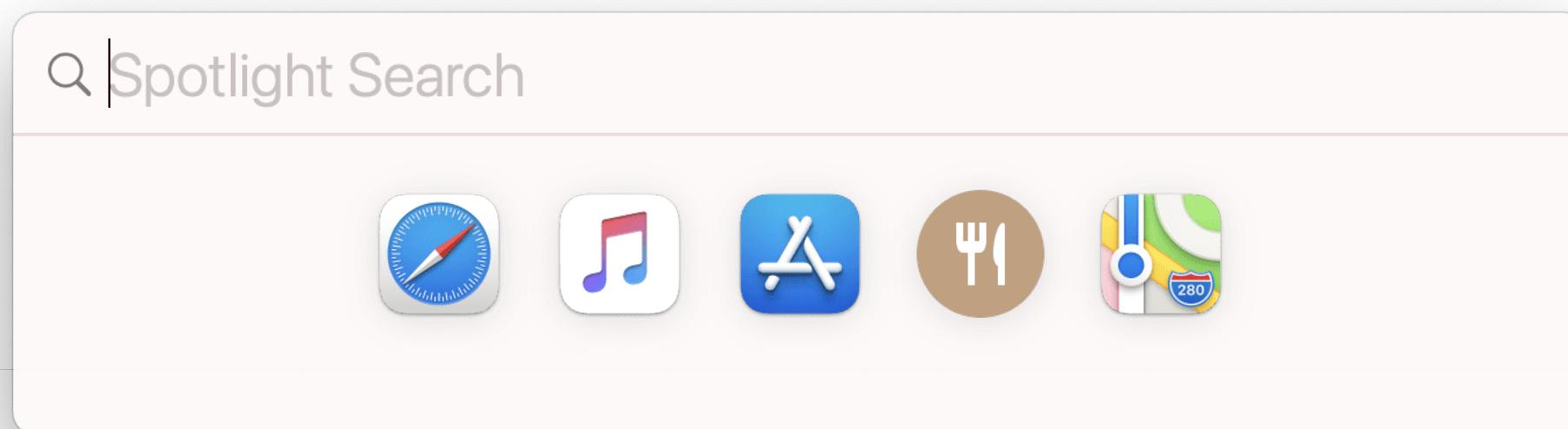


Spotlight – Forensic Goldmine in iOS & macOS

Yogesh Khatri

Associate Professor, Program Director

Champlain College



About

- Yogesh Khatri
- Champlain College
 - Program Director – Digital Forensics
 - Associate Professor
- *15+ years of Forensics & IR*
 - *Industry & Academia*
- Author & Maintainer for *mac_apt – Artifact Parsing Tool*
 - And several standalone scripts/programs for forensic processing



