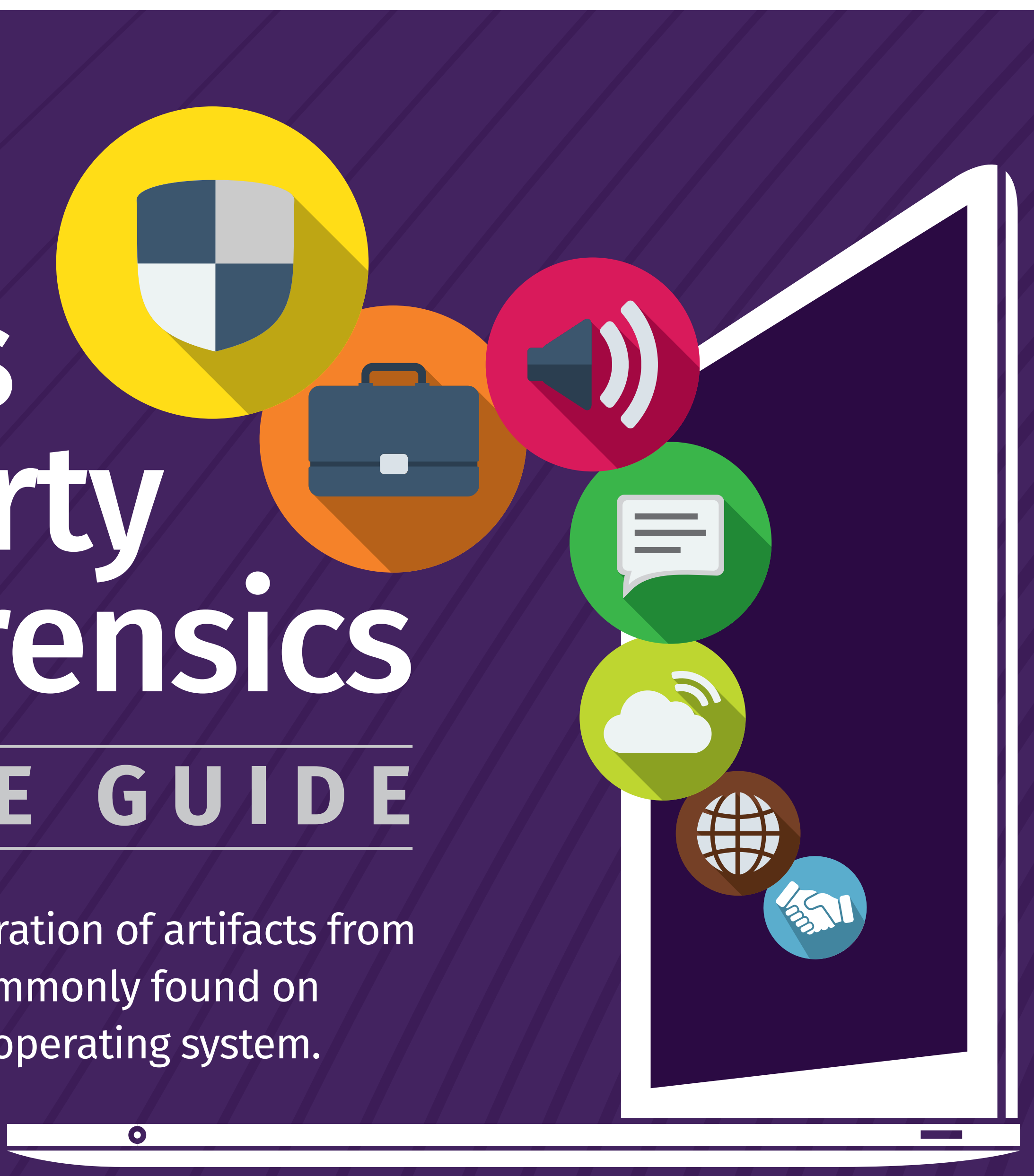
SANS

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.

DFPS_Windows-Apps-v1.4_02-23
This poster was created by Mattia Epifani (@mattiaep) with support of the SANS DFIR Faculty. ©2023 Mattia Epifani. All Rights Reserved.

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.

