

Shedding Light on the macOS Spotlight Desktop Search Service



BlackBag[®]
TECHNOLOGIES

Dr. Vico Marizale
Senior Digital
Forensics Researcher

#whoami

- Researcher: Senior Digital Forensics Researcher, BBT
- Practitioner (formerly): 504ENSICS, mostly civil litigation
- Academic: PhD in CS (Digital Forensics), University of New Orleans
 - Published and presented research and tools at RSA, BlackHat, DOD Cybercrime, a few BSides, DFRWS, OSDFCOn, etc.
- Occasional Gatekeeper: Digital Investigation, DFRWS, others
- Organizer: [BSidesNOLA \(10/26 – tell all ya friends!\)](#), NOLASec
- Tool Author: Scalpel, Registry Decoder, Spotlight Inspector*, DAMM

Basics

- Desktop search on OS X, macOS, and iOS
 - On by default, around since 10.4
 - Indexes file content and metadata
- Many pieces to the framework - client server processes, importers, API access, cmdline and GUI tools, indexes, etc.
- Large parts undocumented by Apple
- Our focus today is on the metadata store on macOS and iOS
 - Holds *attributes* = key: value
 - kMDItemWhatever: string | number | date | etc.
- Note: Ongoing area of research
 - Reminiscent of the Windows registry in some ways

Why do you care?

```
$ mdfind -0 "kMDItemUseCount >= 100" | xargs -0 mdls -name  
kMDItemPath -name kMDItemUseCount -name kMDItemUsedDates
```

```
kMDItemPath =  
"/Applications/Google Chrome.app"  
kMDItemUseCount = 121  
kMDItemUsedDates = (  
    "2015-02-02 08:00:00 +0000",  
    < snip ~80 entries >  
    "2018-07-26 05:00:00 +0000"  
)
```

```
kMDItemPath =  
"/Users/vico/Downloads"  
kMDItemUseCount = 368  
kMDItemUsedDates = (  
    "2015-02-02 06:00:00 +0000",  
    < snip ~200 entries >  
    "2018-08-15 05:00:00 +0000"  
)
```


Why do you care?

```
$ mdfind -0 "kMDItemUseCount >= 100" | xargs -0 mdls -name  
kMDItemPath -name kMDItemUseCount -name kMDItemUsedDates
```

```
kMDItemPath =  
"/Applications/Google Chrome.app"  
kMDItemUseCount = 121  
kMDItemUsedDates = (  
    "2015-02-02 08:00:00 +0000",  
    < snip ~80 entries >  
    "2018-07-26 05:00:00 +0000"  
)
```

```
kMDItemPath =  
"/Users/vico/Downloads"  
kMDItemUseCount = 368  
kMDItemUsedDates = (  
    "2015-02-02 06:00:00 +0000",  
    < snip ~200 entries >  
    "2018-08-15 05:00:00 +0000"  
)
```

Plus

- Message contents
- Email contents
- Phone numbers
- Print activity
- Location information
- Calendar items
- Specific user doing activity

Plus: So Many Timestamps!

kMDItemAttributeChangeDate
kMDItemContentCreationDate
kMDItemContentModificationDate
kMDItemDateAdded
kMDItemFinderOpenDate
kMDItemFSContentChangeDate
kMDItemFSCreationDate
kMDItemLastUsedDate
kMDItemPurchaseDate

kMDItemUsedDates
kMDItemUserCreatedDate
kMDItemUserCreatedUserHandle
kMDItemUserDownloadedDate
kMDItemUserModifiedDate
kMDItemUserModifiedUserHandle
kMDItemUserPrintedDate
kMDItemUserSharedReceivedDate
kMDItemUserSharedSentDate

And more

com_apple_mail_dateLastViewed
com_apple_mail_dateReceived
com_microsoft_outlook_completedDate
com_microsoft_outlook_customDate1
com_microsoft_outlook_customDate2
com_microsoft_outlook_endDate
com_microsoft_outlook_hasDueDate
com_microsoft_outlook_hasStartDate
com_microsoft_outlook_startDate

These are application specific.

Apps can register an importer
and add metadata they want.

Can document not at all if they
choose.

Are all of these even really
timestamps?

Been There, Done That

504ENSICS releases Spotlight Inspector 11/2013 (via DARPA CFT)

<https://web.archive.org/web/20131125211317/http://www.504ensics.com/tools/digital-forensics-tool-spotlight-inspector/>

And takes it offline about a year later

F-Secure Data Leakage 10/2014

<https://www.f-secure.com/weblog/archives/00002752.html>

Sarah Edwards: mdfind/mdls queries 12/2015

<https://github.com/mac4n6/Presentations/tree/master/OSX%20Spotlight%20Queries>

Spotlight MRU/Shortcuts 07/2017

<https://www.mac4n6.com/blog/2017/7/19/script-update-mac-mru-parser-spotlight-shortcuts-blob-parsing>

Lee Whitfield: Spotlight timestamps and use counts

<https://forensic4cast.com/2016/10/mac-os-timestamps-from-extended-attributes-and-spotlight/>

Yogesh Khatri

spotlight_parser announced 08/2018

<https://www.swiftforensics.com/2018/08/parsing-spotlight-database.html>

https://github.com/ydkhatri/spotlight_parser

User-level DBs discovered 10/2018

<https://www.swiftforensics.com/2018/10/the-user-spotlight-database.html>

“Investigating spotlight internals to extract metadata” published 03/2019

<https://www.sciencedirect.com/science/article/pii/S1742287618300860>

Atwal, Scanlon, Le-Khac publish 04/2019

“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?via%3Dihub>

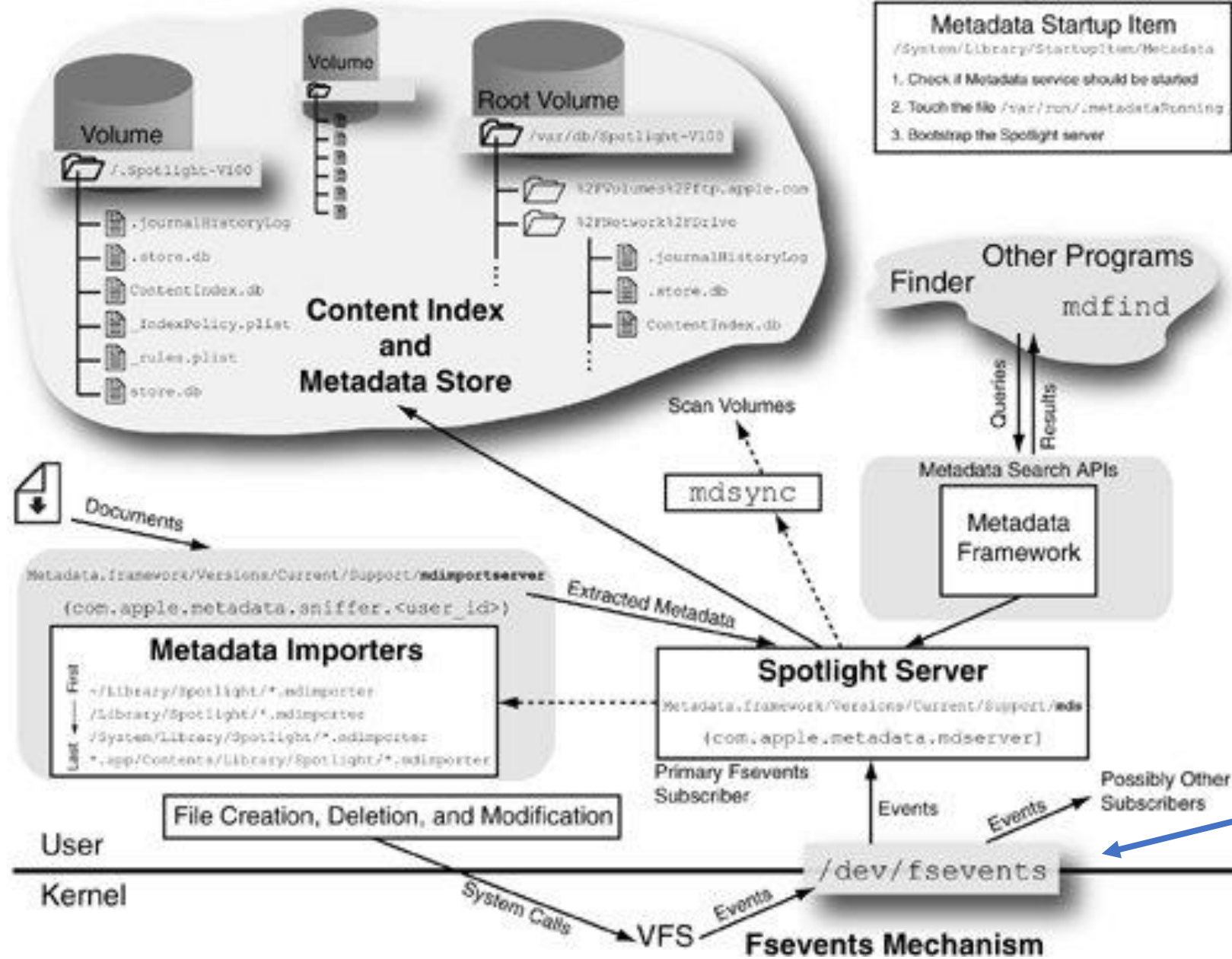
<https://forensicsandsecurity.com/papers/SpotlightMacForensicsSlides.pdf>

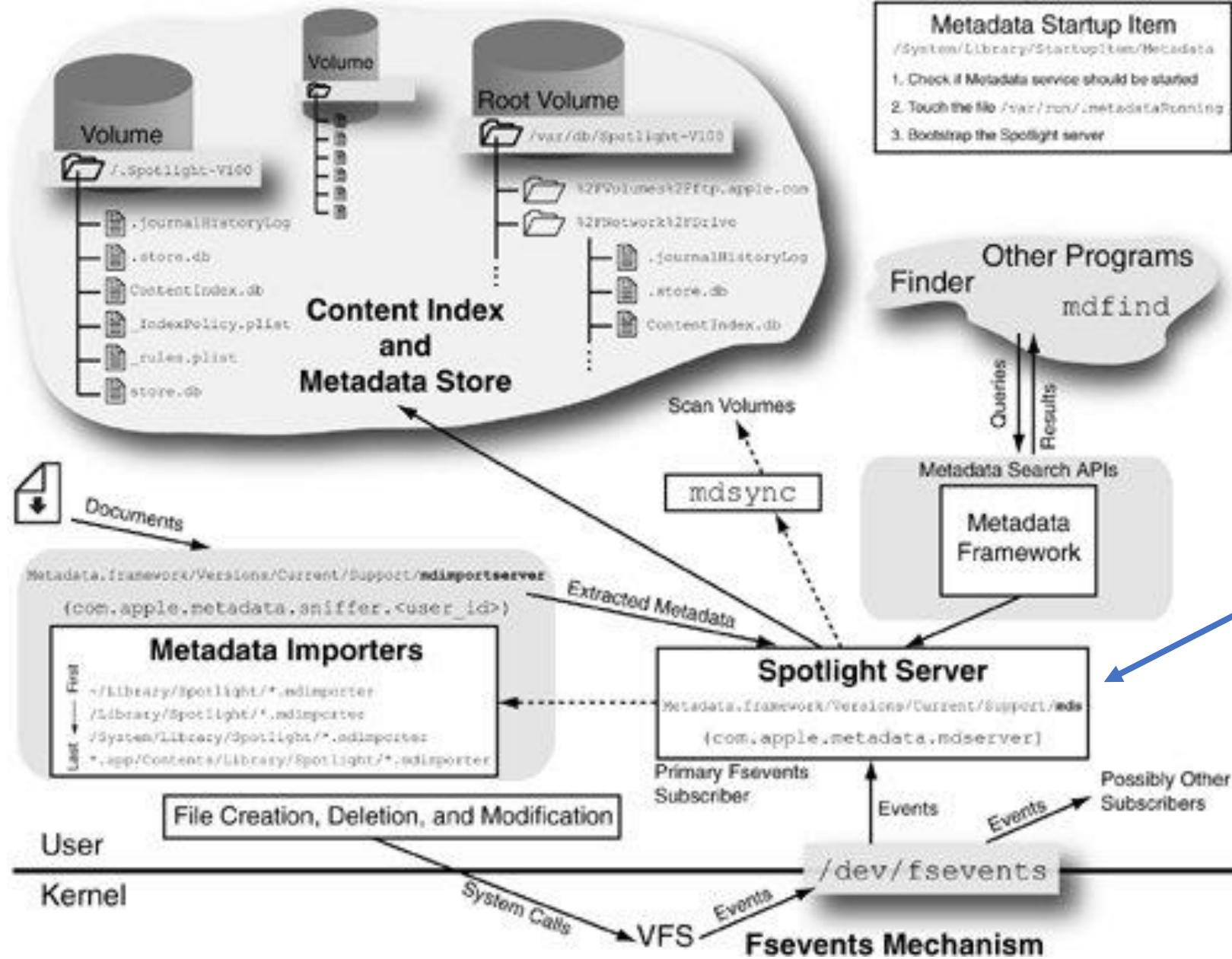
Howard Oakley 2015 and on: tons of Spotlight related goodness