@swiftforensics

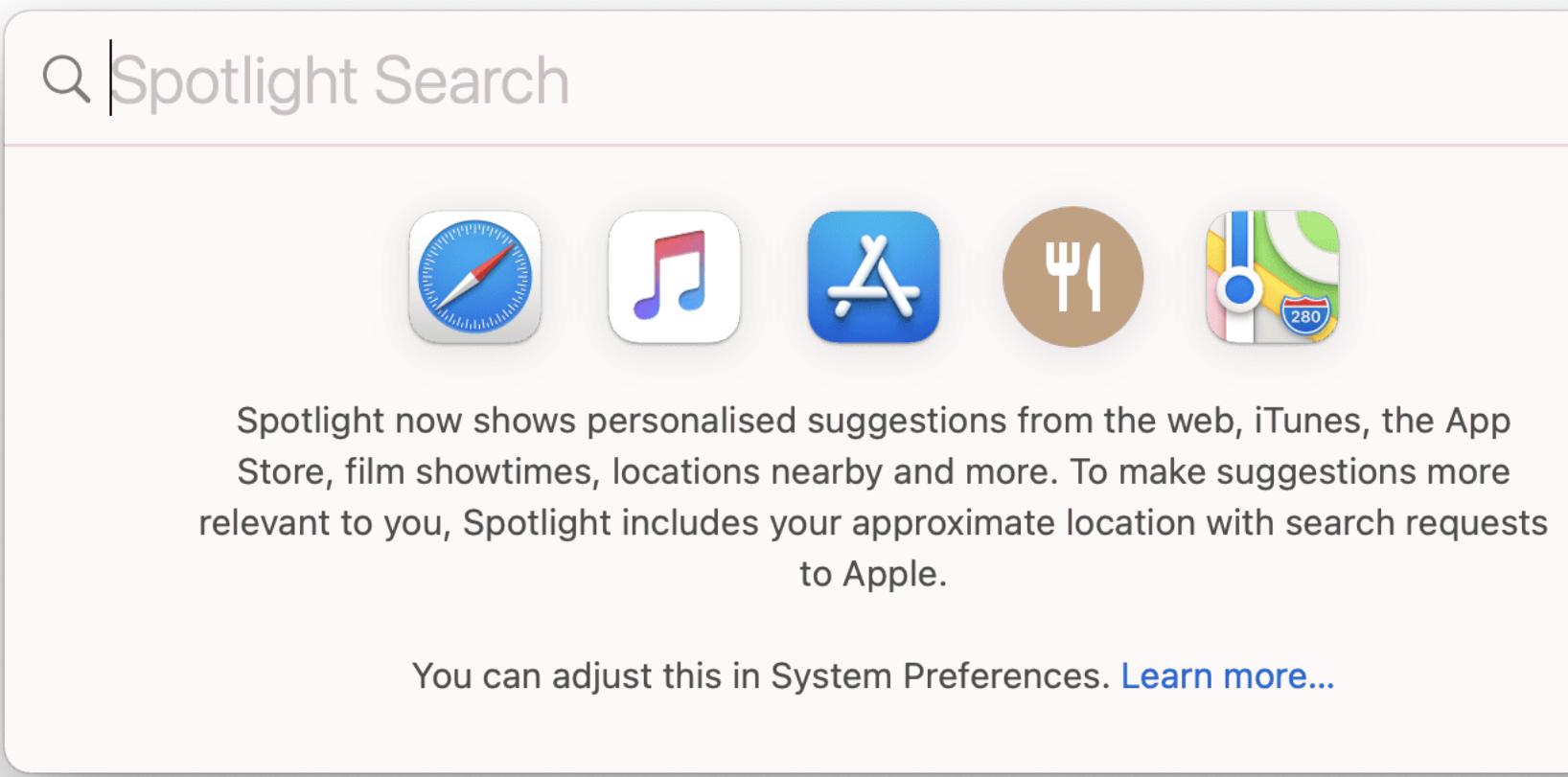


<https://swiftforensics.com>

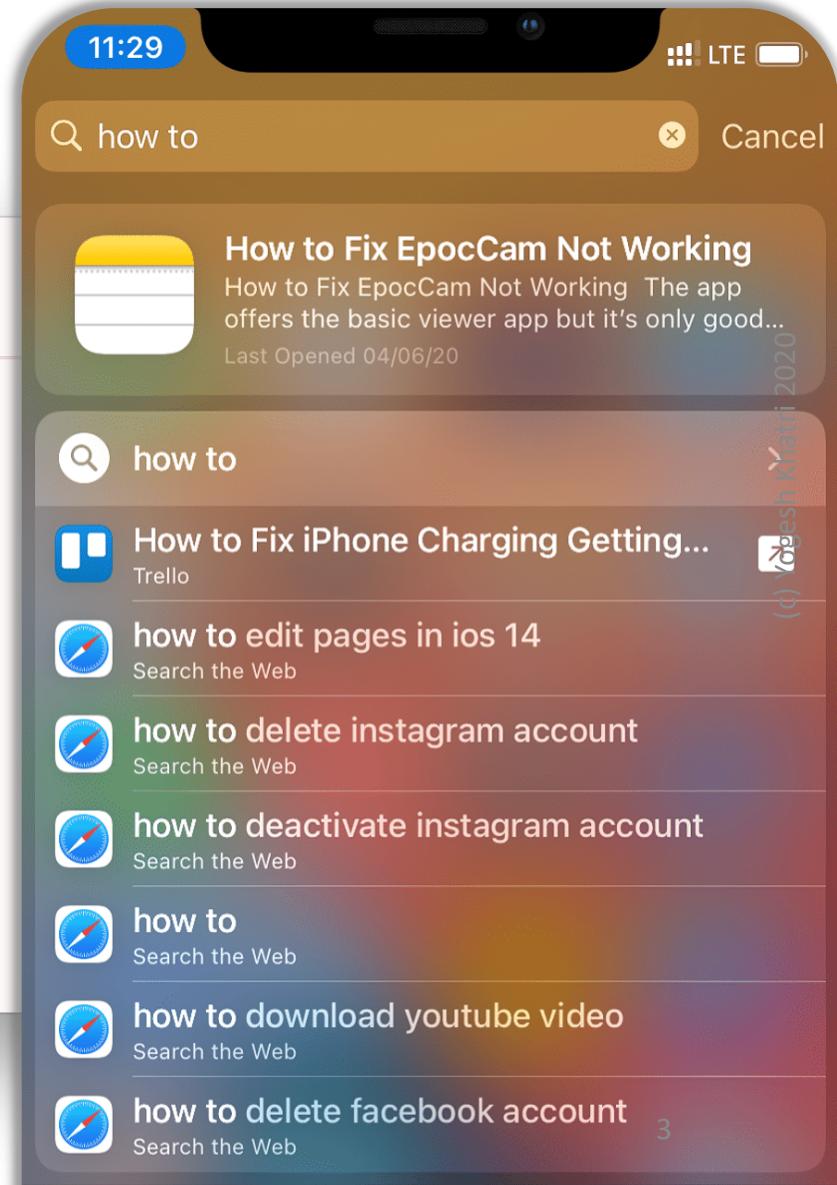


<https://github.com/ydkhatri>

What is Spotlight?



The screenshot shows the macOS Spotlight search interface. At the top left is a search bar with the placeholder "Spotlight Search". Below it are five app icons: Safari, iTunes Store, App Store, Wallet, and Maps. A text block below the icons reads: "Spotlight now shows personalised suggestions from the web, iTunes, the App Store, film showtimes, locations nearby and more. To make suggestions more relevant to you, Spotlight includes your approximate location with search requests to Apple." At the bottom, it says "You can adjust this in System Preferences. [Learn more...](#)".



The screenshot shows an iPhone search results screen with a search bar at the top containing "how to". Below the search bar is a list of suggestions. Each suggestion includes a small icon, the search term, a snippet of text, and the source. The suggestions are: "How to Fix EpocCam Not Working" (last opened 04/06/20), "how to" (Trello), "How to Fix iPhone Charging Getting..." (Trello), "how to edit pages in ios 14" (Search the Web), "how to delete instagram account" (Search the Web), "how to deactivate instagram account" (Search the Web), "how to" (Search the Web), "how to download youtube video" (Search the Web), and "how to delete facebook account" (Search the Web). A small "3" is visible in the bottom right corner of the list.

Prior research – Tooling (and research) history

- 2014 – 504ENSICS – Spotlight Inspector tool
 - *Free (but not open source) tool, withdrawn soon after*
- 2018 – Yogesh Khatri – Spotlight parser tool
 - <https://www.swiftforensics.com/2018/08/parsing-spotlight-database.html>
 - https://github.com/ydkhatri/spotlight_parser , https://github.com/ydkhatri/mac_apt
- 2019 – Yogesh Khatri – Digital Investigation Journal paper
 - Investigating spotlight internals to extract metadata
 - <https://www.sciencedirect.com/science/article/abs/pii/S1742287618300860>
- 2019 – Atwal, Scanlon, Le-Khac - Digital Investigation Journal paper
 - Shining a light on Spotlight: Leveraging Apple's desktop search utility to recover deleted file metadata on macOS
 - <https://www.sciencedirect.com/science/article/pii/S1742287619300295>
- 2019 – Vico Marziale (Blackbag Technologies) – Illuminate Tool
 - Shedding Light on the macOS Spotlight Desktop Search Service - SANS DFIR Summit 2019 -
<https://www.youtube.com/watch?v=Y-vMp3aRIUk>
- Other researchers have talked about accessing data from spotlight since at least 2012..
 - Sara Edwards, Lee Whitfield, Howard Oakley, J. Varsalone, ..

