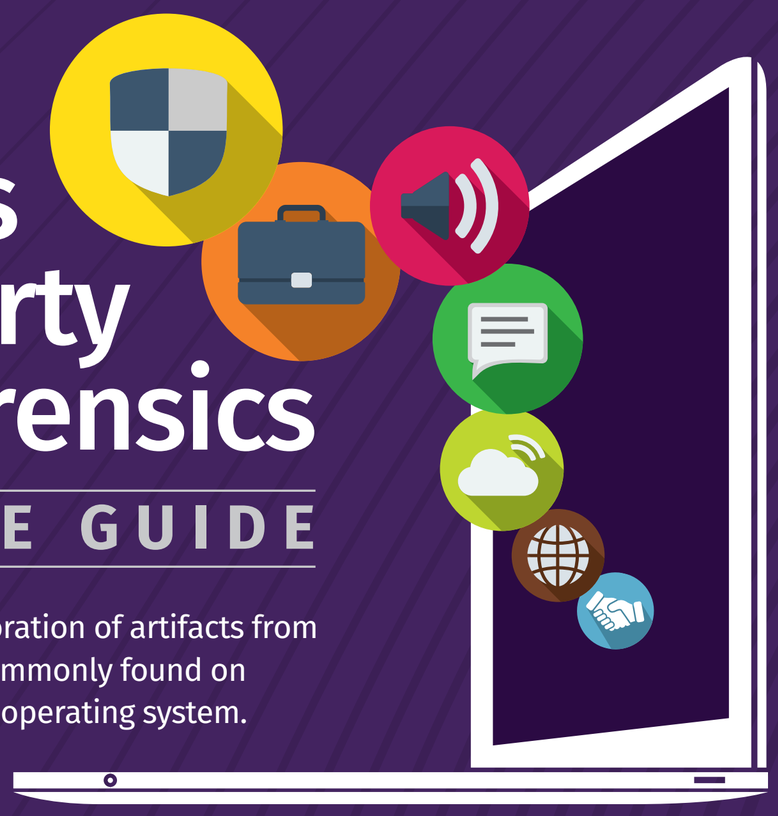
SANS

Windows Third-Party Apps Forensics

REFERENCE GUIDE

This poster is a detailed exploration of artifacts from 46 third-party applications commonly found on devices running the Windows operating system.



The world runs on Microsoft Windows largely because of the diversity of available third-party applications. Artifacts left behind by these applications are as diverse as the applications themselves, spanning the file system. Here you will find some of the most important artifacts available from popular Windows applications including browsers, productivity and communication applications, and cloud storage. Please note that applications change over time and older or newer applications will inevitably store data in different locations. While a comprehensive view is impractical, these locations make excellent places to begin an investigation.

DFPS_Windows-Apps-v1.5_0624

AUDIO & VIDEO

iTunes

https://www.apple.com/itunes

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\Apple Computer\iTunes	iPodDevices.xml	XML
C:\Users\%user%\AppData\Roaming\Apple Computer\ MobileSync\Backup	*	Various
C:\Users\%user%\AppData\Roaming\Apple Computer\Logs\ CrashReporter\MobileDevice	*	Various
C:\Users\%user%\Apple\Mobilesync\Backup\	*	Various
C:\ProgramData\Apple\Lockdown	*.plist	Plist
C:\ProgramData\Apple Computer\iTunes\	iPodDevices.xml	XML

REFERENCES:
https://rb.gy/i7s4pw
https://rb.gy/x3tyg8
https://www.digitalforensics.com/blog/articles/itunes-backup-forensic-analysis
https://forensafe.com/blogs/itunes.html

VLC Media Player

https://www.videolan.org

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\vlc\	vlc-qt-interface.ini	TXT

REFERENCES:
https://www.forensicfocus.com/forums/general/vlc-recent-files
https://superuser.com/questions/287137/does-vlc-media-player-store-the-files-or-its-history-in-a-hidden-location/1206411
https://www.forensafe.com/blogs/vlc.html

COMMUNICATION

Discord

https://discord.com/download

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\discord\cache\	*	Various
C:\Users\%user%\AppData\Roaming\discord\local storage\leveldb\	*	LevelDB

REFERENCES:
https://abrignoni.blogspot.com/2018/03/finding-discord-app-chats-in-windows.html
https://abrignoni.blogspot.com/2020/08/update-on-discord-forensic-artifacts.html
https://www.champlain.edu/Documents/LCDI/ApplicationAnalysis_S17.pdf
https://www.forensafe.com/blogs/discord.html

Telegram

https://telegram.org

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\Telegram Desktop\	*	Various
C:\Users\%user%\Downloads\Telegram Desktop\	*	Various

REFERENCES:
https://www.digitalforensics.com/blog/articles/forensic-analysis-instant-messengers-desktop-applications

Signal

https://signal.org

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\Signal\attachments.noindex\	*	Various
C:\Users\%user%\AppData\Roaming\Signal\Cache\	*	Various
C:\Users\%user%\AppData\Roaming\Signal\logs\	*	TXT
C:\Users\%user%\AppData\Roaming\Signal\sql\	db.sqlite	SQLite
C:\Users\%user%\AppData\Roaming\Signal\	config.json	JSON