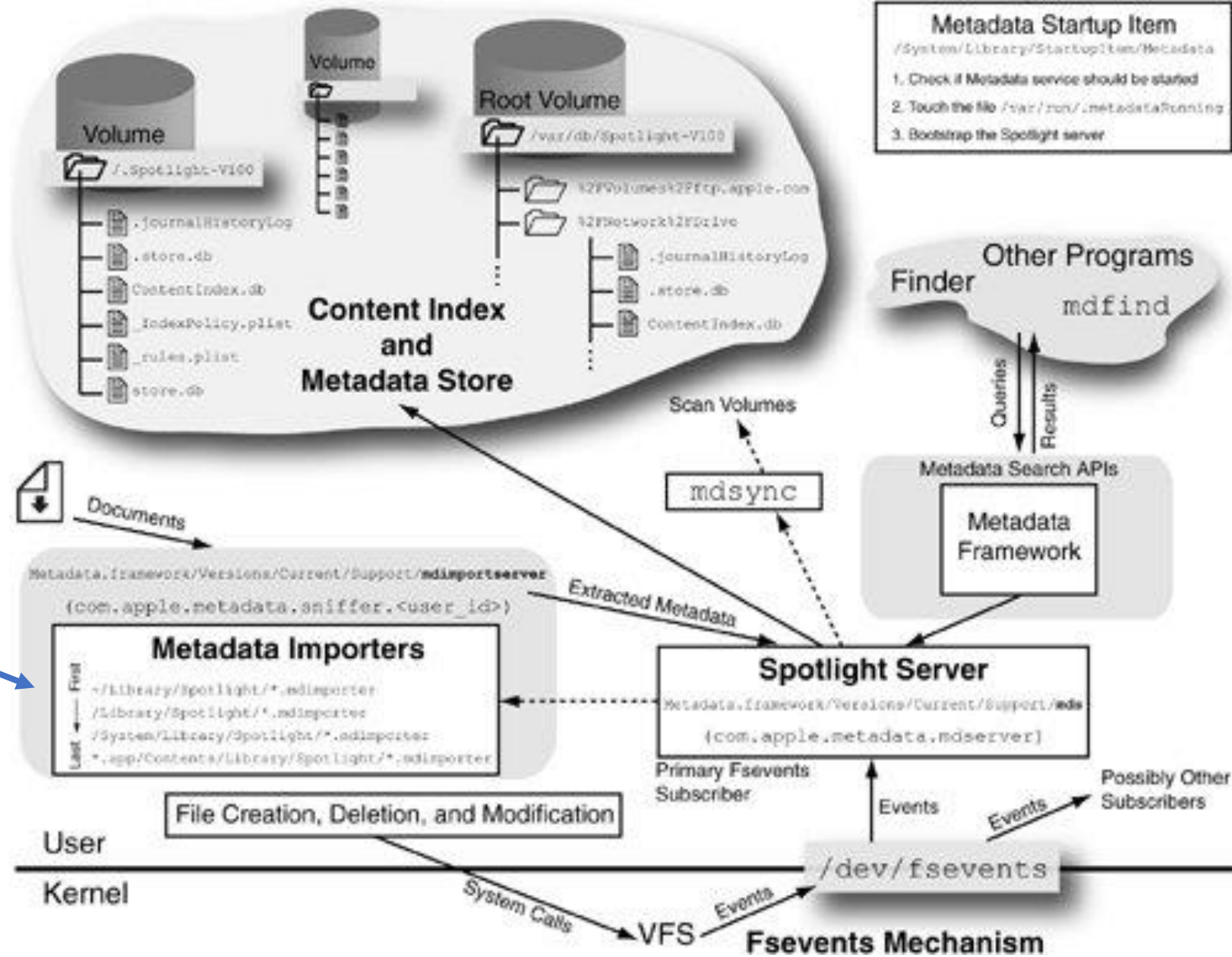
<https://eclecticlight.co/>

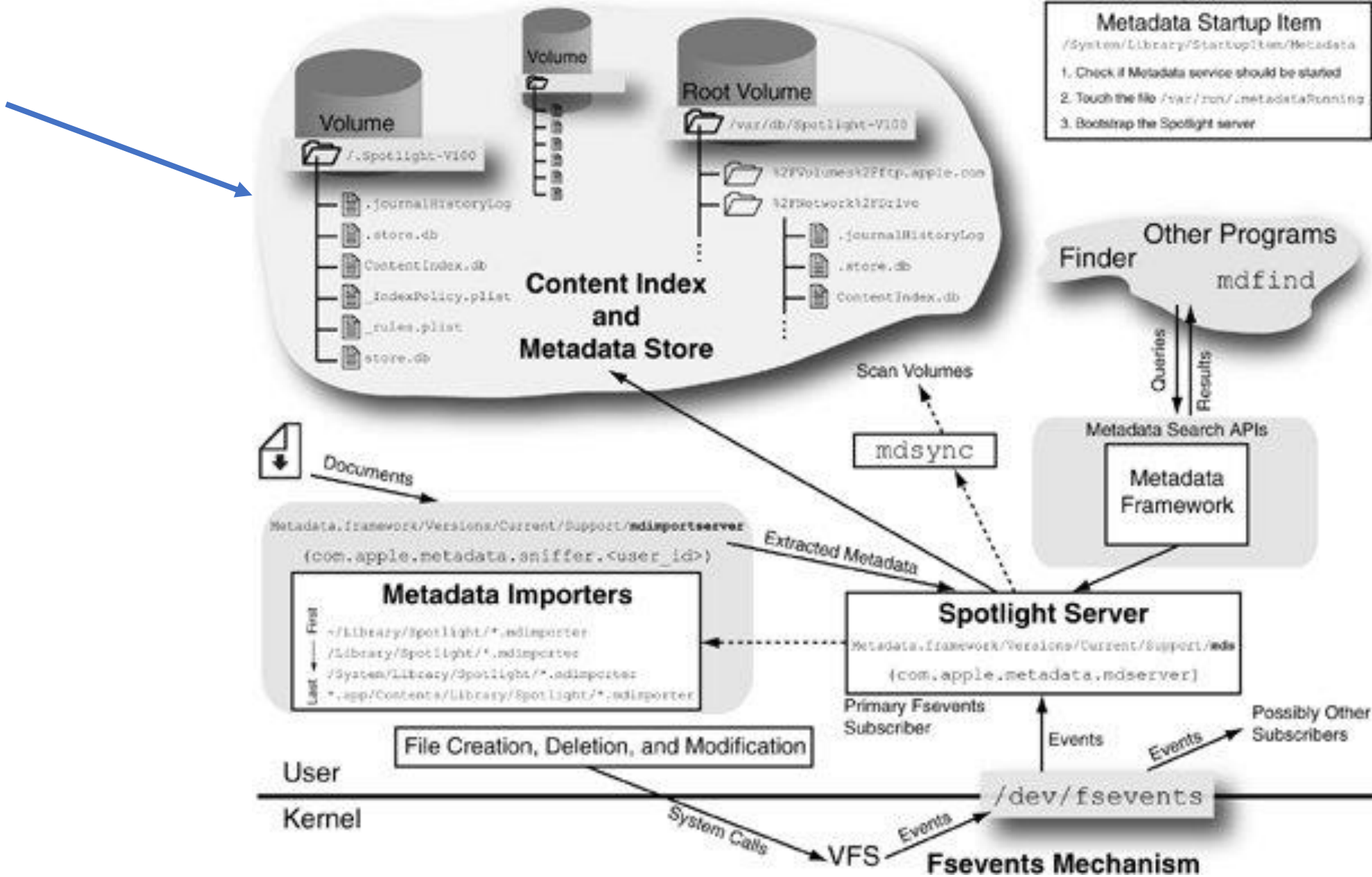


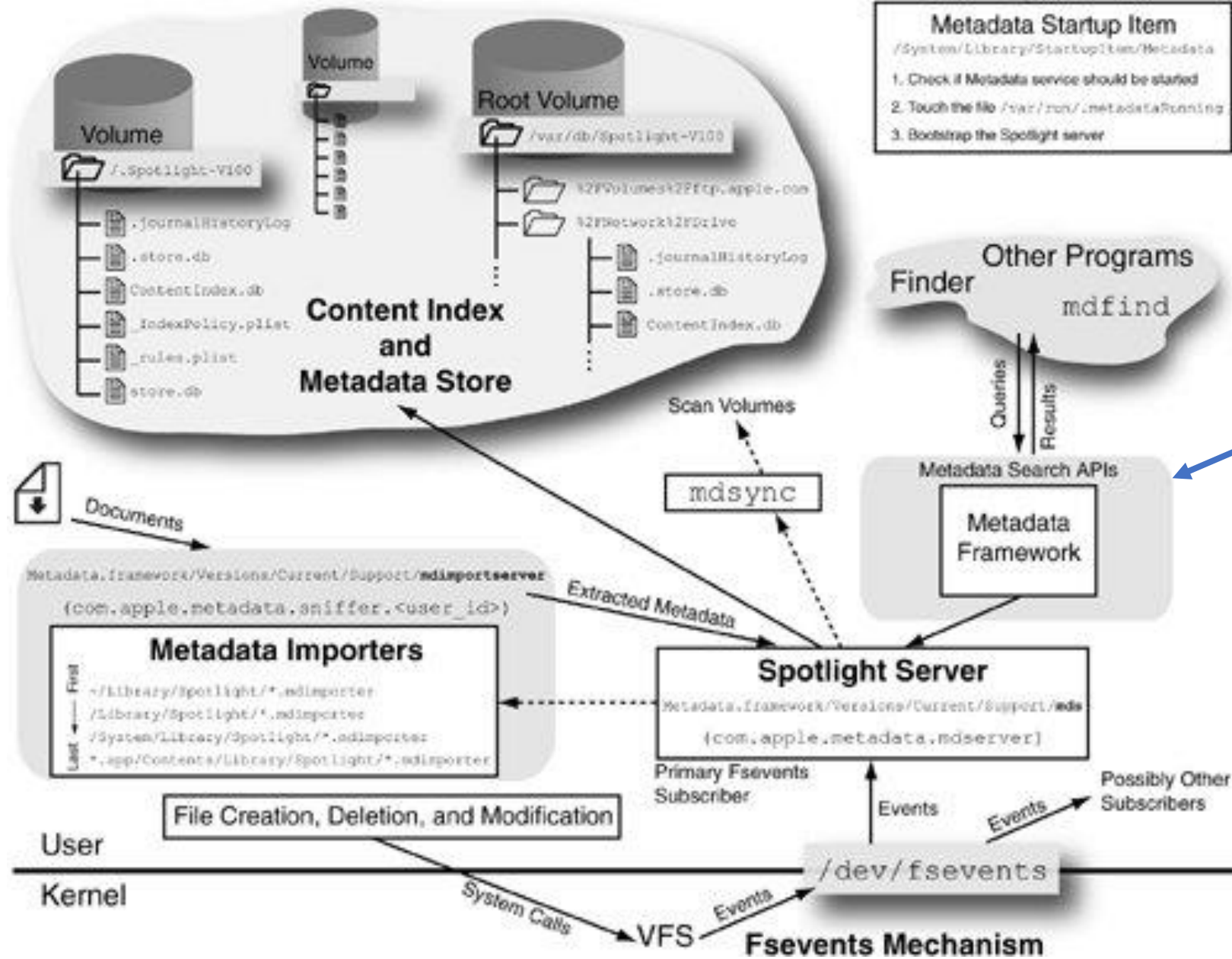
How the Sausage is Made

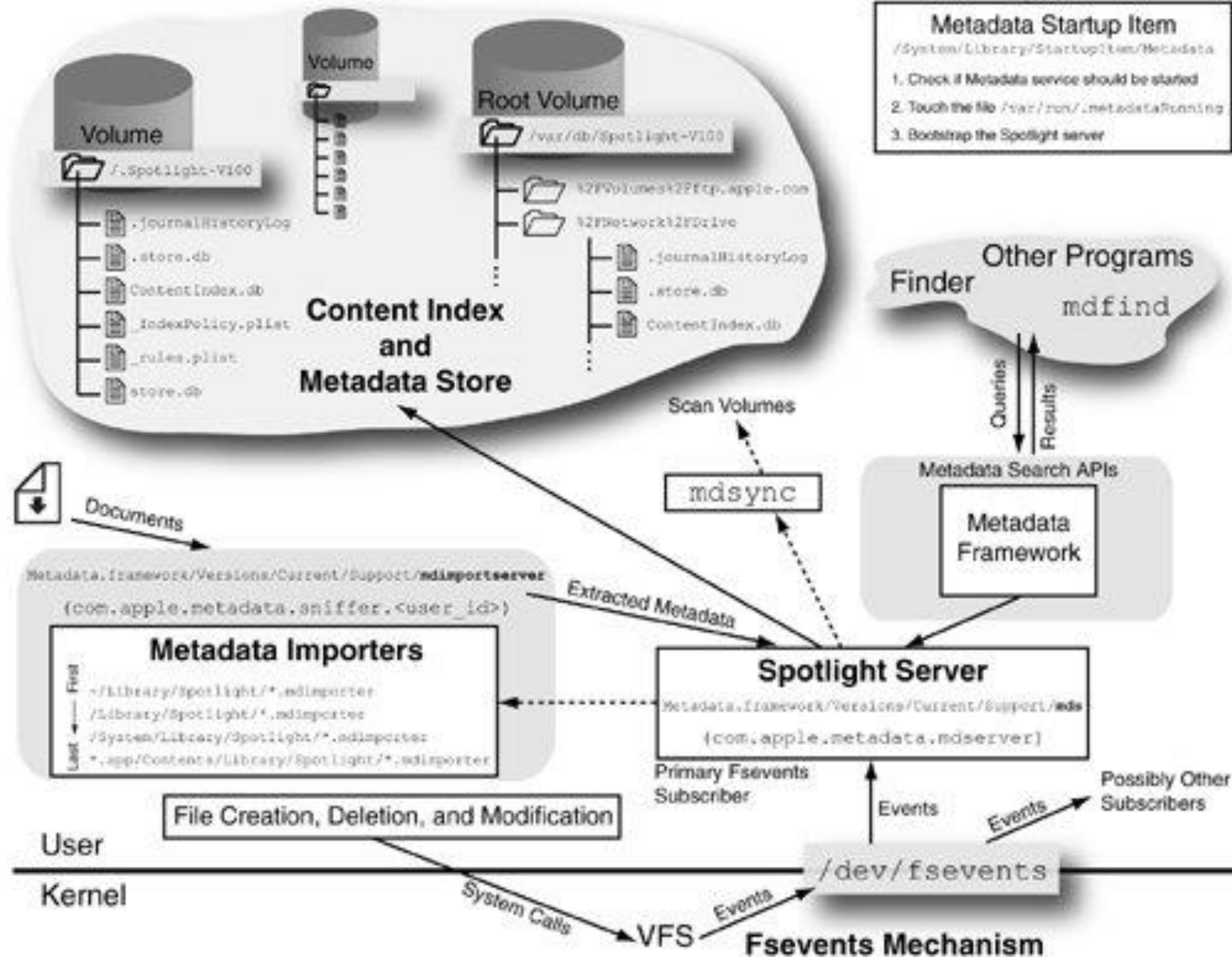












Yeah But Where's the Beef?

Volume-Level Spotlight

macOS Volume-Level Directory Structure

```
/.Spotlight-V100/  
  -- VolumeConfiguration.plist  
  -- Store-V1/  
  -- Store-V2 /  
    -- 20EC0E92-F4BB-4937-8748-25D6A6FF5CBF/  
    -- 736154F6-76DD-423E-9033-A33963A06D07/  
      -- store.db  
      -- .store.db ← The good stuff  
      -- Cache/  
        -- hierarchy of numbered directories  
        -- (dozens of other files)
```

Case Info

Report

Details

Browse

File Filter

Actionable Intel

Communication

Media

Locations

Internet

Productivity

System

Plugins

Notifications

EVIDENCE

Add

Bennett-Computer-19030...

1

Racer

2

1b1ce46edadab95d64...