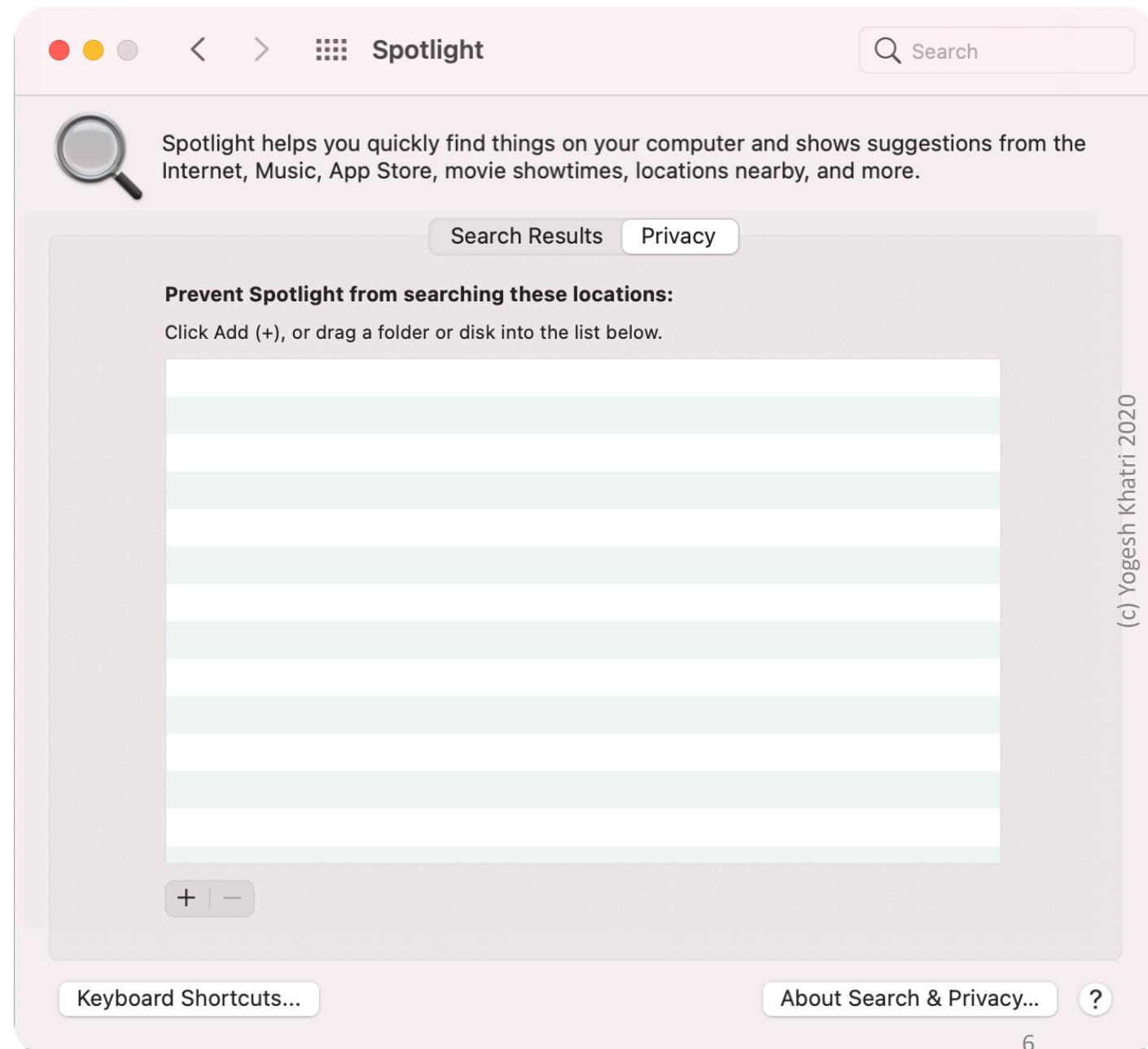
Today's agenda

- Brief overview of Spotlight
 - Database locations
 - Types of data stored
 - macOS & iOS variants
- Extracting and reviewing the information
 - How to interpret the data?
 - Shiny tool demos and walkthroughs



What is indexed?

- Everything, by default
- Exclusions can be defined
 - *Hardly ever used!*



Artifact Location on macOS – One per volume

- At volume's root at `/.Spotlight-V100/`
- On Catalina (10.15) and above (11.0), this folder is located elsewhere
 - DATA volume, same location
 - On live system, this can be accessed via `/System/Volumes/Data`
 - SYSTEM volume
 - `/private/var/db/Spotlight-V100/BootVolume`

```
Yogesh-Khatri:~ yogesh$ ls -al /System/Volumes/Data
total 3418
drwxr-xr-x@ 30 root      wheel      960 Nov 19 13:55 .
drwxr-xr-x   14 root      wheel      448 Jan  1  2020 ..
-rw-rw-r--    1 root      admin     6148 Sep 10  2019 .DS_Store
d--x--x--x    9 root      wheel      288 Nov 23 20:47 .DocumentRevisions-
...
drwx-----  5 root      wheel     160 May 17  2019 .Spotlight-V100
...
```



The folder `".Spotlight-V100"` can't be opened because you don't have permission to see its contents.

OK

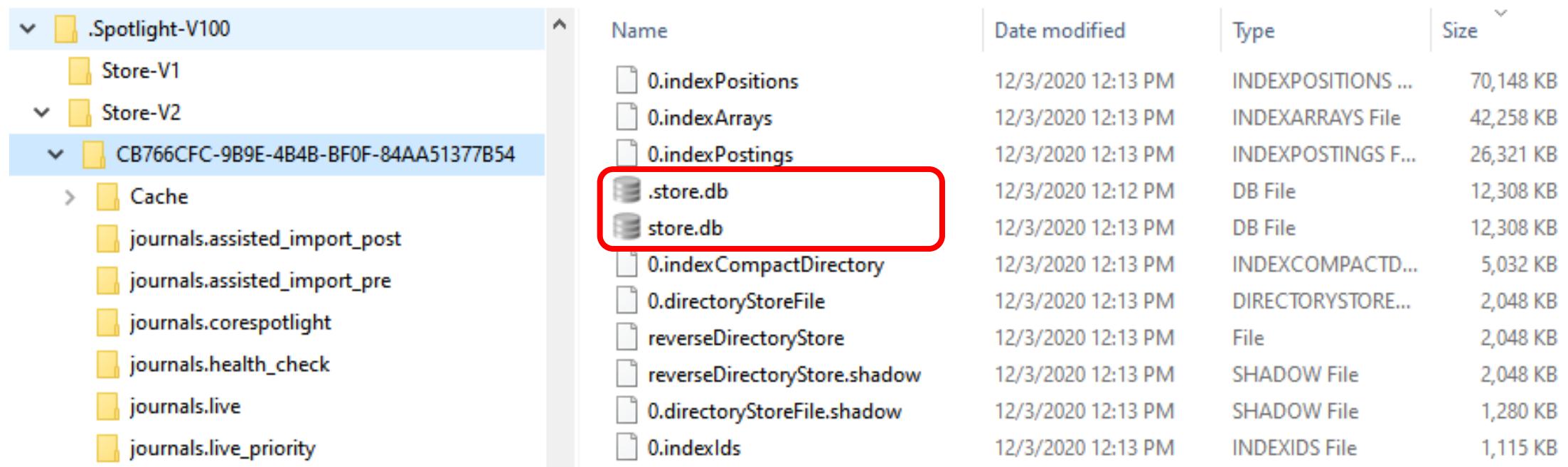
The per volume database

The screenshot shows a file explorer window with two panes. The left pane displays a directory structure under '.Spotlight-V100'. A red arrow points from the 'Cache' folder in this structure to the 'VolumeConfiguration.plist' file in the right pane. The right pane is a table viewer showing the contents of 'VolumeConfiguration.plist'. A red box highlights the file name in the list view, and another red box highlights the volume UUID 'CB766CFC-9B9E-4B4B-BF0F-84AA51377B54' in the detailed view.