REFERENCES:
https://blog.elcomsoft.com/2020/04/forensic-guide-to-imessage-whatsapp-telegram-signal-and-skype-data-acquisition
https://www.bleepingcomputer.com/news/security/signal-desktop-leaves-message-decryption-key-in-plain-sight
https://www.linkedin.com/pulse/signal-desktop-digital-forensics-perspective-surya-teja-masanam
https://www.alexbilz.com/post/2021-06-07-forensic-artifacts-signal-desktop/
https://www.zetetic.net/sqlcipher/sqlcipher-api/#key
https://github.com/signalapp/Signal-Desktop/blob/master/ts/sql/Server.ts#L276
https://www.forensafe.com/blogs/signal.html

Thunderbird

https://www.thunderbird.net

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\Thunderbird\Crash Reports\	InstallTime*	TXT
C:\Users\%user%\AppData\Roaming\Thunderbird\	profiles.ini	TXT
C:\Users\%user%\AppData\Roaming\Thunderbird\Profiles*\	prefs.js	TXT
C:\Users\%user%\AppData\Roaming\Thunderbird\Profiles*\	global-messages-db.sqlite	SQLite
C:\Users\%user%\AppData\Roaming\Thunderbird\Profiles*\	logins.json	JSON
C:\Users\%user%\AppData\Roaming\Thunderbird\Profiles*\	places.sqlite	SQLite
C:\Users\%user%\AppData\Roaming\Thunderbird\Profiles*\ImapMail\	*	Various
C:\Users\%user%\AppData\Roaming\Thunderbird\Profiles*\Mail\	*	Various
C:\Users\%user%\AppData\Roaming\Thunderbird\Profiles*\calendar-data\	local.sqlite	SQLite
C:\Users\%user%\AppData\Roaming\Thunderbird\Profiles*\Attachments\	*	Various
C:\Users\%user%\AppData\Roaming\Thunderbird\Profiles*\	abook.sqlite	SQLite

REFERENCES:
https://www.mailxaminer.com/blog/mozilla-thunderbird-forensics
https://az4n6.blogspot.com/2014/04/whats-word-thunderbird-parser-that-is.html
https://www.forensafe.com/blogs/thunderbird.html

WhatsApp

https://www.whatsapp.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\WhatsApp\Cache\	*	Various
C:\Users\%user%\AppData\Roaming\WhatsApp\Local Storage\leveldb\	*	LevelDB
C:\Users\%user%\AppData\Local\Packages*WhatsAppDesktop*\ LocalCache\Roaming\WhatsApp\Cache\	*	Various
C:\Users\%user%\AppData\Local\Packages*WhatsAppDesktop*\ LocalCache\Roaming\WhatsApp\Local Storage\leveldb\	*	LevelDB
C:\Users\%user%\AppData\Local\Packages*WhatsAppDesktop*\ LocalState\profilePictures\	*	Various
C:\Users\%user%\AppData\Local\Packages*WhatsAppDesktop*\ LocalState\rotatedLogs\	*	TXT
C:\Users\%user%\AppData\Local\Packages*WhatsAppDesktop*\ LocalState\shared\transfers\	*	Various

REFERENCES:
https://belkasoft.com/whatsapp_forensics_on_computers
https://belkasoft.com/forms/whatsapp_webinar
https://security.stackexchange.com/questions/215483/forensics-methods-for-obtaining-whatsapp-data-from-windows-desktop-pcs
https://www.digitalforensics.com/blog/articles/forensic-analysis-instant-messengers-desktop-applications
https://www.researchgate.net/publication/333247702_WhatsApp_Forensics_Locating_Artifacts_in_Web_and_Desktop_Clients
https://www.group-ib.com/blog/whatsapp-forensic-artifacts
https://www.forensafe.com/blogs/whatsapp.html

Skype

https://www.skype.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\Packages\Microsoft.SkypeApp_*\LocalState*\	main.db	SQLite
C:\Users\%user%\AppData\Local\Packages\Microsoft.SkypeApp_*\LocalState*\	skype.db	SQLite
C:\Users\%user%\AppData\Local\Packages\Microsoft.SkypeApp_*\LocalState\	s4l-*.db	SQLite
C:\Users\%user%\AppData\Roaming\Microsoft\Skype for Desktop\ IndexedDB*.leveldb\	*	LevelDB
C:\Users\%user%\AppData\Roaming\Microsoft\Skype for Desktop\Cache\	*	Various

REFERENCES:
https://bebinary4n6.blogspot.com/2019/07/analysis-of-skype-windows-10-app.html
https://bebinary4n6.blogspot.com/2019/07/skype-from-old-one-to-newest-one.html
https://blog.elcomsoft.com/2019/12/extracting-skype-histories-and-deleted-files-metadata-from-microsoft-account
https://bebinary4n6.blogspot.com/2019/07/analysis-skype-app-for-windows-metro.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/microsoft-teams-and-skype-logging-privacy-issue
https://www.forensafe.com/blogs/skype.html

Viber

https://www.viber.com/en

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\ViberPC\	config.db	SQLite
C:\Users\%user%\AppData\Roaming\ViberPC*\	viber.db	SQLite
C:\Users\%user%\AppData\Roaming\ViberPC*\Avatars\	*	Various
C:\Users\%user%\AppData\Roaming\ViberPC*\Backgrounds\	*	Various
C:\Users\%user%\AppData\Roaming\ViberPC*\Thumbnails\	*	Various