Racer.dmg.dd

3

racer

4

racer (Carved Files)

carvertest.dmg

5

carvertest

7

carvertest (Carved F...

ACTIVITY

Export Status

Evidence Status

CONTENT SEARCHES

Add

INDEX SEARCHES

Add

TAGS

Add

INVESTIGATIVE NOTES

Add

Field	Value
BBTID:	1599377
FileSystemID:	941063
Name:	416864.txt
Path:	/.Spotlight-V100/Store-V
Size:	3397
SizeOnDisk:	3397
Extension:	txt
ContentExt...	
Date Created:	2012-01-02 02:26:42 (U
Date Chang...	2012-01-02 02:26:42 (U
Date Modifi...	2012-01-02 02:26:42 (U
Date Acces...	2012-01-02 02:26:42 (U
FileSystem...	UTC
fsType:	HFS+
Directory:	No
Visible:	Yes
Locked:	No

Root

Name	Date Created	Date Modified	Date Accessed	Date Added
Cache	2012-01-02 02:24:33 (UTC)	2012-01-02 02:24:33 (UTC)	2012-01-02 02:24:33 (UTC)	2012-01-02 02:24:33 (UTC)
0000	2012-01-02 02:24:33 (UTC)	2012-01-02 02:24:33 (UTC)	2012-01-02 02:24:33 (UTC)	2012-01-02 02:24:33 (UTC)
0000	2012-01-02 02:24:33 (UTC)	2012-02-05 16:43:00 (UTC)	2012-01-02 02:24:33 (UTC)	2012-01-02 02:24:33 (UTC)
0002	2012-01-02 02:24:41 (UTC)	2012-01-02 02:24:44 (UTC)	2012-01-02 02:24:41 (UTC)	2012-01-02 02:24:41 (UTC)
0003	2012-01-02 02:24:45 (UTC)	2012-01-02 02:26:36 (UTC)	2012-01-02 02:24:45 (UTC)	2012-01-02 02:24:45 (UTC)
0005	2012-01-02 02:26:37 (UTC)	2012-01-02 02:26:37 (UTC)	2012-01-02 02:26:37 (UTC)	2012-01-02 02:26:37 (UTC)
0006	2012-01-02 02:26:38 (UTC)	2012-01-02 02:26:42 (UTC)	2012-01-02 02:26:38 (UTC)	2012-01-02 02:26:38 (UTC)
412303.txt	2012-01-02 02:26:38 (UTC)	2012-01-02 02:26:38 (UTC)	2012-01-02 02:26:38 (UTC)	2012-01-02 02:26:38 (UTC)
412324.txt	2012-01-02 02:26:39 (UTC)	2012-01-02 02:26:39 (UTC)	2012-01-02 02:26:39 (UTC)	2012-01-02 02:26:39 (UTC)
413405.txt	2012-01-02 02:26:39 (UTC)	2012-01-02 02:26:39 (UTC)	2012-01-02 02:26:39 (UTC)	2012-01-02 02:26:39 (UTC)
414143.txt	2012-01-02 02:26:39 (UTC)	2012-01-02 02:26:39 (UTC)	2012-01-02 02:26:39 (UTC)	2012-01-02 02:26:39 (UTC)
416864.txt	2012-01-02 02:26:42 (UTC)	2012-01-02 02:26:42 (UTC)	2012-01-02 02:26:42 (UTC)	2012-01-02 02:26:42 (UTC)
0007	2012-01-02 02:26:43 (UTC)	2012-03-04 20:02:51 (UTC)	2012-01-02 02:26:43 (UTC)	2012-01-02 02:26:43 (UTC)

Hex

Strings

Preview

Metadata

Location

Record

First Name: Josh Last Name: Bennett Email Address: jbenett_mac@me.com Country: United States Address line 1: 15723 Monterey Rd. City: Morgan Hill Post Code: 95037 Telephone: 4087865123 Password: Checkout My Account | Cart Contents | Checkout Fast and Secure Checkout Step 1: Review Your Cart Item # Product Name Qty Unit Price Total Price ML-0002 Auto Jiggler Lockpick Tool 10 Piece Key Set - No USPS Shipping 1 \$14.95 \$14.95 Did you make any changes above? Do you have a promo code? Sub-Total: \$14.95 United Parcel Service (1 pkg x 1 lbs total) (UPS Ground, EDD: March 18, 2010): \$6.59 Total: \$21.54 Step 2: Billing / Shipping Information Billing Address Are you already a customer? Shipments to P.O. Boxes may be delayed Tip: Enter a daytime number where you can be reached if there are any questions regarding your order. Shipping Address Is your shipping address different? Tip: Create a password below to view the status of your order 24/7. Safe & Secure This website is secured by a high-grade 256-bit SSL certificate that encrypts (scrambles) your information to ensure a safe and secure transaction. All credit card information passes directly to our payment processor and is never stored by us. Your security is our first priority. Ordering Information Order Errors: If an error is believed to have been found, we will call you or send you an e-mail to confirm the order. The order will not be sent to our printers until we have verified the order. Processing Time: Orders are generally processed and shipped via UPS within 1-2 business days. Orders are not processed on national holidays or weekends. Time of delivery will depend upon your chosen shipping method and your shipping location. State: California KeepShooting.COM - Online Store https://www.KeepShooting.com/keepshooting-store/catalog/che... 1 of 2 3/10/10 8:47 AM Step 3: Select a Payment Method Visa / MasterCard / American Express / Discover Mail a Money Order Make Payable To: BTP ARMS Send To: KeepShooting.COM - div. of BTP ARMS 1282 Smallwood Drive West #105 Waldorf, MD 20603-4732 800-570-8239 Your order will not ship until we receive payment. Step 4: Select a Shipping Method Free Ground Shipping Available Only for orders \$150 minimum Step 5: Confirm

Type	Value (Litt...
Date/Time	
Chrome	
Cocoa/Webkit	
Cocoa Nanoseconds	
DOS	n/a (???)
FILETIME	
Firefox	
Java	
OLE	
OS X	
Unix	
Integer	
8 bit signed	
8 bit unsigned	
16 bit signed	
16 bit unsigned	
32 bit signed	
32 bit unsigned	
64 bit signed	
64 bit unsigned	
Float	

Little Endian

Hierarchy of folders with 4 digit names; contain .txt files.

Remember: 416864



BlackBag[®]
TECHNOLOGIES

Case Info

Report

Details

Browser

File Filter

Actionable Intel

Communication

Media

Locations

Internet

Productivity

System

Plugins

Notifications

EVIDENCE

Add

Bennett-Computer-19030...

1

Racer

2

1b1ce46edadab95d64...

3

racer

4

racer (Carved Files)

carvertest.dmg

5

carvertest

7

carvertest (Carved F...

ACTIVITY

Export Status

Evidence Status

CONTENT SEARCHES

Add

INDEX SEARCHES

Add

TAGS

Add

INVESTIGATIVE NOTES

Add

Field

Value

BBTID:

2160485

FileSystemID:

416864

Name:

KeepShooting.COM - Onl

Path:

/Users/josh/Documents/k

Size:

270459

SizeOnDisk:

270459

Extension:

pdf

ContentExte...

Date Created:

2010-03-10 16:47:19 (UT

Date Chang...

2010-03-10 16:47:20 (U

Date Modifi...

2010-03-10 16:47:20 (U

Date Acces...

2012-02-03 01:47:02 (U

FileSystem...

UTC

fsType:

HFS+

Directory:

No

Visible:

Yes

Locked:

No

Save Filters:

Select where

all

of the conditions are met:

File System ID

equals

416864

Invert Filter

Ignore Folders and Duplicate Files

Reset...

Save This Filter

Filter

BL ID

FS ID

Name

Size

Date Created

Date Modified

Date

3

2160485

416864

KeepShooting.COM - Online Store.pdf

264.1 KB

2010-03-10 16:47:19 (UTC)

2010-03-10 16:47:20 (UTC)

201

Hex

Strings

Preview

Metadata

Location

Record

Data Fork

Share

Sign In

Step 2: Billing / Shipping Information

Billing Address

Shipping Address

Are you already a customer?

Sign in

Is your shipping address different?

First Name:

Last Name:

Josh

Bennett

Email Address:

jbenett_mac@me.com

Country:

United States

Address line 1:

15723 Monterey Rd.

Shipments to P.O. Boxes may be delayed

City:

Morgan Hill

State:

California

Post Code:

95037

Telephone:

4087865123

Tip: Enter a daytime number where you can be reached if there are any questions regarding your order.

Password:

Tip: Create a password below to view the status of your order 24/7.

your information to ensure a safe and secure transaction.

All credit card information passes directly to our payment processor and is never stored by us. Your security is our first priority.

Ordering Information

Order Errors:

If an error is believed to have been found, we will call you or send you an e-mail to confirm the order. The order will not be sent to our printers until we have verified the order.

Processing Time:

Orders are generally processed and shipped via UPS within 1-2 business days. Orders are not processed on national holidays or weekends. Time of delivery will depend upon your chosen shipping method and your shipping location.

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

2160485.pdf

Convert to

Microsoft Word (*.docx)

Convert and edit PDFs with Acrobat Pro DC

Start Free Trial

(1 of 1) - /racer/Users/josh/Documents/KeepShooting.COM - Online Store.pdf

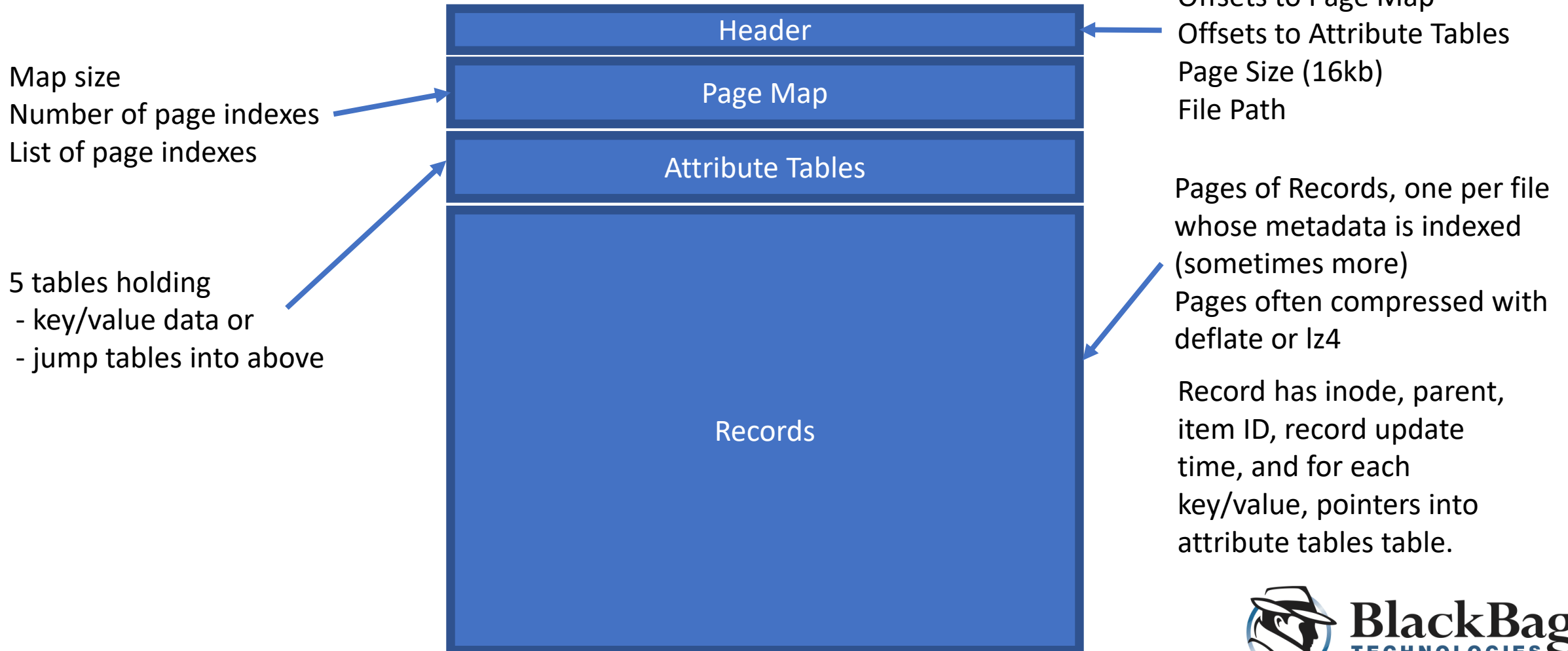
Same text in the file with:
inode number = txt file name



What I've Got in (the) Store for You Next

Store Structure

store.db



Header

Spotlight.blacklight

Case Info Report Details

Browser File Filter Actionable Intel Communication Media Locations Internet Productivity System Plugins Notifications

EVIDENCE Add

- ✓ Bennett-Computer-19030...
 - ✓ 1 Racer
 - 2 1b1ce46edadab95d64...

ACTIVITY

- Export Status
- Evidence Status

CONTENT SEARCHES Add

INDEX SEARCHES Add

TAGS Add

INVESTIGATIVE NOTES Add

Name	Date Created	Date Modified	Date Accessed	Date Ad
Store-V1	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	
Store-V2	2015-06-11 22:55:11 (UTC)	2015-06-11 23:46:27 (UTC)	2016-12-08 14:48:33 (UTC)	
B6423D63-F381-46C0-80BE-...	2015-06-11 23:46:27 (UTC)	2017-11-14 13:28:38 (UTC)	2017-11-29 20:01:38 (UTC)	
CC48CF65-F311-448D-875B-...	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:51 (UTC)	2019-02-26 13:23:14 (UTC)	
.store.db	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:52 (UTC)	2019-02-26 14:17:50 (UTC)	
0.directoryStoreFile	2018-12-12 18:40:42 (UTC)	2019-02-26 13:23:14 (UTC)	2019-02-26 14:18:02 (UTC)	
0.directoryStoreFile.shadow	2018-12-12 18:40:42 (UTC)	2019-01-30 16:34:31 (UTC)	2019-01-30 16:34:48 (UTC)	
0.indexArrays	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	
0.indexBinDates	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	

Hex Strings Preview Metadata Location Record Data Interpreter Data Fork

00000000:	38 74 73 64	01 05 00 00	00 00 00 00	0C 00 00 00	8tsd.....
00000016:	00 00 00 00	03 4B 03 00	00 00 00 00	0E B9 12 00	...K..... ¹ ..
00000032:	00 00 00 00	00 10 00 00	00 80 00 00	00 40 00 00	@..
00000048:	A5 04 00 00	09 00 00 00	0D 00 00 00	11 00 00 00	
00000064:	15 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000080:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000096:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000112:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000128:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000144:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000160:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000176:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000192:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000208:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000224:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000240:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000256:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000272:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000288:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000304:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000320:	00 00 00 00	2F 2E 53 70	6F 74 6C 69	67 68 74 2D	/.Spotlight-
00000336:	56 31 30 30	2F 53 74 6F	72 65 2D 56	32 2F 43 43	V100/Store-V2/CC
00000352:	34 38 43 46	36 35 2D 46	33 31 31 2D	34 34 38 44	48CF65-F311-448D
00000368:	2D 38 37 35	42 2D 46 44	42 31 41 32	35 42 35 43	-875B-FDB1A25B5C
00000384:	37 38 2F 73	74 6F 72 65	2E 64 62 00	00 00 00 00	78/store.db.....
00000400:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000416:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000432:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	

Field Value

BBTID: 39279

FileSystemID: 401445

Name: .store.db

Path: ./Spotlight-V100/Store-V

Size: 19173376

SizeOnDisk: 19173376

Extension: db

ContentExt...