Name	Date modified	Type	Size
Store-V1	12/3/2020 12:12 PM	File folder	
Store-V2	12/3/2020 12:12 PM	File folder	
VolumeConfiguration.plist	12/3/2020 12:12 PM	Property List File	5 KB

Key	Type	Value
Root	dict	
Annotations	dict	
ConfigurationCreationDate	date	2019-09-19 12:56:21
ConfigurationCreationVersion	string	Version 10.13.5 (Build 17F77)
ConfigurationModificationDate	date	2019-09-19 12:56:22
ConfigurationModificationVersion	string	Version 10.13.5 (Build 17F77)
ConfigurationVolumeUUID	string	D0E211F3-FE12-38CE-A9CF-D58382723D3A
ConfigurationWriteback	boolean	false
Exclusions	array	
Options	dict	
ConfigurationType	string	Default
Stores	dict	
CB766CFC-9B9E-4B4B-BF0F-84AA51377B54	dict	
CreationDate	date	2019-09-19 12:56:21
CreationVersion	string	Version 10.13.5 (Build 17F77)
IndexVersion	integer	95
PartialPath	string	/
PolicyDate	date	2019-09-19 12:56:22
PolicyLevel	string	kMDConfigSearchLevelReadWrite
PolicyProcess	string	STORE_ADD
PolicyVersion	string	Version 10.13.5 (Build 17F77)

The per volume database..



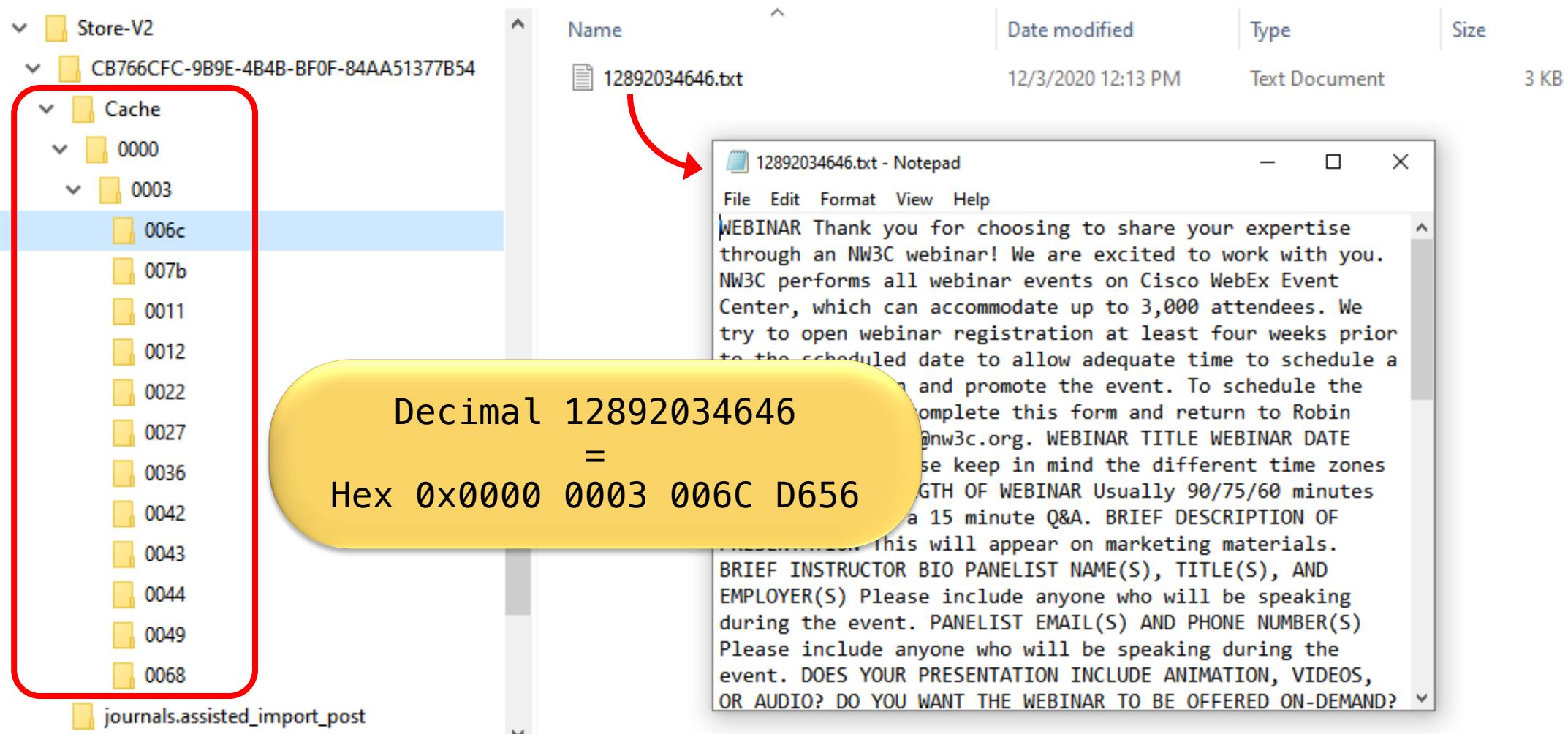
A screenshot of a Windows File Explorer window. The left pane shows a tree view of a volume named '.Spotlight-V100'. Underneath it, several folders are listed: 'Store-V1', 'Store-V2', 'CB766CFC-9B9E-4B4B-BF0F-84AA51377B54', 'Cache', 'journals.assisted_import_post', 'journals.assisted_import_pre', 'journals.corespotlight', 'journals.health_check', 'journals.live', and 'journals.live_priority'. The folder 'CB766CFC-9B9E-4B4B-BF0F-84AA51377B54' is selected. The right pane displays a detailed list of files from this folder. The columns are 'Name', 'Date modified', 'Type', and 'Size'. The files listed are: '0.indexPositions' (12/3/2020 12:13 PM, INDEXPOSITIONS File, 70,148 KB), '0.indexArrays' (12/3/2020 12:13 PM, INDEXARRAYS File, 42,258 KB), '0.indexPostings' (12/3/2020 12:13 PM, INDEXPOSTINGS File, 26,321 KB), '.store.db' (12/3/2020 12:12 PM, DB File, 12,308 KB), 'store.db' (12/3/2020 12:13 PM, DB File, 12,308 KB), '0.indexCompactDirectory' (12/3/2020 12:13 PM, INDEXCOMPACTD... File, 5,032 KB), '0.directoryStoreFile' (12/3/2020 12:13 PM, DIRECTORYSTORE... File, 2,048 KB), 'reverseDirectoryStore' (12/3/2020 12:13 PM, File, 2,048 KB), 'reverseDirectoryStore.shadow' (12/3/2020 12:13 PM, SHADOW File, 2,048 KB), '0.directoryStoreFile.shadow' (12/3/2020 12:13 PM, SHADOW File, 1,280 KB), and '0.indexIds' (12/3/2020 12:13 PM, INDEXIDS File, 1,115 KB). The files '.store.db' and 'store.db' are highlighted with a red rectangular box.