REFERENCES:
https://www.digitalforensics.com/blog/articles/forensic-analysis-instant-messengers-desktop-applications
https://www.alexbilz.com/post/2021-01-29-forensic-artifacts-viber-desktop
https://www.forensafe.com/blogs/viber.html

Zoom

https://zoom.us

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\Zoom\logs\	*	TXT
C:\Users\%user%\AppData\Roaming\Zoom\data\	*	Various
C:\Users\%user%\Documents\Zoom\	*	Various

REFERENCES:
https://www.sciencedirect.com/science/article/pii/S2666281721000019
https://support.zoom.us/hc/en-us/articles/201512326-Troubleshooting-log-for-Windows
https://www.forensafe.com/blogs/zoom.html

BROWSER

Brave Browser

https://brave.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	*	Various
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	Bookmarks*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\Network\	Cookies*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	Favicons*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	History*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	Login Data*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	Media History*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	Network Action Predictor*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	Network Persistent State	JSON
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	Preferences	JSON
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\Network\	Reporting & NEL*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	SecurePreferences	JSON
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	Shotcuts*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	Top Sites*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	Trust Tokens*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\	Web Data*	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\Sync Data\	SyncData.sqlite3	SQLite
C:\Users\%user%\AppData\Local\BraveSoftware\Brave-Browser\User Data*\Sessions\	*	SNSS

REFERENCES:
https://www.forensafe.com/blogs/brave.html

Microsoft Edge

https://www.microsoft.com/en-us/edge

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	Bookmarks*	SQLite
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	Favicons*	SQLite
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	History*	SQLite
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	Login Data*	SQLite
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	Network Action Predictor*	SQLite
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	Preferences	JSON
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	Shotcuts*	SQLite
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	Top Sites*	SQLite
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	Trust Tokens*	SQLite
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	Visited Links	
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\	Web Data*	SQLite
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\Sync Data\LevelDB\	*	LevelDB
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\Sessions\	*	SNSS
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\Collections	collectionsSQLite	SQLite
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\IndexedDB\	*	LevelDB
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\Local Storage\leveldb\	*	LevelDB
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\Session Storage\	*	LevelDB
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\Web Storage\	*	LevelDB
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\Platform Notifications\	*	LevelDB
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\Cache\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\Network\	Cookies*	SQLite
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\Network\	Reporting & NEL*	SQLite

REFERENCES:
https://www.forensicfocus.com/articles/chromium-based-microsoft-edge-from-a-forensic-point-of-view
https://www.dataforensics.org/microsoft-edge-browser-forensics
https://blog.group-ib.com/forensics_edge
https://rb.gy/oj3iic
https://www.foxtonforensics.com/blog/post/investigating-web-history-in-the-new-edge-chromium-browser
https://dfir.blog/a-first-look-at-chromium-based-edge

Google Chrome

https://www.google.com/intl/en_us/chrome

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Bookmarks*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	DownloadMetadata	
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Extension Cookies*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Favicons*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	History*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Login Data*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Media History*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Network Action Predictor*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Network Persistent State	JSON
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Preferences	JSON
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	SecurePreferences	JSON
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Shotcuts*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Top Sites*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Visited Links	
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Web Data*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\Sync Data\LevelDB\	*	LevelDB
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\Sessions\	*	SNSS
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\Extensions\	*	Various
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\File System\	*	LevelDB
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\IndexedDB\	*	LevelDB
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\ Local Storage\leveldb\	*	LevelDB
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\Session Storage\	*	LevelDB
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\Web Storage\	*	LevelDB
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\WebStorage\	QuotaManager*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\ Platform Notifications\	*	LevelDB
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\Network\	Cookies*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\Network\	Reporting & NEL*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\Cache\	*	Various

REFERENCES:
https://nasbench.medium.com/web-browsers-forensics-7e99940c579a
https://www.digitalforensics.com/blog/articles/an-overview-of-web-browser-forensics
https://www.sans.org/blog/google-chrome-forensics
https://rb.gy/43hkbu
https://rb.gy/bbvo8z
https://dfir.blog/chrome-values-lookup-tables
https://dfir.blog/chrome-evolution

Mozilla Firefox

https://www.mozilla.org/en-US/firefox

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	*	Various
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	addons.sqlite	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\weave	bookmarks.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\bookmarkbackups	*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	cookies.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	firefox_cookies.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	downloads.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	extensions.json	JSON
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	favicons.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	formhistory.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	permissions.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	places.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	protections.sqlite*	JSON
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	search.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	signons.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	storage-sync.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	webappstore.sqlite*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	key*.db	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	signon*.*	SQLite
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	logins.json	JSON
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	prefs.js	JSON
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\	sessionstore*	JSON
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\sessionstore-backups\	sessionstore*	JSON
C:\Users\%user%\AppData\Local\Mozilla\Firefox\Profiles*\	*	Various

REFERENCES:
https://www.4n6k.com/2017/11/forensics-quickie-identifying-clear.html
https://www.digitalforensics.com/blog/articles/an-overview-of-web-browser-forensics