Date Created: 2015-06-11 22:55:11 (UT

Date Chang... 2019-02-26 14:17:52 (UT

Date Modifi... 2019-02-26 14:17:52 (UT

Decimal Go To Position Sector Offset: 0x0 (0) Position: 0x0 (0) Selection: 0x4 (4) Little Endian

(1 of 227) - /Racer/.Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/store.db

File header signature





Spotlight.blacklight

Case Info Report Details

Browser File Filter Actionable Intel Communication Media Locations Internet Productivity System Plugins Notifications

EVIDENCE Add

▼ ☒ Bennett-Computer-19030...

☒ 1 Racer

☐ 2 1b1ce46edadab95d64...

ACTIVITY

☒ Export Status

☒ Evidence Status

CONTENT SEARCHES Add

INDEX SEARCHES Add

TAGS Add

INVESTIGATIVE NOTES Add

Name	Date Created	Date Modified	Date Accessed	Date Ad
Store-V1	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	
Store-V2	2015-06-11 22:55:11 (UTC)	2015-06-11 23:46:27 (UTC)	2016-12-08 14:48:33 (UTC)	
B6423D63-F381-46C0-80BE-...	2015-06-11 23:46:27 (UTC)	2017-11-14 13:28:38 (UTC)	2017-11-29 20:01:38 (UTC)	
CC48CF65-F311-448D-875B-...	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:51 (UTC)	2019-02-26 13:23:14 (UTC)	
.store.db	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:52 (UTC)	2019-02-26 14:17:50 (UTC)	
0.directoryStoreFile	2018-12-12 18:40:42 (UTC)	2019-02-26 13:23:14 (UTC)	2019-02-26 14:18:02 (UTC)	
0.directoryStoreFile.shadow	2018-12-12 18:40:42 (UTC)	2019-01-30 16:34:31 (UTC)	2019-01-30 16:34:48 (UTC)	
0.indexArrays	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	
0.indexBinDates	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	

Hex Strings Preview Metadata Location Record Data Interpreter Data Fork

00000000:	38 74 73 64 01 05 00 00 00 00 00 00 0C 00 00 00	8tsd.....
00000016:	00 00 00 00 03 4B 03 00 00 00 00 00 0E B9 12 00	K..... ¹ ..
00000032:	00 00 00 00 00 10 00 00 00 80 00 00 00 40 00 00	@..
00000048:	A5 04 00 00 09 00 00 00 0D 00 00 00 11 00 00 00	¥.....
00000064:	15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000080:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000096:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000112:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000128:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000144:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000160:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000176:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000192:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000208:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000224:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000240:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000256:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000272:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000288:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000304:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000320:	00 00 00 00 2F 2E 53 70 6F 74 6C 69 67 68 74 2D	/.Spotlight-
00000336:	56 31 30 30 2F 53 74 6F 72 65 2D 56 32 2F 43 43	V100/Store-V2/CC
00000352:	34 38 43 46 36 35 2D 46 33 31 31 2D 34 3A 38 44	48CF65-F311-448D
00000368:	2D 38 37 35 42 2D 46 44 42 31 41 32 35 42 35 43	-875B-FDB1A25B5C
00000384:	37 38 2F 73 74 6F 72 65 2E 64 62 00 00 00 00 00	78/store.db....
00000400:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000416:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000432:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Field Value

BBTID: 39279

FileSystemID: 401445

Name: .store.db

Path: /.Spotlight-V100/Store-V

Size: 19173376

SizeOnDisk: 19173376

Extension: db

ContentExt...

Date Created: 2015-06-11 22:55:11 (UT

Date Chang... 2019-02-26 14:17:52 (UT

Date Modifi... 2019-02-26 14:17:52 (UT

Decimal Go To Position Sector Offset: 0x1BD (445) Position: 0x1BD (445) Selection: 0x4 (4) Little Endian

(1 of 227) - /Racer/.Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/.store.db

Page map offset



Spotlight.blacklight

Case Info Report Details

Browser File Filter Actionable Intel Communication Media Locations Internet Productivity System Plugins Notifications

EVIDENCE Add

- ✓ Bennett-Computer-19030...
 - ✓ 1 Racer
 - 2 1b1ce46edadab95d64...
 - Racer.dmg.dd
 - 3 racer
 - 4 racer (Carved Files)
 - carvertest.dmg
 - 5 carvertest
 - 7 carvertest (Carved F...
 - 8 3018772

ACTIVITY

- Export Status
- Evidence Status

CONTENT SEARCHES Add

INDEX SEARCHES Add

TAGS Add

INVESTIGATIVE NOTES Add

Field	Value
BBTID:	39279
FileSystemID:	401445
Name:	.store.db
Path:	/.Spotlight-V100/Store-V
Size:	19173376
SizeOnDisk:	19173376
Extension:	db
ContentExt...	
Date Created:	2015-06-11 22:55:11 (UT
Date Chang...	2019-02-26 14:17:52 (U
Date Modifi...	2019-02-26 14:17:52 (U
Date Acces...	2019-02-26 14:17:50 (U
FileSystem...	UTC
fsType:	APFS
Directory:	No
Visible:	Yes
Locked:	No

Root

Name	Date Created	Date Modified	Date Accessed	Date Ad
Store-V1	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	
Store-V2	2015-06-11 22:55:11 (UTC)	2015-06-11 23:46:27 (UTC)	2016-12-08 14:48:33 (UTC)	
B6423D63-F381-46C0-80BE-...	2015-06-11 23:46:27 (UTC)	2017-11-14 13:28:38 (UTC)	2017-11-29 20:01:38 (UTC)	
CC48CF65-F311-448D-875B-...	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:51 (UTC)	2019-02-26 13:23:14 (UTC)	
.store.db	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:52 (UTC)	2019-02-26 14:17:50 (UTC)	
0.directoryStoreFile	2018-12-12 18:40:42 (UTC)	2019-02-26 13:23:14 (UTC)	2019-02-26 14:18:02 (UTC)	
0.directoryStoreFile.shadow	2018-12-12 18:40:42 (UTC)	2019-01-30 16:34:31 (UTC)	2019-01-30 16:34:48 (UTC)	
0.indexArrays	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	
0.indexBigDates	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	

Hex Strings Preview Metadata Location Record

Data Interpreter Data Fork

00000000: 38 74 73 64 01 05 00 00 00 00 00 00 0C 00 00 00 8tsd.....
00000016: 00 00 00 00 03 48 03 00 00 00 00 00 0E B9 12 00K.....
00000032: 00 00 00 00 00 10 00 00 00 80 00 00 00 40 00 00@..
00000048: A5 04 00 00 09 00 00 00 0D 00 00 00 11 00 00 00¥.....
00000064: 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000096: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000112: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000128: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000144: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000176: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000208: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000224: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000240: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000256: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000272: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000304: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000320: 00 00 00 00 2F 2E 53 70 6F 74 6C 69 67 68 74 2D/.Spotlight-
00000336: 56 31 30 30 2F 53 74 6F 72 65 2D 56 32 2F 43 43V100/Store-V2/CC
00000352: 34 38 43 46 36 35 2D 46 33 31 31 2D 34 34 38 4448CF65-F311-448D
00000368: 2D 38 37 35 42 2D 46 44 42 31 41 32 35 42 35 43-875B-FDB1A25B5C
00000384: 37 38 2F 73 74 6F 72 65 2E 64 62 00 00 00 00 0078/store.db....
00000400: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000416: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000432: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Decimal Go To Position Sector Offset: 0x38 (56) Position: 0x38 (56) Selection: 0x14 (20)

(1 of 227) - /Racer/.Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/.store.db

Type Value (Litt...
String
UTF-8
UTF-16 H
Date/Time
Chrome
Cocoa/Webkit
Cocoa Nanoseconds
DOS n/a (???)
FILETIME
Firefox
Java
OLE
OS X
Unix
Integer
8 bit signed -91
8 bit unsigned 165
16 bit signed 1189
16 bit unsigned 1189
32 bit signed 1189
32 bit unsigned 1189
64 bit signed 38654706...
64 bit unsigned 38654706...
Float
Single (4 byte) 1.666144e...

Offsets in 4kb blocks to each of the 5 attribute tables

Case Info

Report

Details

Browser

File Filter

Actionable Intel

Communication

Media

Locations

Internet

Productivity

System

Plugins

Notifications

EVIDENCE

Add

Bennett-Computer-19030...

1

Racer

2

1b1ce46edadab95d64...

ACTIVITY

Export Status

Evidence Status

CONTENT SEARCHES

Add

INDEX SEARCHES

Add

TAGS

Add

INVESTIGATIVE NOTES

Add

Root

Name	Date Created	Date Modified	Date Accessed	Date Ad
Store-V1	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	
Store-V2	2015-06-11 22:55:11 (UTC)	2015-06-11 23:46:27 (UTC)	2016-12-08 14:48:33 (UTC)	
B6423D63-F381-46C0-80BE-...	2015-06-11 23:46:27 (UTC)	2017-11-14 13:28:38 (UTC)	2017-11-29 20:01:38 (UTC)	
CC48CF65-F311-448D-875B-...	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:51 (UTC)	2019-02-26 13:23:14 (UTC)	
.store.db	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:52 (UTC)	2019-02-26 14:17:50 (UTC)	
0.directoryStoreFile	2018-12-12 18:40:42 (UTC)	2019-02-26 13:23:14 (UTC)	2019-02-26 14:18:02 (UTC)	
0.directoryStoreFile.shadow	2018-12-12 18:40:42 (UTC)	2019-01-30 16:34:31 (UTC)	2019-01-30 16:34:48 (UTC)	
0.indexArrays	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	
0.indexBigDates	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	

Hex

Strings

Preview

Metadata

Location

Record

Data Interpreter

Data Fork

00000000:	38 74 73 64 01 05 00 00 00 00 00 00 0C 00 00 00	8tsd.....
00000016:	00 00 00 00 03 48 03 00 00 00 00 00 0E B9 12 00	K..... ¹ ..
00000032:	00 00 00 00 00 10 00 00 00 80 00 00 00 40 00 00	@..
00000048:	A5 04 00 00 09 00 00 00 0D 00 00 00 11 00 00 00	¥.....
00000064:	15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000080:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000096:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000112:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000128:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000144:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000160:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000176:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000192:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000208:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000224:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000240:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000256:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000272:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000288:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000304:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000320:	00 00 00 00 2F 2E 53 70 6F 74 6C 69 67 68 74 2D	/.Spotlight-
00000336:	56 31 30 30 2F 53 74 6F 72 65 2D 56 32 2F 43 43	V100/Store-V2/CC
00000352:	34 38 43 46 36 35 2D 46 33 31 31 2D 34 34 38 44	48CF65-F311-448D
00000368:	2D 38 37 35 42 2D 46 44 42 31 41 32 35 42 35 43	-875B-FDB1A25B5C
00000384:	37 38 2F 73 74 6F 72 65 2E 64 62 00 00 00 00 00	78/store.db.....
00000400:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000416:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000432:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Field

Value

Name:

.store.db

Path:

/.Spotlight-V100/Store-V

Size:

19173376

SizeOnDisk:

19173376

Extension:

db

ContentExte...

Date Created:

2015-06-11 22:55:11 (UT

Date Chang...

2019-02-26 14:17:52 (UT

Date Modifi...

2019-02-26 14:17:52 (UT

Date Acces...

2019-02-26 14:17:50 (UT

FileSvstem

UTC

Decimal

Go To Position

Sector Offset: 0xA (10)

Position: 0xA (10)

Selection: 0x47 (71)

Little Endian

(1 of 227)

- /Racer/.Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/.store.db

Path to the store file on disk



Attribute Tables

Case Info

Report

Details

Browser

File Filter

Actionable Intel

Communication

Media

Locations

Internet

Productivity

System

Plugins

Notifications

EVIDENCE

Add

Bennett-Computer-19030...

1

Racer

2

1b1ce46edadab95d64...

3

racer

4

racer (Carved Files)

5

carvertest.dmg

6

carvertest

7

carvertest (Carved F...

ACTIVITY

Export Status

Evidence Status

CONTENT SEARCHES

Add

INDEX SEARCHES

Add

TAGS

Add

INVESTIGATIVE NOTES

Add

Field	Value
BBTID:	39279
FileSystemID:	401445
Name:	.store.db
Path:	/.Spotlight-V100/Store-V
Size:	19173376
SizeOnDisk:	19173376
Extension:	db
ContentExt...	
Date Created:	2015-06-11 22:55:11 (UT
Date Chang...	2019-02-26 14:17:52 (U
Date Modifi...	2019-02-26 14:17:52 (U
Date Acces...	2019-02-26 14:17:50 (U
FileSystem...	UTC
fsType:	APFS
Directory:	No
Visible:	Yes
Locked:	No

Root

Name	Date Created	Date Modified	Date Accessed	Date Ad
Store-V1	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	
Store-V2	2015-06-11 22:55:11 (UTC)	2015-06-11 23:46:27 (UTC)	2016-12-08 14:48:33 (UTC)	
B6423D63-F381-46C0-80BE-...	2015-06-11 23:46:27 (UTC)	2017-11-14 13:28:38 (UTC)	2017-11-29 20:01:38 (UTC)	
CC48CF65-F311-448D-875B-...	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:51 (UTC)	2019-02-26 13:23:14 (UTC)	
.store.db	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:52 (UTC)	2019-02-26 14:17:50 (UTC)	
0.directoryStoreFile	2018-12-12 18:40:42 (UTC)	2019-02-26 13:23:14 (UTC)	2019-02-26 14:18:02 (UTC)	
0.directoryStoreFile.shadow	2018-12-12 18:40:42 (UTC)	2019-01-30 16:34:31 (UTC)	2019-01-30 16:34:48 (UTC)	
0.indexArrays	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	
0.indexBigDates	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	

Hex

Strings

Preview

Metadata

Location

Record

Data Interpreter

Data Fork

Type	Value (Littl...
Date/Time	
Chrome	1601-01-01 ...
Cocoa/Webkit	2054-05-15...
Cocoa Nanoseconds	
DOS	2030-03-02...
FILETIME	
Firefox	1970-01-01 ...
Java	1970-01-20 ...
OLE	
OS X	1957-05-14 ...
Unix	2023-05-15...
Integer	
8 bit signed	50
8 bit unsigned	50
16 bit signed	28722
16 bit unsigned	28722
32 bit signed	1684172850
32 bit unsigned	1684172850
64 bit signed	
64 bit unsigned	
Float	
Single (4 byte)	1.670819e+22
Double (8 byte)	
Other	
Base64	

DecimalGo To PositionSector Offset: 0x1D1 (465)Position: 0x4A4FD1 (4870097)Selection

First attribute table
page header

Spotlight.blacklight

Case Info Report Details

Browser File Filter Actionable Intel Communication Media Locations Internet Productivity System Plugins Notifications

EVIDENCE Add

▼ ☒ Bennett-Computer-19030...