Name	Date modified	Type	Size
0.indexPositions	12/3/2020 12:13 PM	INDEXPOSITIONS File	70,148 KB
0.indexArrays	12/3/2020 12:13 PM	INDEXARRAYS File	42,258 KB
0.indexPostings	12/3/2020 12:13 PM	INDEXPOSTINGS File	26,321 KB
.store.db	12/3/2020 12:12 PM	DB File	12,308 KB
store.db	12/3/2020 12:13 PM	DB File	12,308 KB
0.indexCompactDirectory	12/3/2020 12:13 PM	INDEXCOMPACTD... File	5,032 KB
0.directoryStoreFile	12/3/2020 12:13 PM	DIRECTORYSTORE... File	2,048 KB
reverseDirectoryStore	12/3/2020 12:13 PM	File	2,048 KB
reverseDirectoryStore.shadow	12/3/2020 12:13 PM	SHADOW File	2,048 KB
0.directoryStoreFile.shadow	12/3/2020 12:13 PM	SHADOW File	1,280 KB
0.indexIds	12/3/2020 12:13 PM	INDEXIDS File	1,115 KB

store.db has a proprietary format

- Not discussing internals / details here

The per volume database..



Artifact Location on macOS – Per user db

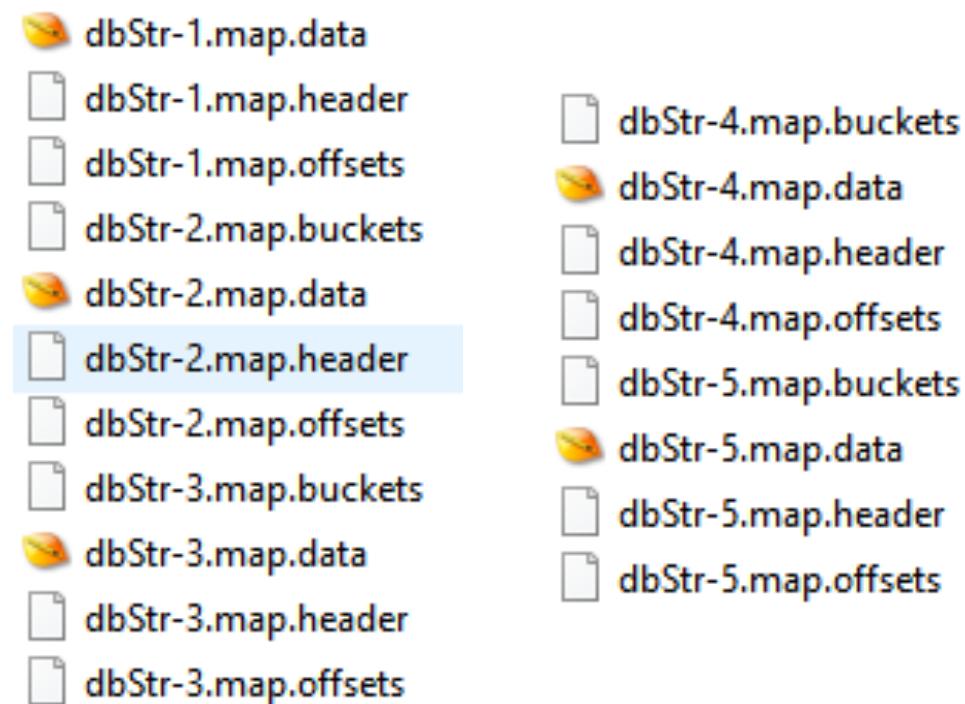
- In user's profile folder

`~/Library/Metadata/CoreSpotlight/index.spotlightV3/`

- `store.db`
- `.store.db`

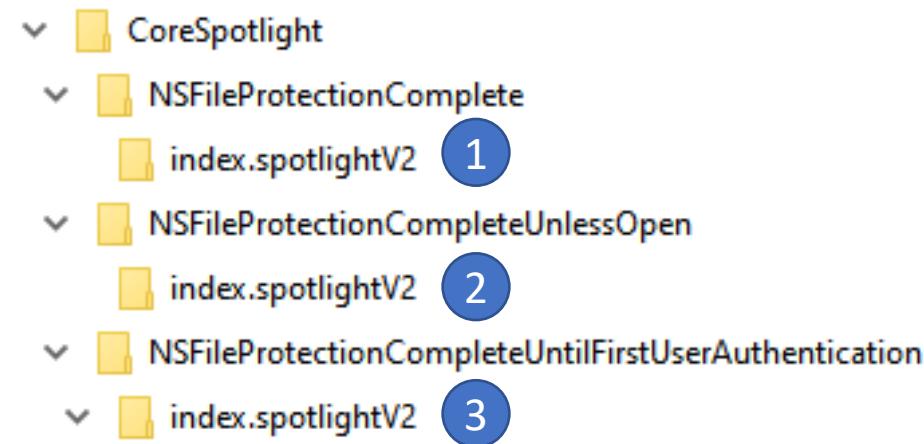
- Database dependencies

- `dbStr-x.map.xxxxx` files



Artifact location on iOS

- /private/var/mobile/Library/Spotlight/CoreSpotlight/*/index.spotlightV2/
 - store.db
 - .store.db



Name	Date modified
4e8a08b3a4bacb2b.img	8/6/2020 7:11 PM
4e8a08b3a4c4ef05.img	4/24/2020 1:45 PM
4e8a08b3a7ae2c19.img	8/6/2020 7:11 PM
4e8a08b3a8c609dc.img	8/14/2020 1:15 PM
4e8a08b3a34db9ca.img	8/6/2020 7:11 PM

The table shows a list of files in the 'Cache' folder of the 'NSFileProtectionCompleteUntilFirstUserAuthentication' directory. The files are listed by name and date modified. The 'Cache' folder itself is highlighted with a blue selection bar at the bottom of the left pane.