Microsoft Internet Explorer

https://www.microsoft.com/it-it/download/internet-explorer.aspx

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\Microsoft\Internet Explorer\	*	Various
C:\Users\%user%\AppData\Roaming\Microsoft\Internet Explorer\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Windows\History\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Windows\Cookies\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Windows\IEDownloadHistory\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Windows\WebCache\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Windows\INetCookies\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Windows\Temporary Internet Files\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Windows\INetCache\	*	Various

REFERENCES:
https://www.digitalforensics.com/blog/articles/an-overview-of-web-browser-forensics
https://www.dataforensics.org/internet-explorer-forensics
https://www.xploreforensics.com/blog/internet-explorer-forensic-artifacts-analysis.html
https://rb.gy/oj3iic

Opera Browser

https://www.opera.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\Opera Software\Opera Stable*\Cache	*	Various
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\	Bookmarks*	SQLite
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\	Favicons*	SQLite
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\	History*	SQLite
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\	Login Data*	SQLite
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\	Network Action Predictor*	SQLite
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\	Preferences	JSON
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\	SecurePreferences	JSON
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\	Shotcuts*	SQLite
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\	Top Sites*	SQLite
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\	Web Data*	SQLite
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\ Sync Data\LevelDB	*	LevelDB
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\Sessions\	*	SNSS
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\Extensions\	*	Various
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\IndexedDB\	*	LevelDB
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\ Local Storage\leveldb\	*	LevelDB
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\Session Storage\	*	LevelDB
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\Web Storage\	QuotaManager	SQLite
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\Network\	Reporting & NEL*	SQLite
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable*\Network\	Cookies*	SQLite

REFERENCES:
https://kb.digital-detective.net/display/BF/Opera
https://www.digitalforensics.com/blog/articles/an-overview-of-web-browser-forensics
https://davidkoepi.wordpress.com/2012/12/16/opera-forensics
https://www.forensafe.com/blogs/opera.html

P2P

BitTorrent

https://www.bittorrent.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\BitTorrent\	*.dat	TXT

REFERENCES:
https://www.researchgate.net/publication/288858418_Investigation_of_Artifacts_Left_by_BitTorrent_Client_on_the_Local_Computer_Operating_under_Windows_81
https://www.sans.org/reading-room/whitepapers/legal/bittorrent-digital-contraband-36887
https://www.sciencedirect.com/science/article/abs/pii/S1742287610000770
https://www.sciencedirect.com/science/article/pii/S1742287614000152
https://forensafe.com/blogs/windows_bittorrent.html

qBittorrent

https://www.qbittorrent.org

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\qBittorrent\	*.ini	TXT
C:\Users\%user%\AppData\Local\qBittorrent\logs\	*	TXT
C:\Users\%user%\AppData\Local\qBittorrent\GeoDB\	*	Various
C:\Users\%user%\AppData\Local\qBittorrent\BT_backup\	*	Various

REFERENCES:
https://troy4n6.blogspot.com/2019/02/text-based-treasure-qbittorent-log-file.html

FrostWire

https://www.frostwire.com

Path	File Name/Mask	File Type
C:\Users\%user%\Documents\FrostWire\Torrent Data	*	Various
C:\Users\%user%\.frostwire5	frostwire.props	TXT
C:\Users\%user%\.frostwire5	itunes.props	TXT

REFERENCES:
https://www.cyberagentsinc.com/2017/08/10/frostwire-artifacts

uTorrent

https://www.utorrent.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\uTorrent\	*.dat	TXT

REFERENCES:
https://robertpearsonblog.wordpress.com/2016/11/11/utorrent-and-windows-10-forensic-nuggets-of-info
https://www.forensicfocus.com/articles/forensic-analysis-of-the-%CE%BCtorrent-peer-to-peer-client-in-windows
https://forensafe.com/blogs/android_utorrent.html

dfir.sans.org

SANS DFIR

PRODUCTIVITY

1Password

https://1password.com/downloads/windows

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\1password\data	1Password10.sqlite	SQLite
C:\Users\%user%\AppData\Local\1password\backups	1Password10.sqlite	SQLite
C:\Users\%user%\AppData\Local\1password\logs	*.log	TXT

REFERENCES:

https://blog.elcomsoft.com/2017/08/attacking-the-1password-master-password-follow-up
https://forensafe.com/blogs/windows_1password.html

Acronis True Image

https://www.acronis.com/en-us/products/true-image

Path	File Name/Mask	File Type
C:\ProgramData\Acronis\TrueImageHome\Logs\ti_demon\	*	Various
C:\ProgramData\Acronis\TrueImageHome\Database	*	Various
C:\ProgramData\Acronis\TrueImageHome\Scripts\	archives.db	SQlite

REFERENCES:

https://care.acronis.com/s/article/49484-Acronis-True-Image-Finding-and-Analyzing-Logs?language=en_US&ckattempt=1

AnyDesk

https://anydesk.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\AnyDesk\	*.trace	TXT
C:\Users\%user%\AppData\Roaming\AnyDesk\	*.conf	TXT
C:\Users\%user%\AppData\Roaming\AnyDesk\	connection_trace.txt	TXT
C:\Users\%user%\AppData\Roaming\AnyDesk\chat\	*	TXT
C:\ProgramData\AnyDesk\	*.trace	TXT
C:\ProgramData\AnyDesk\	*.conf	TXT
C:\ProgramData\AnyDesk\	connection_trace.txt	TXT
C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\AnyDesk\	*	Various