▼ ☒ 1 Racer

▼ ☐ 2 1b1ce46edadab95d64...

▼ ☐ Racer.dmg.dd

▼ ☐ 3 racer

▼ ☐ 4 racer (Carved Files)

▼ ☐ carvertest.dmg

▼ ☐ 5 carvertest

▼ ☐ 7 carvertest (Carved F...

ACTIVITY

Export Status

Evidence Status

CONTENT SEARCHES Add

INDEX SEARCHES Add

TAGS Add

INVESTIGATIVE NOTES Add

Field Value

BBTID: 39279

FileSystemID: 401445

Name: .store.db

Path: /Spotlight-V100/Store-V

Size: 19173376

SizeOnDisk: 19173376

Extension: db

ContentExt...

Date Created: 2015-06-11 22:55:11 (UTC)

Date Chang... 2019-02-26 14:17:52 (UTC)

Date Modifi... 2019-02-26 14:17:52 (UTC)

Date Acces... 2019-02-26 14:17:50 (UTC)

FileSystem... UTC

fsType: APFS

Directory: No

Visible: Yes

Locked: No

Root

Name	Date Created	Date Modified	Date Accessed	Date Ad
Store-V1	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	
Store-V2	2015-06-11 22:55:11 (UTC)	2015-06-11 23:46:27 (UTC)	2016-12-08 14:48:33 (UTC)	
B6423D63-F381-46C0-80BE-...	2015-06-11 23:46:27 (UTC)	2017-11-14 13:28:38 (UTC)	2017-11-29 20:01:38 (UTC)	
CC48CF65-F311-448D-875B-...	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:51 (UTC)	2019-02-26 13:23:14 (UTC)	
.store.db	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:52 (UTC)	2019-02-26 14:17:50 (UTC)	
0.directoryStoreFile	2018-12-12 18:40:42 (UTC)	2019-02-26 13:23:14 (UTC)	2019-02-26 14:18:02 (UTC)	
0.directoryStoreFile.shadow	2018-12-12 18:40:42 (UTC)	2019-01-30 16:34:31 (UTC)	2019-01-30 16:34:48 (UTC)	
0.indexArrays	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	
0.indexBinDates	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	

Hex Strings Preview Metadata Location Record

Data Interpreter Data Fork

Type	Value (Little Endian)
Date/Time	
Chrome	
Cocoa/Webkit	
Cocoa Nanoseconds	
DOS	n/a (???)
FILETIME	
Firefox	
Java	
OLE	
OS X	
Unix	
Integer	
8 bit signed	
8 bit unsigned	
16 bit signed	
16 bit unsigned	
32 bit signed	
32 bit unsigned	
64 bit signed	
64 bit unsigned	
Float	
Single (4 byte)	
Double (8 byte)	
Other	
Base64	

Decimal Go To Position Sector Offset: 0x57 (87) Position: 0x4A5257 (4870743) Selection: 1

(1 of 227) - /Racer/Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/.store.db

First attribute table
contents: key names
kMDItemWhatever



Case Info

Report

Details

Browsers

File Filter

Actionable Intel

Communication

Media

Locations

Internet

Productivity

System

Plugins

Notifications

EVIDENCE

Add

Bennett-Computer-19030...

1

Racer

2

1b1ce46edadab95d64...

3

racer

4

racer (Carved Files)

5

carvertest.dmg

6

carvertest

7

carvertest (Carved F...

ACTIVITY

Export Status

Evidence Status

CONTENT SEARCHES

Add

INDEX SEARCHES

Add

TAGS

Add

INVESTIGATIVE NOTES

Add

Field

Value

BBTID:

39279

FileSystemID:

401445

Name:

.store.db

Path:

/.Spotlight-V100/Store-V

Size:

19173376

SizeOnDisk:

19173376

Extension:

db

ContentExt...

Date Created:

2015-06-11 22:55:11 (UT

Date Chang...

2019-02-26 14:17:52 (U

Date Modifi...

2019-02-26 14:17:52 (U

Date Acces...

2019-02-26 14:17:50 (U

FileSystem...

UTC

fsType:

APFS

Directory:

No

Visible:

Yes

Locked:

No

Root

Name

Date Created

Date Modified

Date Accessed

Date Ad

Store-V1

2015-06-11 22:55:11 (UTC)

2015-06-11 22:55:11 (UTC)

2015-06-11 22:55:11 (UTC)

Store-V2

2015-06-11 22:55:11 (UTC)

2015-06-11 23:46:27 (UTC)

2016-12-08 14:48:33 (UTC)

B6423D63-F381-46C0-80BE-...

2015-06-11 23:46:27 (UTC)

2017-11-14 13:28:38 (UTC)

2017-11-29 20:01:38 (UTC)

CC48CF65-F311-448D-875B-...

2015-06-11 22:55:11 (UTC)

2019-02-26 14:17:51 (UTC)

2019-02-26 13:23:14 (UTC)

.store.db

2015-06-11 22:55:11 (UTC)

2019-02-26 14:17:52 (UTC)

2019-02-26 14:17:50 (UTC)

0.directoryStoreFile

2018-12-12 18:40:42 (UTC)

2019-02-26 13:23:14 (UTC)

2019-02-26 14:18:02 (UTC)

0.directoryStoreFile.shadow

2018-12-12 18:40:42 (UTC)

2019-01-30 16:34:31 (UTC)

2019-01-30 16:34:48 (UTC)

0.indexArrays

2018-12-12 18:40:42 (UTC)

2018-12-12 18:40:52 (UTC)

2019-02-26 14:18:02 (UTC)

0.indexBinDates

2018-12-12 18:40:42 (UTC)

2018-12-12 18:40:52 (UTC)

2019-02-26 14:18:02 (UTC)

Hex

Strings

Preview

Metadata

Location

Record

Data Interpreter

Data Fork

00036784:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00036800:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00036816:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00036832:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00036848:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00036864:

32 70 62 64 00 40 00 00 F6 3F 00 00 21 00 00 00

2pbd.@..ö?..!...

00036880:

00 00 00 00 1D 00 00 00 00 0C 80 0E F3 7F 00 00

.....6...

00036896:

01 00 00 00 70 75 62 6C 69 63 2E 6D 65 73 73 61

....public.messa

00036912:

67 65 00 02 00 00 00 63 6F 6D 2E 61 70 70 6C 65

ge....com.apple

00036928:

2E 6D 61 69 6C 2E 65 6D 6C 78 00 03 00 00 00 63

.mail.emlx.....c

00036944:

6F 6D 2E 61 70 70 6C 65 2E 6D 61 69 6C 2E 65 6D

om.apple.mail.em

00036960:

6C 00 04 00 00 00 63 6F 6D 2E 6D 69 63 72 6F 73

l....com.micros

00036976:

6F 66 74 2E 65 6E 74 6F 75 72 61 67 65 2E 76 69

oft.entourage.vi

00036992:

72 74 75 61 6C 2E 6D 65 73 73 61 67 65 00 05 00

rtual.message...

00037008:

00 00 63 6F 6D 2E 61 70 70 6C 65 2E 69 63 68 61

..com.apple.icha

00037024:

74 2E 74 72 61 6E 73 63 72 69 70 74 00 06 00 00

t.transcript....

00037040:

00 70 75 62 6C 69 63 2E 63 6F 6E 74 61 63 74 00

.public.contact.

00037056:

07 00 00 00 70 75 62 6C 69 63 2E 76 63 61 72 64

....public.vcard

00037072:

00 08 00 00 00 63 6F 6D 2E 61 70 70 6C 65 2E 61

....com.apple.a

00037088:

64 64 72 65 73 73 62 6F 6F 6B 2E 70 65 72 73 6F

ddressbook.perso

00037104:

6E 00 09 00 00 00 63 6F 6D 2E 61 70 70 6C 65 2E

n....com.apple.

00037120:

61 64 64 72 65 73 73 6F 6F 6F 6B 2E 67 72 6F 75

addressbook.grou

00037136:

70 00 0A 00 00 00 63 6F 6D 2E 6D 69 63 72 6F 73

p....com.micros

00037152:

6F 66 74 2E 65 6E 74 6F 75 72 61 67 65 2E 76 69

oft.entourage.vi

00037168:

72 74 75 61 6C 2E 63 6F 6E 74 61 63 74 00 0B 00

rtual.contact...

00037184:

00 00 63 6F 6D 2E 6D 69 63 72 6F 73 6F 66 74 2E

..com.microsoft.

00037200:

65 6E 74 6F 75 72 61 67 65 2E 76 69 72 74 75 61

entourage.virtua

00037216:

6C 2E 67 72 6F 75 70 00 0C 00 00 00 63 6F 6D 2E

l.group....com.

Decimal

Go To Position

Sector Offset: 0x163 (355)

Position: 0x9163 (37219)

Selection: 0x4

Little Endian

(1 of 227) - /Racer/.Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/.store.db

Second attribute table:
page header



Case Info

Report

Details

Browser

File Filter

Actionable Intel

Communication

Media

Locations

Internet

Productivity

System

Plugins

Notifications

EVIDENCE

Add

Bennett-Computer-19030...

1

Racer

2

1b1ce46edadab95d64...

3

racer

4

racer (Carved Files)

5

carvertest

7

carvertest (Carved F...

ACTIVITY

Export Status

Evidence Status

CONTENT SEARCHES

INDEX SEARCHES

TAGS

INVESTIGATIVE NOTES

Field

Value

BBTID:

39279

FileSystemID:

401445

Name:

.store.db

Path:

/.Spotlight-V100/Store-V

Size:

19173376

SizeOnDisk:

19173376

Extension:

db

Date Created:

2015-06-11 22:55:11 (UT

Date Chang...

2019-02-26 14:17:52 (U

Date Modifi...

2019-02-26 14:17:52 (U

Date Acces...

2019-02-26 14:17:50 (U

FileSystem...

UTC

fsType:

APFS

Directory:

No

Visible:

Yes

Locked:

No

Root

Name

Date Created

Date Modified

Date Accessed

Date Ad

Store-V1

2015-06-11 22:55:11 (UTC)

2015-06-11 22:55:11 (UTC)

2015-06-11 22:55:11 (UTC)

Store-V2

2015-06-11 22:55:11 (UTC)

2015-06-11 23:46:27 (UTC)

2016-12-08 14:48:33 (UTC)

B6423D63-F381-46C0-80BE-...

2015-06-11 23:46:27 (UTC)

2017-11-14 13:28:38 (UTC)

2017-11-29 20:01:38 (UTC)

CC48CF65-F311-448D-875B-...

2015-06-11 22:55:11 (UTC)

2019-02-26 14:17:51 (UTC)

2019-02-26 13:23:14 (UTC)

.store.db

2015-06-11 22:55:11 (UTC)

2019-02-26 14:17:52 (UTC)

2019-02-26 14:17:50 (UTC)

0.directoryStoreFile

2018-12-12 18:40:42 (UTC)

2019-02-26 13:23:14 (UTC)

2019-02-26 14:18:02 (UTC)

0.directoryStoreFile.shadow

2018-12-12 18:40:42 (UTC)

2019-01-30 16:34:31 (UTC)

2019-01-30 16:34:48 (UTC)

0.indexArrays

2018-12-12 18:40:42 (UTC)

2018-12-12 18:40:52 (UTC)

2019-02-26 14:18:02 (UTC)

0.indexBinDates

2018-12-12 18:40:42 (UTC)

2018-12-12 18:40:52 (UTC)

2019-02-26 14:18:02 (UTC)

Hex

Strings

Preview

Metadata

Location

Record

00036784:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00036800:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00036816:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00036832:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00036848:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00036864:

32 70 62 64 00 40 00 00 F6 3F 00 00 21 00 00 00

2pbd.@.ö?..!...

00036880:

00 00 00 00 1D 00 00 00 00 0C 80 0E F3 7F 00 00

.....ó...

00036896:

01 00 00 00 70 75 62 6C 69 63 2E 6D 65 73 73 61

...public.messa

00036912:

67 65 00 02 00 00 00 63 6F 6D 2E 61 70 70 6C 65

ge....com.apple

00036928:

2E 6D 61 69 6C 2E 65 6D 6C 78 00 03 00 00 00 63

.mail.emlx....c

00036944:

6F 6D 2E 61 70 70 6C 65 2E 6D 61 69 6C 2E 65 6D

om.apple.mail.em

00036960:

6C 00 04 00 00 00 63 6F 6D 2E 6D 69 63 72 6F 73

l....com.micros

00036976:

6F 66 74 2E 65 6E 74 6F 75 72 61 67 65 2E 76 69

oft.entourage.vi

00036992:

72 74 75 61 6C 2E 6D 65 73 73 61 67 65 00 05 00

rtual.message...

00037008:

00 00 63 6F 6D 2E 61 70 70 6C 65 2E 69 63 68 61

..com.apple.icha

00037024:

74 2E 74 72 61 6E 73 63 72 69 70 74 00 06 00 00

t.transcript....

00037040:

00 70 75 62 6C 69 63 2E 63 6F 6E 74 61 63 74 00

.public.contact.

00037056:

07 00 00 00 70 75 62 6C 69 63 2E 76 63 61 72 64

....public.vcard

00037072:

00 08 00 00 00 63 6F 6D 2E 61 70 70 6C 65 2E 61

....com.apple.a

00037088:

64 64 72 65 73 73 62 6F 6F 6B 2E 70 65 72 73 6F

ddressbook.perso

00037104:

6E 00 09 00 00 00 63 6F 6D 2E 61 70 70 6C 65 2E

n....com.apple.