Information from per volume database

- Info about Files / Folders
 - Date – Created, Modified, Added
 - Other Dates
 - Last usage
 - Last viewed
 - Downloaded date
 - Item Kind
 - UID & GID
 - Logical & Physical size
 - Other attributes
 - Item Description
- Download url
- Doc & Media metadata (EXIF, ID3, ..)
 - Height/Width
 - Lat/Long
 - Codec
 - Author(s)

Inode_Num --> 12886072633

Store_ID --> 76856

Parent_Inode_Num --> 12885640371

Last_Updated --> 2020-12-02 20:06:05.792257

_kMDItemContentChangeDate --> 2019-10-17
04:36:37.020195

_kMDItemCreationDate --> 2019-10-17 04:36:36.730605

_kMDItemFileName --> summit_archive_1528404628.pdf

_kMDItemOwnerGroupID --> 20

_kMDItemOwnerUserID --> 501

kMDItemAuthors --> Yogesh Khatri

kMDItemContentCreationDate --> 2019-10-17
04:36:36.730605

kMDItemContentModificationDate --> 2019-10-17
04:36:37.020195

kMDItemContentType --> com.adobe.pdf

kMDItemCreator --> Microsoft® PowerPoint® 2016

kMDItemDateAdded --> 2019-10-17 04:36:36.730605

kMDItemKind --> PDF document

kMDItemLastUsedDate --> 2019-10-17 17:00:16.939266

kMDItemLogicalSize --> 3542769

kMDItemNumberOfPages --> 28

kMDItemPageHeight --> 450.0

kMDItemPageWidth --> 800.0399780273438

kMDItemPhysicalSize --> 3543040

kMDItemSecurityMethod --> None

kMDItemTitle --> mac_apt

kMDItemUseCount --> 7

kMDItemUsedDates --> 2019-10-17 04:00:00

kMDItemWhereFroms --> <https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1528404628.pdf>

Data from spotlight parser
(some fields have been removed to fit data here)

Inode_Num --> 12889266235
Store_ID --> 128692
Parent_Inode_Num --> 12889266234
Last_Updated --> 2020-12-02 20:06:06.154310
_kMDItemFileName --> IMG_0002.PNG
kMDItemBitsPerSample --> 32
kMDItemColorSpace --> RGB
kMDItemComment --> Screenshot
kMDItemContentCreationDate --> 2020-05-08 16:55:08
kMDItemContentModificationDate --> 2020-05-08 16:55:25.782376
kMDItemContentType --> public.png
kMDItemContentTypeTree --> public.png, public.image, public.data, public.item, public.content
kMDItemDateAdded --> 2020-05-08 16:55:26.071326
kMDItemDisplayName --> IMG_0002.PNG
kMDItemDownloadedDate --> 2020-05-08 16:55:26.097162
kMDItemKind --> PNG image
kMDItemLogicalSize --> 213480
kMDItemOrientation --> 1
kMDItemOriginApplicationIdentifier --> com.apple.messages
kMDItemOriginSenderHandle --> hazelhill010@icloud.com
kMDItemPhysicalSize --> 217088
kMDItemPixelCount --> 3145728
kMDItemPixelHeight --> 2048
kMDItemPixelWidth --> 1536

kMDItemProfileName --> sRGB IEC61966-2.1
kMDItemTransportAccount --> E:janesmithmacfor@icloud.com
kMDItemTransportService --> iMessage
kMDItemUserSharedReceivedDate --> 2020-05-08 16:55:26.099445
kMDItemUserSharedReceivedRecipient --> janesmithmacfor@icloud.com
kMDUserSharedReceivedRecipientHandle --> janesmithmacfor@icloud.com
kMDItemUserSharedReceivedSender --> hazelhill010@icloud.com
kMDItemUserSharedReceivedSenderHandle --> hazelhill010@icloud.com
kMDItemUserSharedReceivedTransport --> com.apple.messages
kMDItemWhereFroms --> hazelhill010@icloud.com, Received via
Messages file transfer

Attachment from iMessage
-
Data from spotlight parser (*some fields have been removed to fit data here*)

Inode_Num --> 12889266299

Flags --> 0

Store_ID --> 141374

Parent_Inode_Num --> 12889266082

Last_Updated --> 2020-12-02 20:06:06.354879

_kMDItemFileName --> hazelhill010@icloud.com on 2020-05-08 at 12.36.46.ichat

_kMDItemIsExtensionHidden --> 1

_kMDItemLocked --> 1

_kMDItemOwnerGroupID --> 20

_kMDItemOwnerUserID --> 501

com_apple_metadata_modtime --> 610650577.177143

kMDItemAuthorAddresses --> e:janesmithmacfor@icloud.com

kMDItemContentCreationDate --> 2020-05-08 16:36:46.134475

kMDItemContentModificationDate --> 2020-05-08 17:09:37.177143

kMDItemContentType --> com.apple.ichat.transcript

kMDItemDateAdded --> 2020-05-08 17:09:52.282463

kMDItemDeliveryType --> iMessage

kMDItemDisplayName --> hazelhill010@icloud.com on 2020-05-08 at 12.36.46

kMDItemKind --> Chat transcript

kMDItemLastUsedDate --> 2020-05-08 16:36:44.388566

kMDItemLogicalSize --> 226689

kMDItemPhysicalSize --> 229376

kMDItemRecipientAddresses --> hazelhill010@icloud.com

kMDItemUseCount --> 2

kMDItemUsedDates --> 2020-05-08 04:00:00

iMessage parsed out

-
Data from spotlight parser
(some fields have been removed to fit data here)

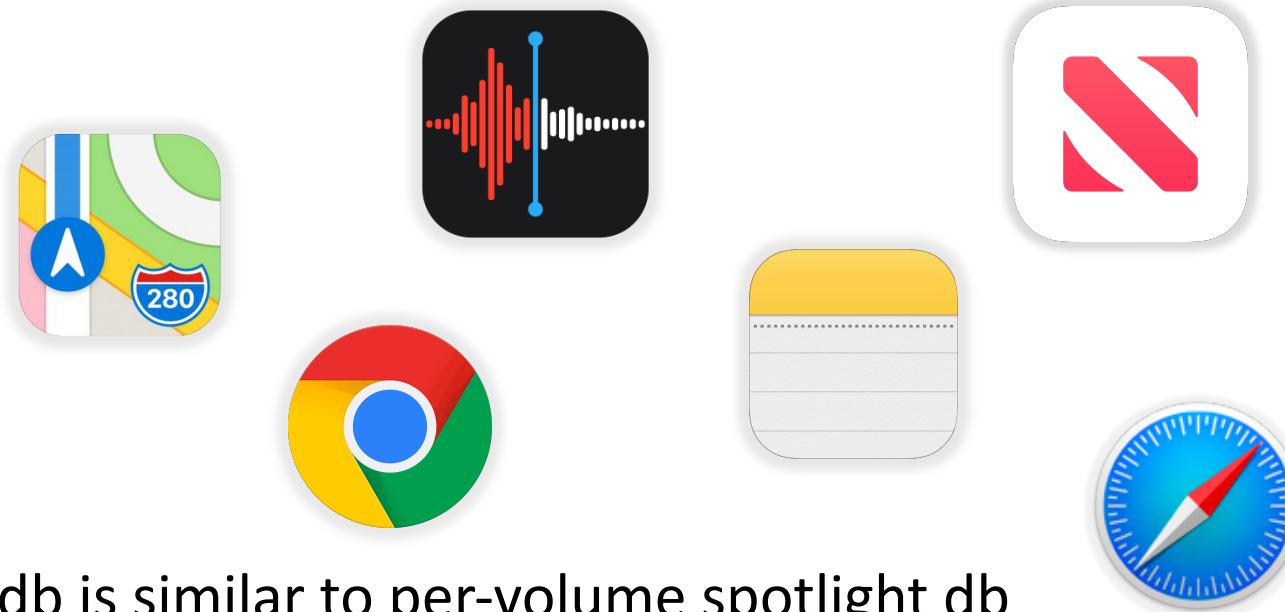
Safari history hacked into Spotlight.. earlier