REFERENCES:

https://support.anydesk.com/Trace_Files
https://www.inversecos.com/2021/02/forensic-analysis-of-anydesk-logs.html
https://medium.com/mii-cybersec/digital-forensic-artifact-of-anydesk-application-c9b8cfb23ab5
https://medium.com/@inginformatico/forensic-analysis-to-anydesk-forensic-artifacts-and-log-analysis-eng-3897da98324d
https://www.forensafe.com/blogs/anydesk.html
https://www.iblue.team/incident-response-1/anydesk-remote-access
https://www.linkedin.com/posts/mohamed-adil-re_github-mohamed-adil-cyberanydesk-velociraptorir-log-collector-activity-7039113200994287616-ig-e
https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_1_1_yamashige-nakatani-tanaka_en.pdf
https://www.synacktiv.com/en/publications/legitimate-rats-a-comprehensive-forensic-analysis-of-the-usual-suspects
https://hatsoffsecurity.com/2022/02/28/anydesk-forensic-analysis-and-artefacts
https://docs.velociraptor.app/exchange/artifacts/pages/windows.applications.anydesk
https://support.anydesk.com/knowledge/anydesk-id-and-alias
https://vikas-singh.notion.site/vikas-singh/Remote-Access-Software-Forensics-3e38d9a66ca0414ca9c882ad67f4f71b

Evernote

https://evernote.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\Evernote\Evernote\ Databases\	*.accounts	TXT
C:\Users\%user%\AppData\Local\Evernote\Evernote\Databases\	*.exb	SQLite
C:\Users\%user%\AppData\Local\Evernote\Evernote\Databases\	*.exb.snippets	Various

REFERENCES:

https://arxiv.org/pdf/1709.10395
https://www.forensicfocus.com/articles/evernote-introduction
https://rb.gy/nuwobq
https://www.forensafe.com/blogs/evernote.html

Filezilla

https://filezilla-project.org

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\FileZilla\	*.xml*	XML
C:\Users\%user%\AppData\Roaming\FileZilla\	*.sqlite3*	SQLite

REFERENCES:

https://www.sans.org/reading-room/whitepapers/forensics/evidence-data-exfiltration-containerised-applications-virtual-private-servers-38555
https://wiki.filezilla-project.org/Logs
https://www.hecfblog.com/2013/09/daily-blog-93-filezilla-artifacts.html
https://forensafe.com/blogs/filezilla.html

LogMeIn

https://www.logmein.com

Path	File Name/Mask	File Type
C:\ProgramData\LogMeIn\Logs\	*	Various
C:\Users\%user%\AppData\Local\temp\LogMeInLogs\	*	Various

REFERENCES:

https://support.logmeininc.com/pro/help/how-to-view-logmein-event-log-files-logmein-t-host-preferences-log
https://www.researchgate.net/publication/313796589_An_exploration_of_artefacts_of_remote_desktop_applications_on_Windows
https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1166&context=adf
https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_1_1_yamashige-nakatani-tanaka_en.pdf

Microsoft OneNote

https://www.onenote.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\Packages\Microsoft.Office.OneNote_8wekyb3d8bbwe\LocalState\AppData\Local\OneNote*\FullTextSearchIndex	*	Various
C:\Users\%user%\AppData\Local\Packages\Microsoft.Office.OneNote_8wekyb3d8bbwe\LocalState\AppData\Local\OneNote\Notifications	*	Various
C:\Users\%user%\AppData\Local\Packages\Microsoft.Office.OneNote_8wekyb3d8bbwe\LocalState\AppData\Local\OneNote\16.0\AccessibilityCheckerIndex	*	Various
C:\Users\%user%\AppData\Local\Packages\Microsoft.Office.OneNote_8wekyb3d8bbwe\LocalState\AppData\Local\OneNote\16.0\NoteTags	*LiveId.db	SQLite
C:\Users\%user%\AppData\Local\Packages\Microsoft.Office.OneNote_8wekyb3d8bbwe\LocalState\AppData\Local\OneNote\16.0\RecentSearches	RecentSearches.db	SQLite

REFERENCES:

https://www.microsoft.com/en-us/microsoft-365/onenote/digital-note-taking-app

IrfanView

https://www.irfanview.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\IrfanView\	i_view32.ini	TXT

Microsoft Teams

https://www.microsoft.com/en-us/microsoft-teams/group-chat-software

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\Microsoft\Teams\IndexedDB\	*	LevelDB
C:\Users\%user%\AppData\Roaming\Microsoft\Teams\Local Storage\	*	LevelDB
C:\Users\%user%\AppData\Roaming\Microsoft\Teams\Cache\	*	Various
C:\Users\%user%\AppData\Roaming\Microsoft\Teams\	desktop-config.json	JSON
C:\Users\%user%\AppData\Local\Packages\MicrosoftTeams_8wekyb3d8bbwe\LocalCache\Microsoft\MSTeams\Logs\	*	Various

REFERENCES:

https://rb.gy/tbkt1l
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/microsoft-teams-and-skype-logging-privacy-issue
https://netsecninja.github.io/analysis/2021/02/11/ms-teams-logs-activity.html
https://rb.gy/tby3y9
https://www.alexbilz.com/post/2021-09-09-forensic-artifacts-microsoft-teams
https://bakerstreetforensics.com/2021/05/10/collecting-from-microsoft-teams-using-powershell
https://github.com/lxndrblz/forensicsim