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

REFERENCES:
https://cyberforensicator.com/2017/03/01/how-to-find-passwords-for-encrypted-itunes-backups/
https://farleyforensics.com/2019/04/14/forensic-analysis-of-itunes-backups/
https://www.digitalforensics.com/blog/itunes-backup-forensic-analysis/

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

Antivirus

Avast

https://www.avast.com

Path	File Name/Mask	File Type
C:\ProgramData\Avast Software\Avast\Log\	*	Various
C:\ProgramData\Avast Software\Avast\Chest\	index.xml	XML
C:\Users\%user%\Avast Software\Avast\Log\	*	Various

REFERENCES:
https://businesshelp.avast.com/Content/Products/General_Help/LogLocations/BaseAntivirusLogs.htm

AVG

https://www.avg.com

Path	File Name/Mask	File Type
C:\ProgramData\AVG\Antivirus\log	*	Various
C:\ProgramData\AVG\Antivirus\report	*	Various

REFERENCES:
https://businesshelp.avast.com/Content/Products/General_Help/LogLocations/BaseAntivirusLogs.htm

Avira

https://www.avira.com

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

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

Bitdefender

https://www.bitdefender.com

Path	File Name/Mask	File Type
C:\ProgramData\Bitdefender\Endpoint Security\Logs\	*	Various
C:\ProgramData\Bitdefender\Desktop\Profiles\Logs\	*	Various
C:\Program Files*\Bitdefender*\	*	SQLite

REFERENCES:
https://anelshaer.medium.com/browsing-history-in-bitdefender-dbs-2d63ba940f92

ESET

https://www.eset.com

Path	File Name/Mask	File Type
C:\ProgramData\ESET\ESET NOD32 Antivirus\Logs\	*	Various

REFERENCES:
https://github.com/laciKE/EsetLogParser

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

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

Sophos

https://www.sophos.com

Path	File Name/Mask	File Type
C:\ProgramData\Sophos\Sophos *\Logs\	*	Various

REFERENCES:
https://support.sophos.com/support/s/article/KB-000033591?language=en_US

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

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

Windows Defender

https://www.microsoft.com/en-us/windows/comprehensive-security

Path	File Name/Mask	File Type
C:\ProgramData\Microsoft\Microsoft AntiMalware\Support\	*	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

REFERENCES:
https://knez.github.io/posts/how-to-extract-quarantine-files-from-windows-defender/

Browser

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*\	*	Various
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Bookmarks*	SQLIte
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Cookies*	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*\	QuotaManager*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Reporting and NEL*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	SecurePreferences	JSON
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Shortcuts*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Top Sites*	SQLite
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\	Trust Tokens*	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	SyncData.sqlite3	SQLite
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\	*	Various
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/an-overview-of-web-browser-forensics/
https://www.sans.org/blog/google-chrome-forensics/
http://cyberforensicator.com/wp-content/uploads/2017/02/20160919.pdf
https://forensicswiki.xyz/wiki/index.php?title=Google_Chrome
https://dfir.blog/chrome-values-lookup-tables/
https://dfir.blog/chrome-evolution/
https://www.sans.org/blog/forensically-mining-new-nuggets-of-google-chrome/
https://digitalinvestigation.wordpress.com/tag/snss/

Microsoft Edge (Legacy)

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

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Windows\WebCache\	*	Various

Microsoft Edge (Chromium)

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*\	Cookies*	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*\	Media History*	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*\	Shortcuts*	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	SyncData.sqlite3	SQLite
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*\File System\	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Edge \User Data*\Cache\	*	Various

REFERENCES:
https://www.forensicfocus.com/articles/chromium-based-microsoft-edge-from-a-forensic-point-of-view/
https://blog.group-ib.com/forensics_edge
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/

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
C:\Users\%user%\AppData\Local\Microsoft\Internet Explorer\Recovery	*	Various
C:\Users\%user%\AppData\Local\Microsoft\Internet Explorer\TabRoaming	*	Various

REFERENCES:
https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download
https://www.digitalforensics.com/blog/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://cyberforensicator.com/2017/02/07/windows-10-forensics/

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*	
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles\*\sessionstore-backups	Web Data*	SQLite
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/an-overview-of-web-browser-forensics/
https://www.foxtonforensics.com/browser-history-examiner/firefox-history-location

Opera Browser

https://www.opera.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\Opera Software\Opera Stable	*	Various
C:\Users\%user%\AppData\Roaming\Opera Software\Opera Stable	*	Various