- Prior to macOS 10.13, files could be seen under
~/Library/Caches/Metadata/Safari/
- These .webhistory files represent urls visited

```
-rw-r--r-- 1 yogesh staff 162 Dec 11 2017 https:%2F%2Fwww.bhphotovideo.com%2Ffind%2FthankYouSurvey.jsp.webhistory
-rw-r--r-- 1 yogesh staff 156 Jan 11 2018 https:%2F%2Fwww.binaryhexconverter.com%2Fdecimal-to-hex-converter.webhistory
-rw-r--r-- 1 yogesh staff 105 Jun 10 16:16 https:%2F%2Fwww.bing.com%2F.webhistory
-rw-r--r-- 1 yogesh staff 92 Apr 11 2018 https:%2F%2Fwww.blogger.com%2F?tab=mj.webhistory
-rw-r--r-- 1 yogesh staff 131 Apr 11 2018 https:%2F%2Fwww.blogger.com%2Fblogger.g?tab=mj%23welcome.webhistory
-rw-r--r-- 1 yogesh staff 121 Apr 11 2018 https:%2F%2Fwww.blogger.com%2Fblogger.g?tab=mj.webhistory
-rw-r--r-- 1 yogesh staff 113 Nov 30 2017 https:%2F%2Fwww.blogger.com%2Fprofile%2F08966595734678290320.webhistory
-rw-r--r-- 1 yogesh staff 241 Feb 16 2018 https:%2F%2Fwww.bloomberg.com%2Fnews%2Farticles%2F2018-02-16%2Fgoogle-firing-of-d
-rw-r--r-- 1 yogesh staff 244 Feb 16 2018 https:%2F%2Fwww.bloomberg.com%2Fnews%2Farticles%2F2018-02-16%2Fu-s-charges-13-rus
-rw-r--r-- 1 yogesh staff 231 Aug 13 08:52 https:%2F%2Fwww.bloomberg.com%2Fnews%2Farticles%2F2018-08-09%2Fcryptokidnapping-o
-rw-r--r-- 1 yogesh staff 250 Aug 13 08:59 https:%2F%2Fwww.bloomberg.com%2Fnews%2Farticles%2F2018-08-12%2Flira-extends-retre
-rw-r--r-- 1 yogesh staff 203 Apr 23 20:44 https:%2F%2Fwww.booking.com%2Fdirections.en-us.html?hotel_id=56473&aid=389181.web
-rw-r--r-- 1 yogesh staff 122 May 13 16:24 https:%2F%2Fwww.burlingtonfreepress.com%2F.webhistory
-rw-r--r-- 1 yogesh staff 126 May 13 16:26 https:%2F%2Fwww.burlingtonfreepress.com%2Fbiz%2F.webhistory
-rw-r--r-- 1 yogesh staff 134 May 13 16:26 https:%2F%2Fwww.burlingtonfreepress.com%2Fnews%2F.webhistory
-rw-r--r-- 1 yogesh staff 148 Jan 3 2018 https:%2F%2Fwww.burlingtonfreepress.com%2Fsection%2Fglobal%2Fnation-now%2F.webhis
-rw-r--r-- 1 yogesh staff 138 May 13 16:26 https:%2F%2Fwww.burlingtonfreepress.com%2Fsports%2F.webhistory
```

Solution – a db not linked to the filesystem

- Per-user or iOS spotlight db
 - 3rd party apps can add their own fields (metadata types)
 - Developers can implement in-app searches for any kind of data now
 - Used by
 - Notes app
 - Maps app
 - Apple Mail
 - iMessage (on iOS)
 - Safari
 - Chrome (on iOS)
 - Voice Memos app
 - ..
 - Internal format of store.db is similar to per-volume spotlight db



Tools please..

- Spotlight parser
 - <https://github.com/ydkhatri/spotlight-parser>
 - Not updated (yet!) to write to an sqlite database!
- `mac_apt_artifact_only` script to work on individual spotlight dbs
 - Part of `mac_apt` suite
 - https://github.com/ydkhatri/mac_apt
 - Lots of functionality but we only need the SPOTLIGHT plugin
 - Recent functionality includes creating views for easy review



GitHub - ydkhatri/mac_apt: macOS Artifact Parsing Tool

github.com/ydkhatri/mac_apt

Search or jump to... / Pull requests Issues Marketplace Explore

Unwatch 37 Star 291 Fork 51

Code Issues 4 Pull requests 1 Actions Projects Wiki Security Insights Settings

master 1 branch 16 tags Go to file Add file Code

ydkhatri version change in readme 7ad35bb 2 hours ago 421 commits

Libraries_For_Windows python 3.8 compiled libs for windows 3 months ago

Licenses added license 17 months ago

other_dependencies Add Encryption support and more (#39) 6 months ago

plugins Add views for Spotlight ios/user db output 2 hours ago

.gitignore gitignore updated 4 months ago

AUTHORS.md Update AUTHORS.md 4 months ago

CHANGES.txt type fix 6 months ago

LICENSE.txt Rename LICENSE to LICENSE.txt 3 years ago

README.md version change in readme 2 hours ago

extract_apfs_fs.py Version change to 0.9.dev 2 hours ago

About

macOS Artifact Parsing Tool

swiftforensics.com

dfir forensics macos

Readme

MIT License

Releases 16

20201205 Latest 12 minutes ago

+ 15 releases

Packages 21

No packages published

Running mac_apt_artifact_only

```
C:\> mac_apt_artifact_only.exe -i P:\ios_spotlight1\store.db -o W:\output SPOTLIGHT
```

Output path was : W:\output

MAIN-INFO-Started macOS Artifact Parsing Tool - Artifact Only mode, version 0.9.dev

MAIN-INFO-Dates and times are in UTC unless the specific artifact being parsed saves it as local time!