Notepad++

https://notepad-plus-plus.org

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\Notepad++\backup\	*	Various
C:\Users\%user%\AppData\Roaming\Notepad++\	config.xml	XML
C:\Users\%user%\AppData\Roaming\Notepad++\	session.xml	XML

REFERENCES:

https://forensafe.com/blogs/windows_notepad++.html

Slack

https://slack.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\Slack\Cache\	*	Various
C:\Users\%user%\AppData\Roaming\Slack\IndexedDB\	*	LevelDB
C:\Users\%user%\AppData\Roaming\Slack\Local Storage\leveldb\	*	LevelDB
C:\Users\%user%\AppData\Roaming\Slack\logs\	*	TXT
C:\Users\%user%\AppData\Roaming\Slack\storage\	*	TXT
C:\Users\%user%\AppData\Roaming\Slack\storage\	root-state.json	JSON

TeamViewer

https://www.teamviewer.com

Path	File Name/Mask	File Type
C:\Program Files*\TeamViewer\	connections*.txt	TXT
C:\Program Files*\TeamViewer\	TeamViewer*_Logfile*	TXT
C:\Users\%user%\AppData\Roaming\TeamViewer\MRU\RemoteSupport\	*	TXT

REFERENCES:

https://rb.gy/qbhfug
https://svch0st.medium.com/writeup-magnet-user-summit-dfir-ctf-2019-activity-79cf149c04d7
https://www.systoolsgroup.com/forensics/teamviewer
https://athenaforensics.co.uk/teamviewer-forensics
https://medium.com/mii-cybersec/digital-forensic-artifact-of-teamviewer-application-cfd6290dc0a7
https://www.forensafe.com/blogs/teamviewer.html
https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1166&context=adf
https://vikas-singh.notion.site/vikas-singh/Remote-Access-Software-Forensics-3e38d9a66ca0414ca9c882ad67f4f71b
https://www.researchgate.net/publication/359220574_Remote_Desktop_Software_as_a_forensic_resource
https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_1_1_yamashige-nakatani-tanaka_en.pdf
https://www.synacktiv.com/en/publications/legitimate-rats-a-comprehensive-forensic-analysis-of-the-usual-suspects.html

TeraCopy

https://www.codesector.com/teracopy

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\TeraCopy\	*	Various

REFERENCES:

https://www.kraftkennedy.com/teracopy-forensics-finding-elusive-copy-log
https://www.stark4n6.com/2018/11/teracopy-forensic-analysis-part-1.html
https://www.stark4n6.com/2018/11/teracopy-forensic-analysis-part-2.html

VMWare

https://www.vmware.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\VMware\	*	Various

REFERENCES:

https://crucialsecurity.wordpress.com/2011/05/23/virtual-machine-files-essential-to-forensic-investigations
https://blog.salvationdata.com/2018/06/01/case-study-how-to-forensically-extract-evidence-data-from-a-virtual-machine

WinSCP

https://winscp.net

Path	File Name/Mask	File Type
C:*	WinSCP.ini	TXT

REFERENCES:

https://az4n6.blogspot.com/2020/02/detecting-laterial-movment-with-winscp.html

ANTIVIRUS

Avast

https://www.avast.com

Path	File Name/Mask	File Type
C:\ProgramData\Avast Software\Avast\Log\	*	Various
C:\ProgramData\Avast Software\Avast\Log\	aswAr*.log	TXT
C:\ProgramData\Avast Software\Avast\Log\	AvastSvc.log	TXT
C:\ProgramData\Avast Software\Avast\Chest\	index.xml	XML
C:\ProgramData\Avast Software\Icarus\Logs\	*	Various
C:\ProgramData\Avast Software\Persistent Data\Avast\Logs\	*	Various
C:\Users\%user%\Avast Software\Avast\Log\	*	Various

REFERENCES:

https://businesshelp.avast.com/Content/Products/General_Help/LogLocations/BaseAntivirusLogs.htm
https://forensafe.com/blogs/windows_avast.html

AVG

https://www.avg.com

Path	File Name/Mask	File Type
C:\ProgramData\AVG\Antivirus\log\	*	Various
C:\ProgramData\AVG\Antivirus\report\	*	Various
C:\ProgramData\AVG\Persistent Data\Antivirus\Logs\	*	Various
C:\ProgramData\AVG\Antivirus\	FileInfo2.db	SQLite
C:\ProgramData\AVG\Antivirus\	lsdb2.json	JSON

REFERENCES:

https://businesshelp.avast.com/Content/Products/General_Help/LogLocations/BaseAntivirusLogs.htm
https://forensafe.com/blogs/windows_avg.html

Avira

https://www.avira.com

Path	File Name/Mask	File Type
C:\ProgramData\Avira\Antivirus\LOGFILES\	*	Various
C:\ProgramData\Avira\Security\Logs\	*	Various
C:\ProgramData\Avira\VPN\	*	Various

REFERENCES:

https://support.avira.com/hc/en-us/community/posts/360013822317-Where-are-the-logs-for-Avira-Security-Smart-Scan-
https://forensafe.com/blogs/windows_avira.html

