>

Appendix 1 - Windows 10 Artifact Locations

SmartGlassSettings.sg	Connection settings	C:\Users\ <username>\AppData\Local\Packages\<xboxapp>\LocalState\ModelManager\SmartGlass</xboxapp></username>
SocialAlerts.xml	Social Activity	C:\Users\ <username>\AppData\Local\Packages\<xboxapp>\LocalState\ModelManager</xboxapp></username>
XboxLiveApp.log	Action log	C:\Users\ <username>\AppData\Local\Packages\<xboxapp>\LocalState\ModelManager</xboxapp></username>
Xboxlivegamer.xml	User info, Gamer Tag	C:\Users\ <username>\AppData\Local\Packages\<xboxapp>\LocalState\ModelManager</xboxapp></username>
XboxLiveGamerID.xml	Logged on user	C:\Users\ <username>\AppData\Local\Packages\<xboxglassapp>\LocalState\</xboxglassapp></username>