MAIN-INFO-----

MAIN-INFO-Running plugin SPOTLIGHT

MAIN-INFO-----

MAIN.SPOTLIGHT-INFO-Module Started as standalone

MAIN.SPOTLIGHT-INFO-Now processing file P:\ios_spotlight1\store.db

MAIN.SPOTLIGHT-INFO-Processing P:\ios_spotlight1\store.db

MAIN.SPOTLIGHT-INFO-Creating output folder for spotlight at W:\output\SPOTLIGHT_DATA

MAIN.HELPERS.SPOTLIGHT_FILTER-INFO-24 views added for table Spotlight-store.db

MAIN-INFO-----

MAIN-INFO-Finished in time = 00:00:01

MAIN-INFO-Review the Log file and report any ERRORS or EXCEPTIONS to the developers

Plugin to run

Script options

-i <PATH_TO_STORE.DB>
-o <OUTPUT_FOLDER>

Output database

Table representing
parsed data from
store.db

Views created from table
One view per App (BundleID)

*App-based views are only on User/iOS databases.
Volume databases can't be split like this*

DB Browser for SQLite - D:\nw3c\output\bigsur\mac_apt.db

File Edit View Tools Help

New Database Open Database Write Changes

Database Structure Browse Data Edit Pragmas Execute SQL

Create Table Create Index Print

Name	Type
Tables (1)	
Spotlight-store.db	
Indices (0)	
Views (6)	
Spotlight-store.db_com.apple.Notes	
Spotlight-store.db_com.apple.Safari	
Spotlight-store.db_com.apple.mail	
Spotlight-store.db_com.apple.news	
Spotlight-store.db_com.apple.reminders	
Spotlight-store.db_com.apple.searchd	

Demo



main ▾

[spotlight_queries / queries / com.apple.mail.md](#)[Go to file](#)

...



ydkhatri Create com.apple.mail.md

Latest commit 61bf9af 11 hours ago

[History](#)

1 contributor

8 lines (7 sloc) | 350 Bytes

[Raw](#)[Blame](#)

(c) Yogesh Khatri 2020

```
SELECT _kMDItemExternalID, kMDItemContentCreationDate, kMDItemSubject, com_apple_mail_dateLastViewed,  
com_apple_mail_read, kMDItemUseCount,  
_kMDItemSnippet, kMDItemAuthorEmailAddresses, kMDItemAuthors, kMDItemPrimaryRecipientEmailAddresses  
FROM "Spotlight-store.db" -- Change db name here to yours  
WHERE kMDItemKind LIKE "email message"
```



com.apple.mobilesafari.md

Create com.apple.mobilesafari.md

10 hours ago

25

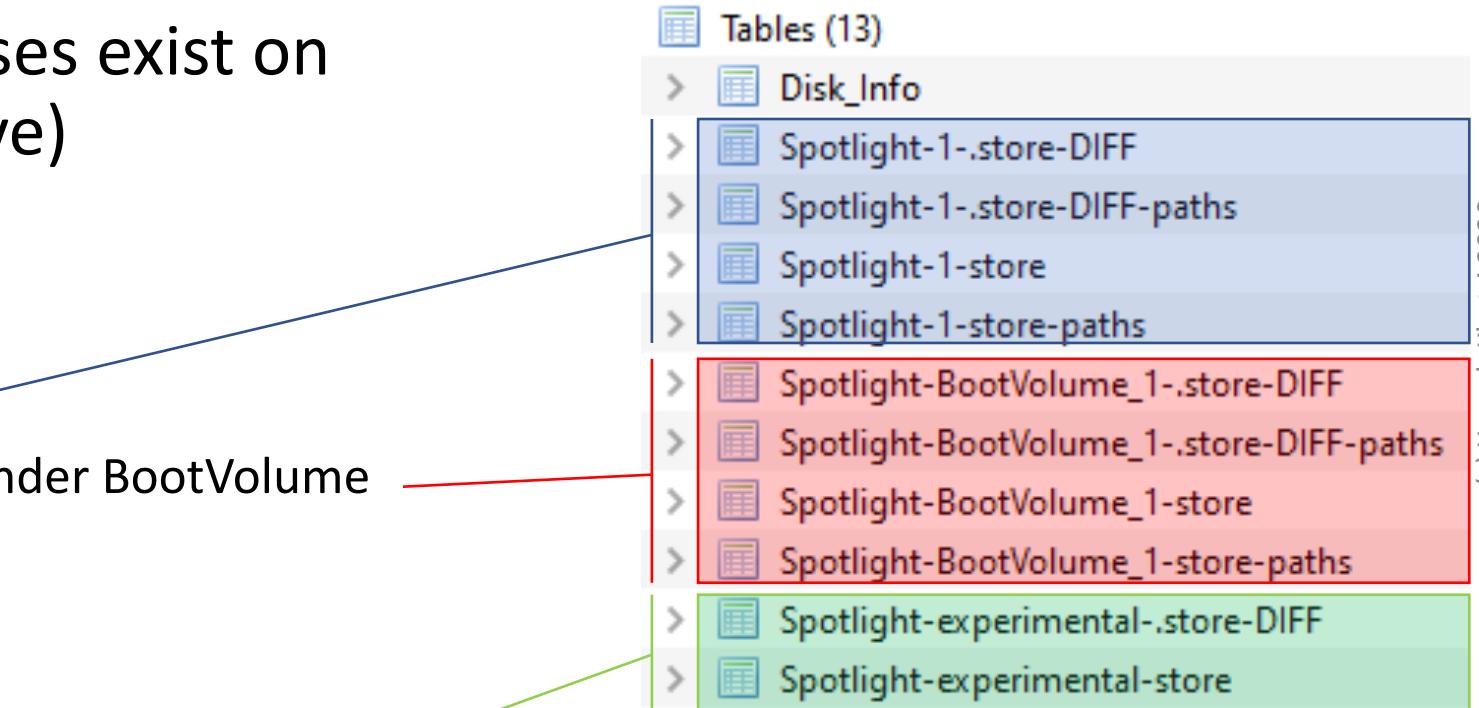
Email searched and launched from Spotlight Search

SQL 1				
	kMDItemAuthors	ItemPrimaryRecipientEmailAddre	_kMDItemLaunchString	_kMDItemShortcutLastUsedDate
2	Google	goashleymcdonald@gmail.com		
3	The Blogs at The Times of Israel	goashleymcdonald@gmail.com		
4	VegasInsider.com	goAshleymcdonald@gmail.com	vegas	2020-12-03 17:35:28.834117
5	People News	goashleymcdonald@gmail.com		

Searched Term

Understanding mac_apt's SPOTLIGHT output (for Catalina – 10.15 or above)

- Multiple spotlight databases exist on macOS Catalina (and above)
 - Volume databases
 - One for DATA volume
 - One for SYSTEM volume (under BootVolume folder)
 - Per-user databases
 - One per user (stores records from Apps that user interacts with). Here user name was *experimental*



Thanks for watching!

Any Questions?



https://github.com/ydkhatri/mac_apt
https://github.com/ydkhatri/spotlight_queries



@*swiftforensics*



Yogesh@swiftforensics.com