ESET

https://www.eset.com

Path	File Name/Mask	File Type
C:\ProgramData\ESET\ESET NOD32 Antivirus\Logs\	*	Various
C:\ProgramData\ESET\ESET Security\Logs\	*	Various
C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\	*	Various
C:\Users\%user%\AppData\Local\ESET\ESET Security\Quarantine\	*	Various
C:\Windows\System32\config\systemprofile\AppData\Local\ESET\ESET Security\Quarantine\	*	Various

REFERENCES:

https://www.eset.com/int/support/log-collector
https://github.com/laciKE/EsetLogParser
https://help.eset.com/protect_admin/80/en-US/fs_agent_connection_troubleshooting.html

F-Secure

https://www.f-secure.com

Path	File Name/Mask	File Type
C:\ProgramData\F-Secure\Log\	*	Various
C:\Users\%user%\AppData\Local\F-Secure\Log\	*	Various
C:\ProgramData\F-Secure\Antivirus\ScheduledScanReports\	*	Various

REFERENCES:

https://community.f-secure.com/en/discussion/122488/removing-f-secure-log-files-from-internet-security
ftp://ftp.f-secure.com/support/tools/debugtools
https://forensafe.com/blogs/windows_f-secure.html

McAfee

https://www.mcafee.com

Path	File Name/Mask	File Type
C:\ProgramData\McAfee\DesktopProtection\	*	Various
C:\ProgramData\McAfee\Endpoint Security\Logs\	*	Various
C:\ProgramData\McAfee\Endpoint Security\Logs_Old\	*	Various
C:\ProgramData\Mcafee\VirusScan\	*	Various

REFERENCES:

https://techadminblog.com/mcafee-log-file-locations-cheat-sheet-windows

Malwarebytes

https://www.malwarebytes.com

Path	File Name/Mask	File Type
C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\Logs\	mbam-log-*.xml	XML
C:\ProgramData\Malwarebytes\MBAMService\logs\	mbamservice.log*	TXT
C:\Users\%user%\AppData\Roaming\Malwarebytes\Malwarebytes Anti-Malware\Logs\	*	Various
C:\ProgramData\Malwarebytes\MBAMService\ScanResults\	*	Various

REFERENCES:

https://for500.com/malwarebytes
https://forensafe.com/blogs/windows_malwarebytes.html

Microsoft Defender

https://www.microsoft.com/en-us/microsoft-365/microsoft-defender-for-individuals

Path	File Name/Mask	File Type
C:\ProgramData\Microsoft\Microsoft AntiMalware\Support\	*	Various
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Service\DetectionHistory*\	*	Various
C:\ProgramData\Microsoft\Windows Defender\Support\	*	Various
C:\ProgramData\Microsoft\Windows Defender\Quarantine\	*	Various
C:\Windows\Temp\	MpCmdRun.log	TXT
C:\Windows.old\Temp\	MpCmdRun.log	TXT
C:\Windows\System32\winevt\Logs\	Microsoft-Windows-Windows Defender*.evtx	EVTX

REFERENCES:

https://knez.github.io/posts/how-to-extract-quarantine-files-from-windows-defender
https://www.crowdstrike.com/blog/how-to-use-microsoft-protection-logging-for-forensic-investigations
https://github.com/jklepsercyber/defender-detectionhistory-parser/blob/main/README.md
https://forensafe.com/blogs/windows_defender.html
https://m365internals.com/2021/07/05/why-are-windows-defender-av-logs-so-important-and-how-to-monitor-them-with-azure-sentinel
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/troubleshoot-windows-defender-antivirus
https://www.sans.org/blog/uncovering-windows-defender-real-time-protection-history-with-dhparser
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide

Sophos

https://www.sophos.com

Path	File Name/Mask	File Type
C:\ProgramData\Sophos\Sophos *\Logs\	*	Various
C:\ProgramData\Sophos\Sophos Anti-Virus\logs\	*	Various

REFERENCES:

https://support.sophos.com/support/s/article/KB-000033591?language=en_US
https://community.sophos.com/kb/en-us/133912

Symantec

https://www.norton.com

Path	File Name/Mask	File Type
C:\ProgramData\Symantec\Symantec Endpoint Protection*\Data\Logs\	*	Various
C:\Users\%user%\AppData\Local\Symantec\Symantec Endpoint Protection\Logs\	*	Various
C:\ProgramData\Symantec\Symantec Endpoint Protection*\Data\Quarantine\	*	Various
C:\ProgramData\Symantec\Symantec Endpoint Protection*\Data\CmnClnt\ccSubSDK\	*	Various
C:\ProgramData\Symantec\Symantec Endpoint Protection*\Data\	registrationInfo.xml	XML
C:\Windows\System32\winevt\logs\	Symantec Endpoint Protection Client.evtx	EVTX
C:\Windows.old\System32\winevt\logs\	Symantec Endpoint Protection Client.evtx	EVTX

REFERENCES:

https://malwaremaloney.blogspot.com/p/all-things-symantec.html
https://github.com/Beercow/SEPparser
https://github.com/Beercow/SEPparser/wiki/VBN-File-Format-Windows
http://hexacorn.com/d/DeXRAY.pl