00037120:

61 64 64 72 65 73 73 62 6F 6F 6B 2E 67 72 6F 75

addressbook.grou

00037136:

70 00 0A 00 00 00 63 6F 6D 2E 6D 69 63 72 6F 73

p....com.micros

00037152:

6F 66 74 2E 65 6E 74 6F 75 72 61 67 65 2E 76 69

oft.entourage.vi

00037168:

72 74 75 61 6C 2E 63 6F 6E 74 61 63 74 00 0B 00

rtual.contact...

00037184:

00 00 63 6F 6D 2E 6D 69 63 72 6F 73 6F 66 74 2E

..com.microsoft.

00037200:

65 6E 74 6F 75 72 61 67 65 2E 76 69 72 74 75 61

entourage.virtua

00037216:

6C 2E 67 72 6F 75 70 00 0C 00 00 63 6F 6D 2E

l.group....com.

Type

Value (Littl...

Date/Time

Chrome

1601-01-01 ...

Cocoa/Webkit

2001-01-01 ...

Cocoa Nanoseconds

DOS

1979-11-30 ...

FILETIME

Firefox

1970-01-01 ...

Java

1970-01-01 ...

OLE

OS X

1904-01-01 ...

Unix

1970-01-01 ...

Integer

8 bit signed

29

8 bit unsigned

29

16 bit signed

29

16 bit unsigned

29

32 bit signed

29

32 bit unsigned

29

64 bit signed

64 bit unsigned

Float

Single (4 byte)

4.063766e-...

Double (8 byte)

Other

Base64

Decimal

Go To Position

Sector Offset: 0x1C6 (454)

Position: 0x8FC6 (36806)

Selection: 0x

Little Endian

(1 of 227)

- /Racer/.Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/.store.db

Second attribute table:
next page offset in 4kb
blocks

Spotlight.blacklight

Case Info Report Details

Browser File Filter Actionable Intel Communication Media Locations Internet Productivity System Plugins Notifications

EVIDENCE Add

▼ ☒ Bennett-Computer-19030...

☒ 1 Racer

☐ 2 1b1ce46edadab95d64...

▼ ☐ Racer.dmg.dd

☐ 3 racer

☐ 4 racer (Carved Files)

▼ ☐ carvertest.dmg

☐ 5 carvertest

☐ 7 carvertest (Carved F...

ACTIVITY

Export Status

Evidence Status

CONTENT SEARCHES Add

INDEX SEARCHES Add

TAGS Add

INVESTIGATIVE NOTES Add

Name	Date Created	Date Modified	Date Accessed	Date Ad
Store-V1	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	
Store-V2	2015-06-11 22:55:11 (UTC)	2015-06-11 23:46:27 (UTC)	2016-12-08 14:48:33 (UTC)	
B6423D63-F381-46C0-80BE-...	2015-06-11 23:46:27 (UTC)	2017-11-14 13:28:38 (UTC)	2017-11-29 20:01:38 (UTC)	
CC48CF65-F311-448D-875B-...	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:51 (UTC)	2019-02-26 13:23:14 (UTC)	
.store.db	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:52 (UTC)	2019-02-26 14:17:50 (UTC)	
0.directoryStoreFile	2018-12-12 18:40:42 (UTC)	2019-02-26 13:23:14 (UTC)	2019-02-26 14:18:02 (UTC)	
0.directoryStoreFile.shadow	2018-12-12 18:40:42 (UTC)	2019-01-30 16:34:31 (UTC)	2019-01-30 16:34:48 (UTC)	
0.indexArrays	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	
0.indexBinDates	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	

Hex Strings Preview Metadata Location Record

Data Interpreter Data Fork

Type	Value (Little Endian)
Date/Time	
Chrome	
Cocoa/Webkit	
Cocoa Nanoseconds	
DOS	n/a (???)
FILETIME	
Firefox	
Java	
OLE	
OS X	
Unix	
Integer	
8 bit signed	
8 bit unsigned	
16 bit signed	
16 bit unsigned	
32 bit signed	
32 bit unsigned	
64 bit signed	
64 bit unsigned	
Float	
Single (4 byte)	
Double (8 byte)	
Other	
Base64	

Field Value

BBTID: 39279

FileSystemID: 401445

Name: .store.db

Path: /.Spotlight-V100/Store-V

Size: 19173376

SizeOnDisk: 19173376

Extension: db

ContentExt...

Date Created: 2015-06-11 22:55:11 (UTC)

Date Chang... 2019-02-26 14:17:52 (UTC)

Date Modifi... 2019-02-26 14:17:52 (UTC)

Date Acces... 2019-02-26 14:17:50 (UTC)

FileSystem... UTC

fsType: APFS

Directory: No

Visible: Yes

Locked: No

Decimal Go To Position Sector Offset: 0x0 (0) Position: 0x0 (0) Selection: 0x88 (136)

(1 of 227) - /Racer/.Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/.store.db

Second attribute table
contents: value data



Records (Finally)

Records

- Organized into pages like the other data we've seen
- Pages often compressed
 - lz4
 - Deflate
- Composed of
 - Length of record
 - Inode*
 - Flags*
 - Unique item identifier*
 - Parent inode*
 - Date updated
 - A set of key/value pairs

* Indicates a variable length integer

Case Info

Report

Details

Browser

File Filter

Actionable Intel

Communication

Media

Locations

Internet

Productivity

System

Plugins

Notifications

EVIDENCE

Add

Bennett-Computer-19030...

1

Racer

2

1b1ce46edadab95d64...

3

racer

4

racer (Carved Files)

5

carvertest

7

carvertest (Carved F...

ACTIVITY

Export Status

Evidence Status

CONTENT SEARCHES

Add

INDEX SEARCHES

Add

TAGS

Add

INVESTIGATIVE NOTES

Add

Field

Value

BBTID:

39279

FileSystemID:

401445

Name:

.store.db

Path:

/.Spotlight-V100/Store-V

Size:

19173376

SizeOnDisk:

19173376

Extension:

db

ContentExt...

Date Created:

2015-06-11 22:55:11 (UT

Date Chang...

2019-02-26 14:17:52 (U

Date Modifi...

2019-02-26 14:17:52 (U

Date Acces...

2019-02-26 14:17:50 (U

FileSystem...

UTC

fsType:

APFS

Directory:

No

Visible:

Yes

Locked:

No

Root

Name

Date Created

Date Modified

Date Accessed

Date Ad

Store-V1

2015-06-11 22:55:11 (UTC)

2015-06-11 22:55:11 (UTC)

2015-06-11 22:55:11 (UTC)

2015-06-11 22:55:11 (UTC)

Store-V2

2015-06-11 22:55:11 (UTC)

2015-06-11 23:46:27 (UTC)

2016-12-08 14:48:33 (UTC)

2016-12-08 14:48:33 (UTC)

B6423D63-F381-46C0-80BE-...

2015-06-11 23:46:27 (UTC)

2017-11-14 13:28:38 (UTC)

2017-11-29 20:01:38 (UTC)

2017-11-29 20:01:38 (UTC)

CC48CF65-F311-448D-875B-...

2015-06-11 22:55:11 (UTC)

2019-02-26 14:17:51 (UTC)

2019-02-26 13:23:14 (UTC)

2019-02-26 13:23:14 (UTC)

.store.db

2015-06-11 22:55:11 (UTC)

2019-02-26 14:17:52 (UTC)

2019-02-26 14:17:50 (UTC)

2019-02-26 14:17:50 (UTC)

0.directoryStoreFile

2018-12-12 18:40:42 (UTC)

2019-02-26 13:23:14 (UTC)

2019-02-26 14:18:02 (UTC)

2019-02-26 14:18:02 (UTC)

0.directoryStoreFile.shadow

2018-12-12 18:40:42 (UTC)

2019-01-30 16:34:31 (UTC)

2019-01-30 16:34:48 (UTC)

2019-01-30 16:34:48 (UTC)

0.indexArrays

2018-12-12 18:40:42 (UTC)

2018-12-12 18:40:52 (UTC)

2019-02-26 14:18:02 (UTC)

2019-02-26 14:18:02 (UTC)

0.indexBigDates

2018-12-12 18:40:42 (UTC)

2018-12-12 18:40:52 (UTC)

2019-02-26 14:18:02 (UTC)

2019-02-26 14:18:02 (UTC)

Hex

Strings

Preview

Metadata

Location

Record

Data Interpreter

Data Fork

00872288:

00 00 BF 28 00 00 C0 28 00 00 C1 28 00 00 C2 28

..zC..AC..AC..AC

00872304:

00 00 C3 28 00 00 C4 28 00 00 C5 28 00 00 C6 28

..AC..AC..AC..AC

00872320:

00 00 C7 28 00 00 C8 28 00 00 C9 28 00 00 CA 28

..CC..EC..EC..EC

00872336:

00 00 CB 28 00 00 CC 28 00 00 CD 28 00 00 CE 28

..EC..IC..IC..IC

00872352:

00 00 CF 28 00 00 D0 28 00 00 D1 28 00 00 D2 28

..IC..DC..NC..OC

00872368:

00 00 D3 28 00 00 D4 28 00 00 00 00 00 00 00 00

..OC..OC.....

00872384:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00872400:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00872416:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00872432:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

00872448:

32 70 62 64 00 40 00 00 30 03 00 00 09 00 00 00

zpb@..0.....

00872464:

C3 07 00 00 78 5E A5 93 5F 48 53 51 1C C7 CF B9

Ä...x^Y..HSQ.ÇI¹

00872480:

CE 6E D6 5C B5 4C B2 44 6F 44 84 D1 2E 6E D0 CA

ÎnÖµL²DoD.N.nÐÊ

00872496:

A8 60 A9 98 22 5A FE 41 82 C2 76 BD 57 B7 E6 FE

""@."ZpA.ÄvW.æp

00872512:

70 77 F7 D0 9F 87 CD 3F 50 D1 1F E8 C1 02 E9 8F

pw+D..Î?PN.èÄ.é.

00872528:

10 D1 43 A2 48 85 22 D1 2D 65 81 FA 10 41 F8 50

..NCqH."N-e.ú.AøP

00872544:

92 BD 47 FF F7 D0 CB EA 9C B3 EB F1 3A DD D4 62

..%Gy+DÊè.³èñ:YOb

00872560:

2F 67 E7 9C DF B9 DF DF E7 7C 8E 0A 00 98 DC F4

/gç.B¹Bßçl...Üô

00872576:

9B 7B 75 BB EA 07 D8 D3 B0 3B 9E 79 71 FA 0A BB

..{u»è.00°;yqu.»

00872592:

37 C8 76 4A D0 C8 3C BA 01 CD 50 3D 03 8C DD 07

7EvJDÊ<°.IP=.Y.

00872608:

20 60 80 01 6D 7E 21 97 8F 3A A0 6C 12 7F F5 0D

..`..m~!...l..ö.

00872624:

A9 0E 08 D0 4F 3D 61 65 E8 0A 9A 60 00 CC 75 29

0..Ð0=aeè...`Îu)

00872640:

4A 40 E4 5B FC BE 56 3E 20 4B 96 50 40 74 2A 12

J@ä[üV>.K.P@t*.

00872656:

5A D1 0E A0 03 C3 D6 25 77 E6 32 20 13 84 6F C2

ZN. .ÄÖ%wæ2...oÄ

00872672:

F0 25 54 01 0A D1 97 70 45 F8 59 D9 A8 A3 70 FE

ð%T. .N.pEøYÜ~`fpp

00872688:

53 DA 4C 0F EE 21 AF 97 EB F9 10 95 6A 71 03 97

SÜL.i!`..èü..jq..

00872704:

FB 1D 33 6C 16 CA BF 13 66 65 DB 61 0E 0A 04 32

û.3l.Êç.fEuA...2

00872720:

D0 A6 AF 0A CE 4E 07 91 D8 82 69 12 9C 2D 0D 05

Ð!`..IN..0.i...-

Decimal

Go To Position

Sector Offset: 0x173 (371)

Position: 0xD4F73 (872307)

Selection: 0x

Little Endian

(1 of 227)

-.Racer/.Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/.store.db

Record page header



Case Info

Report

Details

Browser

File Filter

Actionable Intel

Communication

Media

Locations

Internet

Productivity

System

Plugins

Notifications

EVIDENCE

Add

Bennett-Computer-19030...

1

Racer

2

1b1ce46edadab95d64...

3

racer

4

racer (Carved Files)

5

carvertest

7

carvertest (Carved F...

ACTIVITY

Export Status

Evidence Status

CONTENT SEARCHES

Add

INDEX SEARCHES

Add

TAGS

Add

INVESTIGATIVE NOTES

Add

Field	Value
BBTID:	39279
FileSystemID:	401445
Name:	.store.db
Path:	/.Spotlight-V100/Store-V
Size:	19173376
SizeOnDisk:	19173376
Extension:	db
ContentExte...	
Date Created:	2015-06-11 22:55:11 (UT
Date Chang...	2019-02-26 14:17:52 (UT
Date Modifi...	2019-02-26 14:17:52 (UT
Date Acces...	2019-02-26 14:17:50 (U
FileSystem...	UTC
fsType:	APFS
Directory:	No
Visible:	Yes
Locked:	No

Root

Name	Date Created	Date Modified	Date Accessed	Date Ad
Store-V1	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	
Store-V2	2015-06-11 22:55:11 (UTC)	2015-06-11 23:46:27 (UTC)	2016-12-08 14:48:33 (UTC)	
B6423D63-F381-46C0-80BE-...	2015-06-11 23:46:27 (UTC)	2017-11-14 13:28:38 (UTC)	2017-11-29 20:01:38 (UTC)	
CC48CF65-F311-448D-875B-...	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:51 (UTC)	2019-02-26 13:23:14 (UTC)	
.store.db	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:52 (UTC)	2019-02-26 14:17:50 (UTC)	
0.directoryStoreFile	2018-12-12 18:40:42 (UTC)	2019-02-26 13:23:14 (UTC)	2019-02-26 14:18:02 (UTC)	
0.directoryStoreFile.shadow	2018-12-12 18:40:42 (UTC)	2019-01-30 16:34:31 (UTC)	2019-01-30 16:34:48 (UTC)	
0.indexArrays	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	
0.indexBigData...	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	

Hex

Strings

Preview

Metadata

Location

Record

Data Interpreter

Data Fork

Type	Value (Litt...
Date/Time	
Chrome	1601-01-01...
Cocoa/Webkit	2001-01-0...
Cocoa Nanoseconds	
DOS	1979-11-3...
FILETIME	
Firefox	1970-01-0...
Java	1970-01-0...
OLE	
OS X	1904-01-0...
Unix	1970-01-0...
Integer	
8 bit signed	0
8 bit unsigned	0
16 bit signed	16384
16 bit unsigned	16384
32 bit signed	16384
32 bit unsigned	16384
64 bit signed	
64 bit unsigned	
Float	
Single (4 byte)	2.295887e...
Double (8 byte)	
Other	
Base64	

Decimal

Go To Position

Sector Offset: 0x190 (400)

Position: 0xD4F90 (872336)

Selection: C

Little Endian

(1 of 227)

- /Racer/.Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/.store.db

Record page length

Case Info

Report

Details

Browser

File Filter

Actionable Intel

Communication

Media

Locations

Internet

Productivity

System

Plugins

Notifications

EVIDENCE

Add

Bennett-Computer-19030...