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

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/

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\	*	Various

REFERENCES:

http://sersc.org/journals/index.php/IJAST/article/download/17649/8916/

https://core.ac.uk/download/pdf/214330118.pdf

AnyDesk

https://anydesk.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Roaming\AnyDesk\	*.trace	TXT
C:\Users\%user%\AppData\Roaming\AnyDesk\	Connection_trace.txt	TXT
C:\ProgramData\AnyDesk\	*.trace	TXT
C:\ProgramData\AnyDesk\	Connection_trace.txt	TXT

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

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/

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

IrfanView

https://www.irfanview.com

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

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

Microsoft Teams

https://www.microsoft.com/en-us/microsoft-teams/log-in

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

REFERENCES:

https://cyberforensicator.com/2020/04/16/looking-at-microsoft-teams-from-a-dfir-perspective/

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://www.datadigitally.com/2020/09/microsoft-teams-artifacts-and-chat-logs.html

https://www.alexbilz.com/post/2021-09-09-forensic-artifacts-microsoft-teams/

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://krknsec.com/2020/04/18/miscellaneous-windows-10-forensic-artifacts

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\	*	Various
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\	*	Various

REFERENCES:

https://www.champlain.edu/Documents/LCDI/ApplicationAnalysis_S17.pdf

Microsoft OneNote

https://www.onenote.com

Path	File Name/Mask	File Type
C:\Users\%user%\AppData\Local\Microsoft\OneNote\16.0	*	Various
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

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

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/

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

REFERENCES:

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

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/

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\	*	Various

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

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.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

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/

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/forensic-analysis-instant-messengers-desktop-applications/

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

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/forensic-analysis-instant-messengers-desktop-applications/

https://www.alexbilz.com/post/2021-01-29-forensic-artifacts-viber-desktop/

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	*	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/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

Zoom

https://zoom.us

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

REFERENCES:

https://www.sciencedirect.com/science/article/pii/S2666281721000019

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://cyberforensicator.com/2018/04/21/cloud-forensics-box/

https://dpmforensics.com/2017/03/12/cloud-forensics-box/

https://www.sans.org/blog/cloud-storage-acquisition-from-endpoint-devices

Dropbox

https://www.dropbox.com

Path	File Name/Mask	File Type
C:\Users\%user%\Dropbox*\	*	Various
C:\Users\%user%\AppData\Local\Dropbox\	info.json	JSON
C:\Users\%user%\AppData\Local\Dropbox\	filecache.dbx	SQLite
C:\Users\%user%\AppData\Local\Dropbox\	config.dbx	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://www.scribd.com/document/228562978/Cloud-Storage-Forensics-Mattia-Eppifani

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/

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://www.scribd.com/document/228562978/Cloud-Storage-Forensics-Mattia-Eppifani

https://www.researchgate.net/publication/330319091_Cloud_Drives_Forensic_Artifacts_A_Google_Drive_Case

https://cyberforensicator.com/2018/10/19/cloud-forensics-google-drive/

https://www.atropos4n6.com/cloud-artifacts/google-drive-forensics/

https://www.atropos4n6.com/cloud-artifacts/google-drive-forensics-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/

@SANSForensics dfir.to/DFIRCast dfir.to/LinkedIn

SANS DFIR CURRICULUM

DIGITAL FORENSICS

FOR308
Digital Forensics Essentials

FOR498
Digital Acquisition and Rapid Triage
GBFA

FOR500
Windows Forensic Analysis
GCFE

FOR518
Mac and iOS Forensic Analysis & Incident Response
GIME

FOR585
Smartphone Forensic Analysis In-Depth
GASF

INCIDENT RESPONSE & THREAT HUNTING

FOR508
Advanced Incident Response, Threat Hunting & Digital Forensics
GCFA

FOR509
Enterprise Cloud Forensics & Incident Response
GCFR

FOR528
Ransomware for Incident Responders

FOR532
Enterprise Memory Forensics In-Depth

FOR572
Advanced Network Forensics: Threat Hunting, Analysis & Incident Response
GNFA

FOR578
Cyber Threat Intelligence
GCTI

FOR608
Enterprise-Class Incident Response & Threat Hunting

FOR610
REM: Malware Analysis Tools & Techniques
GREM

FOR710
Reverse-Engineering Malware: Advanced Code Analysis

SEC504
Hacker Tools, Techniques & Incident Handling
GCIH