Trend Micro

https://www.trendmicro.com

Path	File Name/Mask	File Type
C:\ProgramData\Trend Micro\	*	Various
C:\Program Files*\Trend Micro\Security Agent\Report\	*	Various
C:\Program Files*\Trend Micro\Security Agent\ConnLog\	*	Various

REFERENCES:

https://docs.trendmicro.com/en-us/documentation/article/trend-micro-apex-one-2019-server-online-help-trend_client_program_021

CLOUD STORAGE

Box

https://www.box.com

Path	File Name/Mask	File Type
C:\Users\%user%\Box\	*	Various
C:\Users\%user%\Box Sync\	*	Various
C:\Users\%user%\AppData\Local\Box\Box\	*	Various
C:\Users\%user%\AppData\Local\Box Sync\	*	Various

REFERENCES:

https://rb.gy/l2xzdg
https://rb.gy/ifwfhk
https://www.sans.org/blog/cloud-storage-acquisition-from-endpoint-devices
https://www.researchgate.net/publication/340816615_Forensic_Analysis_in_Cloud_Storage_with_Live_Forensics_in_Windows_Adrive_Case_Study
https://www.forensafe.com/blogs/box.html

Google Drive

https://www.google.com/drive/download

Path	File Name/Mask	File Type
C:\Users\%user%\Google Drive*\	*	Various
C:\Users\%user%\AppData\Local\Google\Drive\	*	Various
C:\Users\%user%\AppData\Local\Google\DriveFS\	*	Various

REFERENCES:

https://docplayer.net/2233170-Cloud-storage-forensics-mattia-epifani-sans-european-digital-forensics-summit-prague-7-october-2013.html
https://www.researchgate.net/publication/330319091_Cloud_Drives_Forensic_Artifacts_A_Google_Drive_Case
https://rb.gy/91zwro
https://www.atropos4n6.com/cloud-artifacts/google-drive-forensics/
https://www.atropos4n6.com/cloud-artifacts/google-drive-forensics-2/
https://www.forensafe.com/blogs/googledrive.html
https://forensafe.com/blogs/windows_google_drive.html
https://github.com/00010111/gMetaDataParse
https://github.com/net-protect/google-fs-recover
https://github.com/AmgdGocha/DriveFS-Sleuth
https://amgedwageh.medium.com/drivefs-sleuth-revealing-the-hidden-intelligence-82f043c452e4

Dropbox

https://www.dropbox.com

Path	File Name/Mask	File Type
C:\Users\%user%\Dropbox*\	*	Various
C:\Users\%user%\Dropbox*\.dropbox.cache\	*	Various
C:\Users\%user%\AppData\Local\Dropbox\	config.dbx	SQLite
C:\Users\%user%\AppData\Local\Dropbox\	filecache.dbx	SQLite
C:\Users\%user%\AppData\Local\Dropbox\	host.db	SQLite
C:\Users\%user%\AppData\Local\Dropbox\	info.json	JSON
C:\Users\%user%\AppData\Local\Dropbox\machine_storage\	tray-thumbnails.db	SQLite
C:\Users\%user%\AppData\Local\Dropbox\instance*\	aggregation.dbx	SQLite
C:\Users\%user%\AppData\Local\Dropbox\instance*\	avatarcache.db	SQLite
C:\Users\%user%\AppData\Local\Dropbox\instance*\	home.db	SQLite
C:\Users\%user%\AppData\Local\Dropbox\instance*\	icon.db	SQLite
C:\Users\%user%\AppData\Local\Dropbox\instance*\	sync_history.db	SQLite
C:\Users\%user%\AppData\Local\Dropbox\instance*\sync\	nucleus.sqlite3	SQLite
C:\Users\%user%\AppData\Local\Dropbox\machine_storage\	tray-thumbnails.db	SQLite
C:\Users\%user%\AppData\Roaming\Microsoft\Protect\	*	Various

REFERENCES:

https://www.marshall.edu/forensics/files/Treleven-Dropbox-Paper-FINAL.pdf
https://arxiv.org/pdf/1709.10395
https://docplayer.net/2233170-Cloud-storage-forensics-mattia-epifani-sans-european-digital-forensics-summit-prague-7-october-2013.html
https://www.sans.org/blog/digital-forensics-dropbox
https://www.researchgate.net/publication/342991973_Forensic_Analysis_of_Dropbox_Data_Remnants_on_Windows_10
https://www.atropos4n6.com/cloud-forensics/windows-10-artifacts-of-dropboxs-native-app-usage
https://www.atropos4n6.com/cloud-forensics/artifacts-of-dropbox-usage-on-windows-10-part-2

Microsoft OneDrive

https://www.microsoft.com/en-us/microsoft-365/onedrive/online-cloud-storage

Path	File Name/Mask	File Type
C:\Users\%user%\OneDrive*\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\OneDrive\logs\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\OneDrive\settings\	*	Various

REFERENCES:

https://www.sans.org/blog/cloud-storage-acquisition-from-endpoint-devices/
https://www.forensicfocus.com/forums/general/onedrive-files-on-demand-windows-10-storage-sense-settings
https://www.swiftforensics.com/2022/02/reading-onedrive-logs.html
https://www.forensafe.com/blogs/onedrive.html
https://github.com/Beercow/OneDriveExplorer