1

Racer

2

1b1ce46edadab95d64...

3

racer

4

racer (Carved Files)

5

carvertest

7

carvertest (Carved F...

ACTIVITY

Export Status

Evidence Status

CONTENT SEARCHES

INDEX SEARCHES

TAGS

INVESTIGATIVE NOTES

Field

Value

BBTID: 39279

FileSystemID: 401445

Name: .store.db

Path: /Spotlight-V100/Store-V

Size: 19173376

SizeOnDisk: 19173376

Extension: db

ContentExte...

Date Created: 2015-06-11 22:55:11 (UT

Date Chang... 2019-02-26 14:17:52 (UT

Date Modifi... 2019-02-26 14:17:52 (UT

Date Acces... 2019-02-26 14:17:50 (UT

FileSystem... UTC

fsType: APFS

Directory: No

Visible: Yes

Locked: No

Root

Name	Date Created	Date Modified	Date Accessed	Date Ad
Store-V1	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	
Store-V2	2015-06-11 22:55:11 (UTC)	2015-06-11 23:46:27 (UTC)	2016-12-08 14:48:33 (UTC)	
B6423D63-F381-46C0-80BE-...	2015-06-11 23:46:27 (UTC)	2017-11-14 13:28:38 (UTC)	2017-11-29 20:01:38 (UTC)	
CC48CF65-F311-448D-875B-...	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:51 (UTC)	2019-02-26 13:23:14 (UTC)	
.store.db	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:52 (UTC)	2019-02-26 14:17:50 (UTC)	
0.directoryStoreFile	2018-12-12 18:40:42 (UTC)	2019-02-26 13:23:14 (UTC)	2019-02-26 14:18:02 (UTC)	
0.directoryStoreFile.shadow	2018-12-12 18:40:42 (UTC)	2019-01-30 16:34:31 (UTC)	2019-01-30 16:34:48 (UTC)	
0.indexArrays	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	
0.indexBigData...	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	

Hex

Strings

Preview

Metadata

Location

Record

00872288: 00 00 BF 28 00 00 C0 28 00 00 C1 28 00 00 C2 28

00872304: 00 00 C3 28 00 00 C4 28 00 00 C5 28 00 00 C6 28

00872320: 00 00 C7 28 00 00 C8 28 00 00 C9 28 00 00 CA 28

00872336: 00 00 CB 28 00 00 CC 28 00 00 CD 28 00 00 CE 28

00872352: 00 00 CF 28 00 00 D0 28 00 00 D1 28 00 00 D2 28

00872368: 00 00 D3 28 00 00 D4 28 00 00 00 00 00 00 00 00

00872384: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00872400: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00872416: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00872432: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00872448: 32 70 62 64 00 40 00 00 30 03 00 00 09 00 00 00

00872464: C3 07 00 00 78 5E A5 93 5F 48 53 51 1C C7 CF B9

00872480: CE 6E D6 5C B5 4C B2 44 6F 44 84 D1 2E 6E D0 CA

00872496: A8 60 A9 98 22 5A FE 41 82 C2 76 BD 57 B7 E6 FE

00872512: 70 77 F7 D0 9F 87 CD 3F 50 D1 1F E8 C1 02 E9 8F

00872528: 10 D1 43 A2 48 85 22 D1 2D 65 81 FA 10 41 F8 50

00872544: 92 BD 47 FF F7 D0 CB EA 9C B3 EB F1 3A DD D4 62

00872560: 2F 67 E7 9C DF B9 DF DF E7 7C 8E 0A 00 98 DC F4

00872576: 9B 7B 75 BB EA 07 D8 D3 B0 3B 9E 79 71 FA 0A BB

00872592: 37 C8 76 4A D0 C8 3C BA 01 CD 50 3D 03 8C D0 07

00872608: 20 60 80 01 6D 7E 21 97 8F 3A A0 6C 12 7F F5 0D

00872624: A9 0E 08 D0 4F 3D 61 65 E8 0A 9A 60 00 CC 75 29

00872640: 4A 40 E4 5B FC BE 56 3E 20 4B 96 50 40 74 2A 12

00872656: 5A D1 0E A0 03 C3 D6 25 77 E6 32 20 13 84 6F C2

00872672: F0 25 54 01 0A D1 97 70 45 F8 59 D9 A8 A3 70 FE

00872688: 53 DA 4C 0F EE 21 AF 9F EF F9 10 95 6A 71 03 97

00872704: FB 1D 33 6C 16 CA BF 13 66 65 DB 61 0E 0A 04 32

00872720: D0 A6 AF 0A CE 4E 07 91 D8 82 69 12 9C 2D 0D 05

Decimal

Go To Position

Sector Offset: 0x170 (368)

Position: 0xD4F70 (872304)

Selection: 0

Little Endian

Record page used length

Spotlight.blacklight

Case Info Report Details

Browser File Filter Actionable Intel Communication Media Locations Internet Productivity System Plugins Notifications

EVIDENCE Add

▼ ☒ Bennett-Computer-19030...

☒ 1 Racer

☐ 2 1b1ce46edadab95d64...

▼ ☐ Racer.dmg.dd

☐ 3 racer

☐ 4 racer (Carved Files)

▼ ☐ carvertest.dmg

☐ 5 carvertest

☐ 7 carvertest (Carved F...

ACTIVITY

 Export Status

 Evidence Status

▼ **CONTENT SEARCHES** Add

▼ **INDEX SEARCHES** Add

▼ **TAGS** Add

▼ **INVESTIGATIVE NOTES** Add

Name	Date Created	Date Modified	Date Accessed	Date Ad
Store-V1	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	
Store-V2	2015-06-11 22:55:11 (UTC)	2015-06-11 23:46:27 (UTC)	2016-12-08 14:48:33 (UTC)	
B6423D63-F381-46C0-80BE-...	2015-06-11 23:46:27 (UTC)	2017-11-14 13:28:38 (UTC)	2017-11-29 20:01:38 (UTC)	
CC48CF65-F311-448D-875B-...	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:51 (UTC)	2019-02-26 13:23:14 (UTC)	
.store.db	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:52 (UTC)	2019-02-26 14:17:50 (UTC)	
0.directoryStoreFile	2018-12-12 18:40:42 (UTC)	2019-02-26 13:23:14 (UTC)	2019-02-26 14:18:02 (UTC)	
0.directoryStoreFile.shadow	2018-12-12 18:40:42 (UTC)	2019-01-30 16:34:31 (UTC)	2019-01-30 16:34:48 (UTC)	
0.indexArrays	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	
0.indexBisData	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	

Hex Strings Preview Metadata Location Record Data Interpreter Data Fork

Field	Value
BBTID:	39279
FileSystemID:	401445
Name:	.store.db
Path:	/.Spotlight-V100/Store-V
Size:	19173376
SizeOnDisk:	19173376
Extension:	db
ContentExt...	
Date Created:	2015-06-11 22:55:11 (UTC)
Date Chang...	2019-02-26 14:17:52 (UTC)
Date Modifi...	2019-02-26 14:17:52 (UTC)
Date Acces...	2019-02-26 14:17:50 (UTC)
FileSystem...	UTC
fsType:	APFS
Directory:	No
Visible:	Yes
Locked:	No

Type	Value (Little Endian)
Date/Time	
Chrome	1601-01-01...
Cocoa/Webkit	2001-01-0...
Cocoa Nanoseconds	
DOS	1979-11-3...
FILETIME	
Firefox	1970-01-0...
Java	1970-01-0...
OLE	
OS X	1904-01-0...
Unix	1970-01-0...
Integer	
8 bit signed	9
8 bit unsigned	9
16 bit signed	9
16 bit unsigned	9
32 bit signed	9
32 bit unsigned	9
64 bit signed	
64 bit unsigned	
Float	
Single (4 byte)	1.261169e-...
Double (8 byte)	
Other	
Base64	

00872288: 00 00 BF 28 00 00 C0 28 00 00 C1 28 00 00 C2 28 ..zC..AC..AC..AC
00872304: 00 00 C3 28 00 00 C4 28 00 00 C5 28 00 00 C6 28 ..AC..AC..AC..AC
00872320: 00 00 C7 28 00 00 C8 28 00 00 C9 28 00 00 CA 28 ..C..E..E..E
00872336: 00 00 CB 28 00 00 CC 28 00 00 CD 28 00 00 CE 28 ..E..I..I..I
00872352: 00 00 CF 28 00 00 D0 28 00 00 D1 28 00 00 D2 28 ..I..D..N..D
00872368: 00 00 D3 28 00 00 D4 28 00 00 00 00 00 00 00 00 ..D..D.....
00872384: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00872400: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00872416: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00872432: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00872448: 32 70 62 64 00 40 00 00 30 03 00 00 09 00 00 00 2pbd.@..0...
00872464: C3 07 00 00 78 5E A5 93 5F 48 53 51 1C C7 CF B9 A...x^_..HSQ.CI
00872480: CE 6E D6 5C B5 4C B2 44 6F 44 84 D1 2E 6E D0 CA InO\pL^DoD.N.nD
00872496: A8 60 A9 98 22 5A FE 41 82 C2 76 BD 57 B7 E6 FE ""O."ZpA.AvW.a
00872512: 70 77 F7 D0 9F 87 CD 3F 50 D1 1F E8 C1 02 E9 8F pw+D..I?PN.eA.e.
00872528: 10 D1 43 A2 48 85 22 D1 2D 65 81 FA 10 41 F8 50 .NCqH."N-e..u.AoP
00872544: 92 BD 47 FF F7 D0 CB EA 9C B3 EB F1 3A DD D4 62 .%Gy+DEe..3en:YOb
00872560: 2F 67 E7 9C DF B9 DF DF E7 7C 8E 0A 00 98 DC F4 /gc.B^B8cI...Uo
00872576: 9B 78 75 BB EA 07 D8 D3 B0 3B 9E 79 71 FA 0A BB {u»e..00°;.yqu.»
00872592: 37 C8 76 4A D0 C8 3C BA 01 CD 50 3D 03 8C DD 07 7EvJDE<°.IP=..Y.
00872608: 20 60 80 01 6D 7E 21 97 8F 3A A0 6C 12 7F F5 0D .'.m~!...:l..o.
00872624: A9 0E 08 D0 4F 3D 61 65 E8 0A 9A 60 00 CC 75 29 @..D0=aeè..'.Iu)
00872640: 4A 40 E4 5B FC BE 56 3E 20 4B 96 50 40 74 2A 12 J@a[üXV>.K.Pet*.
00872656: 5A D1 0E A0 03 C3 D6 25 77 E6 32 20 13 84 6F C2 ZN..AÖ%wæ2...oA
00872672: F0 25 54 01 0A D1 97 70 45 F8 59 D9 A8 A3 70 FE %T..N.pEoYÜ"Épp
00872688: 53 DA 4C 0F EE 21 AF 97 EB F9 10 95 6A 71 03 97 SÚL.i!~.èü..jq..
00872704: FB 1D 33 6C 16 CA BF 13 66 65 DB 61 0E 0A 04 32 ú.3l.Êz.feüa...2
00872720: D0 A6 AF 0A CE 4E 07 91 D8 82 69 12 9C 2D 0D 05 DI~.IN..ø.i...~

Decimal Go To Position Sector Offset: 0x0 (0) Position: 0x0 (0) Selection: 0x4 (4)

(1 of 227) - /Racer/.Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/.store.db

Flags (can indicate compression, as it does here)

Spotlight.blacklight

Case Info Report Details

Browser File Filter Actionable Intel Communication Media Locations Internet Productivity System Plugins Notifications

EVIDENCE Add

- ✓ Bennett-Computer-19030...
 - ✓ 1 Racer
 - 2 1b1ce46edadab95d64...
- Racer.dmg.dd
 - 3 racer
 - 4 racer (Carved Files)
- carvertest.dmg
 - 5 carvertest
 - 7 carvertest (Carved F...

ACTIVITY

- Export Status
- Evidence Status

CONTENT SEARCHES Add

INDEX SEARCHES Add

TAGS Add

INVESTIGATIVE NOTES Add

Field	Value
BBTID:	39279
FileSystemID:	401445
Name:	.store.db
Path:	./Spotlight-V100/Store-V
Size:	19173376
SizeOnDisk:	19173376
Extension:	db
ContentExt...	
Date Created:	2015-06-11 22:55:11 (UT
Date Chang...	2019-02-26 14:17:52 (UT
Date Modifi...	2019-02-26 14:17:52 (UT
Date Acces...	2019-02-26 14:17:50 (UT
FileSystem...	UTC
fsType:	APFS
Directory:	No
Visible:	Yes
Locked:	No

Name	Date Created	Date Modified	Date Accessed	Date Ad
Store-V1	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	2015-06-11 22:55:11 (UTC)	
Store-V2	2015-06-11 22:55:11 (UTC)	2015-06-11 23:46:27 (UTC)	2016-12-08 14:48:33 (UTC)	
B6423D63-F381-46C0-80BE-...	2015-06-11 23:46:27 (UTC)	2017-11-14 13:28:38 (UTC)	2017-11-29 20:01:38 (UTC)	
CC48CF65-F311-448D-875B-...	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:51 (UTC)	2019-02-26 13:23:14 (UTC)	
.store.db	2015-06-11 22:55:11 (UTC)	2019-02-26 14:17:52 (UTC)	2019-02-26 14:17:50 (UTC)	
0.directoryStoreFile	2018-12-12 18:40:42 (UTC)	2019-02-26 13:23:14 (UTC)	2019-02-26 14:18:02 (UTC)	
0.directoryStoreFile.shadow	2018-12-12 18:40:42 (UTC)	2019-01-30 16:34:31 (UTC)	2019-01-30 16:34:48 (UTC)	
0.indexArrays	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	
0.indexBisData...	2018-12-12 18:40:42 (UTC)	2018-12-12 18:40:52 (UTC)	2019-02-26 14:18:02 (UTC)	

Hex Strings Preview Metadata Location Record

Data Interpreter Data Fork

Type	Value (Litt...
Date/Time	
Chrome	1601-01-01...
Cocoa/Webkit	2001-01-0...
Cocoa Nanoseconds	
DOS	1979-11-3...
FILETIME	
Firefox	1970-01-0...
Java	1970-01-0...
OLE	
OS X	1904-01-0...
Unix	1970-01-0...
Integer	
8 bit signed	-61
8 bit unsigned	195
16 bit signed	1987
16 bit unsigned	1987
32 bit signed	1987
32 bit unsigned	1987
64 bit signed	
64 bit unsigned	
Float	
Single (4 byte)	2.784380e...
Double (8 byte)	
Other	
Base64	

00872288: 00 00 BF 28 00 00 C0 28 00 00 C1 28 00 00 C2 28 ..zC..AC..AC..AC
00872304: 00 00 C3 28 00 00 C4 28 00 00 C5 28 00 00 C6 28 ..AC..AC..AC..AC
00872320: 00 00 C7 28 00 00 C8 28 00 00 C9 28 00 00 CA 28 ..C..E..E..E
00872336: 00 00 CB 28 00 00 CC 28 00 00 CD 28 00 00 CE 28 ..E..I..I..I
00872352: 00 00 CF 28 00 00 D0 28 00 00 D1 28 00 00 D2 28 ..I..D..N..D
00872368: 00 00 D3 28 00 00 D4 28 00 00 00 00 00 00 00 00 ..D..D.....
00872384: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00872400: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00872416: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00872432: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00872448: 32 70 62 64 00 40 00 00 30 03 00 00 09 00 00 00 2pbd.@..0.....
00872464: C3 07 00 00 78 5E A5 93 5F 48 53 51 1C C7 CF B9 A...x^_HSQ.Ci1
00872480: CE 6E D6 5C B5 4C B2 44 6F 44 84 D1 2E 6E D0 CA InOµL²DoD.N.nDÉ
00872496: A8 60 A9 98 22 5A FE 41 82 C2 76 BD 57 B7 E6 FE ""O."ZpA.ÂvZW·æp
00872512: 70 77 F7 D0 9F 87 CD 3F 50 D1 1F E8 C1 02 E9 8F pw+D..I?Pñ.èÁ.é.
00872528: 10 D1 43 A2 48 85 22 D1 2D 65 81 FA 10 41 F8 50 .NCqH."N-e.ú.AøP
00872544: 92 BD 47 FF F7 D0 CB EA 9C B3 EB F1 3A DD D4 62 .%Gy+DÉè.³èñ:YOb
00872560: 2F 67 E7 9C DF B9 DF DF E7 7C 8E 0A 00 98 DC F4 /gç.B¹Bçl...Üö
00872576: 9B 78 75 BB EA 07 D8 D3 B0 3B 9E 79 71 FA 0A BB .{u»è.00°;.yqu.»
00872592: 37 C8 76 4A D0 C8 3C BA 01 CD 50 3D 03 8C D0 07 7ÈvJÐÈ<º.ÎP=..Ý.
00872608: 20 60 80 01 6D 7E 21 97 8F 3A A0 6C 12 7F F5 0D .'.m~!...:l..ö.
00872624: A9 0E 08 D0 4F 3D 61 65 E8 0A 9A 60 00 CC 75 29 @..Ð0=aeè..'.Îu)
00872640: 4A 40 E4 5B FC BE 56 3E 20 48 96 50 40 74 2A 12 J@a[ü%V>.K.Pet*.
00872656: 5A D1 0E A0 03 C3 D6 25 77 E6 32 20 13 84 6F C2 ZÑ..ÄÖ%wæ2...oÅ
00872672: F0 25 54 01 0A D1 97 70 45 F8 59 D9 A8 A3 70 FE ø%T..Ñ.pEøYÜ"Épp
00872688: 53 DA 4C 0F EE 21 AF 97 EB F9 10 95 6A 71 03 97 SÚL.í!~.èù..jq..
00872704: FB 1D 33 6C 16 CA BF 13 66 65 DB 61 0E 0A 04 32 ú.3l.Êç.feûa...2
00872720: D0 A6 AF 0A CE 4E 07 91 D8 82 69 12 9C 2D 0D 05 ÐI~.ÎN..Ø.i...~

Decimal Go To Position Sector Offset: 0x178 (376) Position: 0xD4F78 (872312) Selection: 0

(1 of 227) - /Racer/Spotlight-V100/Store-V2/CC48CF65-F311-448D-875B-FDB1A25B5C78/.store.db

Uncompressed length



Spotlight.blacklight

Case Info Report Details

Browser File Filter Actionable Intel Communication Media Locations Internet Productivity System Plugins Notifications

EVIDENCE Add

- Bennett-Computer-19030...
 - 1 Racer
 - 2 1b1ce46edadab95d64...
- Racer.dmg.dd
 - 3 racer
 - 4 racer (Carved Files)
- carvertest.dmg
 - 5 carvertest
 - 7 carvertest (Carved F...
- 3018772

ACTIVITY

Export Status Evidence Status

CONTENT SEARCHES Add

INDEX SEARCHES Add

TAGS Add

INVESTIGATIVE NOTES Add

Field	Value
BBTID:	2351892
FileSystemID:	1
Name:	3018772
Path:	3018772
Size:	42491
SizeOnDisk:	42491
Extension:	
ContentExte...	
Date Created:	2019-07-14 00:13:10 (UT
Date Modifi...	2019-07-14 00:13:10 (UT
Date Acces...	2019-07-14 00:28:01 (U
FileSystem...	UTC
fsType:	File
Directory:	No
Visible:	Yes
Locked:	false
Owner ID:	0

Root

Name	Date Created	Date Modified	Date Accessed	Date Added
8 3018772	2019-07-14 00:13:10 (UTC)	2019-07-14 00:13:10 (UTC)	2019-07-14 00:28:01 (UTC)	

Hex Strings Preview Metadata Location Record

Data Interpreter Data Fork

Type	Value (Litt...
String	
UTF-8	
UTF-16	
Date/Time	
Chrome	
Cocoa/Webkit	
Cocoa Nanoseconds	
DOS	
FILETIME	
Firefox	
Java	
OLE	
OS X	
Unix	
Integer	
8 bit signed	
8 bit unsigned	
16 bit signed	
16 bit unsigned	
32 bit signed	
32 bit unsigned	
64 bit signed	

Decimal Go To Position Sector Offset: 0x0 (0) Position: 0xA (10) Little Endian

(1 of 1) - 3018772

Uncompressed page contents

There are strings here, and they are useful for strings/grep analysis, but:

- 1) integer, date, lat/long types are all VLI
- 2) These are only values, key names are in the attribute tables
- 3) Time constraints prohibit us from digging deeper but let it be known the complexity doesn't end here



macOS Volume-Level Contents

- You've already seen this before.
- Cool tidbit: there can be multiple records for a file

(Duplicate Record)

oid: 423874, parentOID: 2471310, len: 261, flags: 98, itemID: 10524814, dateUpdated: 2019-02-12 01:55:40 -0600 CST

path:

_kMDItemContentChangeDate: 2015-04-10 15:12:28 +0000 UTC

_kMDItemCreationDate: 2015-04-10 15:12:28 +0000 UTC

_kMDItemFileName: UNADJUSTEDNONRAW_largepv_218.jpg

oid: 423874, parentOID: 2471310, len: 219, flags: 66, itemID: 16683, dateUpdated: 2018-10-03 14:49:09 -0500 CDT

path:

_kMDItemContentChangeDate: 2015-04-10 15:12:28 +0000 UTC

_kMDItemCreationDate: 2015-04-10 15:12:28 +0000 UTC

_kMDItemFileName: IMG_0008.jpg

User-Level Spotlight

macOS User-Level Directory Structure

/Users/vico/Library/Caches/com.apple.helpd/

-- index.spotlightV3/

(looks like just built-in help info)

/Users/vico/Library/Metadata/CoreSpotlight/

-- index.spotlightV3/

-- .store.db

-- store.db

macOS User-Level Store Structure

- Mostly the same as the volume level store
- Indexes metadata about items for specific user
- Does not use inode – some large int
- Parent always zero
- Linkage to filesystem object unknown
- Otherwise, effectively the same as Volume-Level

macOS User-Level Contents: Safari History

kMDItemKind: Safari history item

kMDItemContentURL: <http://www.car-part.com/>

kMDItemDescription: <U+200E>car-part.com

kMDItemLastUsedDate: 2019-02-11 15:01:52 +0000 UTC

kMDItemTitle: Car-Part.com--Used Auto Parts Market

kMDItemUseCount: 1

kMDItemUsedDates: 2019-02-11 05:00:00 +0000 UTC

pageVisitCount: 7

kMDItemExternalID: 3F10D554E5D9DCDA80EEF096CA3238AD2ECFE2FFC...

macOS User-Level Contents: Safari Bookmark

kMDItemContentURL: <https://vindecoder.eu/bmw>

kMDItemKind: Safari bookmark

kMDItemTitle: Get Bmw VIN History Report | Bmw Vindecoder

macOS User-Level Contents: Notes

DataSourceIdentifier: Modern

ManagedObjectID: x-coredata://7040EBDF-4ADC-4A3C-86B8-6CF589CEA187/ICNote/p10

_ICItemDisplayName: I am a note to see if this text is populates in the Spotlight user...

_kMDItemBundleID: com.apple.Notes

_kMDItemDomainIdentifier: LocalAccount

_kMDItemExpirationDate: 2247-05-05 01:16:18.871345152 +0000 UTC

_kMDItemExternalID: 939E8B67-7A33-495A-90B9-9E195F60B35E

kMDItemContentCreationDate: 2019-07-08 16:21:34 +0000 UTC

kMDItemContentModificationDate: 2019-07-08 16:22:11 +0000 UTC

kMDItemContentType: com.apple.notes.spotlightrecord

kMDItemDescription: -level store.

kMDItemDisplayName: I am a note to see if this text is populates in the Spotlight user...

kMDItemKind: Spotlight Notes Record



macOS User-Level Contents: Maps

Large blob of
base64 encoded
content

_kMDItemExternalID: KnhDZlQJEgvR/FvEz1tB9A==

_kMDItemUserActivityRequiredString:

v1.0/com.apple.Maps/t='Maps'&u={'bs'=\$NwAAAEJaaDExQVk...hOo\$}

_kMDItemUserActivityType: com.apple.Maps

kMDItemApplicationName: Maps

kMDItemContentCreationDate: 2019-07-08 16:46:49 +0000 UTC

kMDItemContentCreationDate_Ranking: 2019-07-08 00:00:00 +0000 UTC

kMDItemLastUsedDate: 2019-07-08 16:46:49 +0000 UTC

kMDItemUseCount: 1

kMDItemUsedDates: 2019-07-08 05:00:00 +0000 UTC

macOS User-Level Contents: News

_kMDItemBundleID: com.apple.news

_kMDItemDomainIdentifier: com.apple.news.article.history

_kMDItemExternalID: AvqV8m7xAQ-eH1meDYbv6sQ

kMDItemContentCreationDate: 2019-07-05 15:27:01 +0000 UTC

kMDItemDescription: The popular wallet service Electrum is soon to add official support for bitcoin's lightning network, its founder has told CoinDesk.

kMDItemKind: text

kMDItemNamedLocation: CoinDesk

kMDItemTitle: Electrum Wallet Is Adding Support for Bitcoin's Lightning Network

macOS User-Level Contents: Evernote

kMDItemKind: text

_kMDItemBundleID: com.evernote.Evernote

_kMDItemExternalID: 47194390 ...

... x-coredata://5B55776F-696C-4560-B375-4620995A4D77/ENNote/p38

kMDItemContentCreationDate: 2018-11-20 19:38:11 +0000 UTC

kMDItemContentModificationDate: 2018-11-20 19:38:11 +0000 UTC

kMDItemTitle: [Windows 10 Notification WAL database](#)

iOS Spotlight

iOS Directory Structure

```
/private/var/mobile/Library/Spotlight/CoreSpotlight
-- NSFileProtectionComplete
-- NSFileProtectionCompleteUnlessOpen
-- NSFileProtectionCompleteUntilFirstUserAuthentication
-- index.spotlightV2
-- store.db
-- .store.db
-- dbStr-1.map.buckets
-- dbStr-1.map.data
-- dbStr-1.map.header
-- dbStr-1.map.offsets
-- Cache\
-- hierarchy of numbered directories
-- (dozens of other files)
```

iOS Store Structure

- Parts are similar to the Volume-Level store with a major exception
- Attribute tables are not in the *store.db* file
- They are stored in pieces in text files in the same dir as the store
- As with User-Level stores, no inode-parent relationships
- Linkage to filesystem objects unknown

iOS: SMS

_kMDItemBundleID: com.apple.MobileSMS

_kMDItemDomainIdentifier: SMS;-;+14083917778

_kMDItemSnippet: Hey you with your old man

kMDItemAccountHandles: +14083340589

kMDItemAccountIdentifier: 04BB96C4-4F17-4045-B9D6-33C623CF6704

kMDItemAuthorAddresses: +14083340589

kMDItemContentCreationDate: 2017-08-29 10:10:33 +0000 UTC

kMDItemInstantMessageAddresses (2)

+14083917778

+14083340589

kMDItemKind: message

kMDItemRecipientAddresses: +14083917778

kMDItemRecipientContactIdentifiers: 8285E550-18E9-4100-8D79-7731AF9C5A17

kMDItemRecipients (2)

Darlene Munroe

iOS: iMessage

_kMDItemBundleID: com.apple.MobileSMS
_kMDItemDomainIdentifier: iMessage;-;donniea01@aol.com
_kMDItemExternalID: C42F618F-ED59-45D5-8C6E-B311572E5735
_kMDItemSnippet: [Was wondering if you got pinched?](#)
kMDItemAccountHandles: +14083340589
kMDItemAccountIdentifier: 9000C790-4D13-410E-B878-52830849F7FF
kMDItemAuthorAddresses: +14083340589
kMDItemContentCreationDate: 2014-03-10 20:06:25 +0000 UTC
kMDItemContentType: public.message
kMDItemInstantMessageAddresses
 donniea01@aol.com
 +14083340589
kMDItemKind: message
kMDItemRecipientAddresses: donniea01@aol.com

iOS: Maps

`_kMDItemExpirationDate: 2018-04-23 16:22:20 +0000 UTC`
`_kMDItemUserActivityRequiredString: v1.0/com.apple.Maps/t='301%20Roncesvalles%20Ave%20in%20Toronto'&...`
`kMDItemCity: Toronto`
`kMDItemContentCreationDate: 2018-03-24 16:22:20 +0000 UTC`
`kMDItemContentType: com.apple.Maps`
`kMDItemCountry: Canada`
`kMDItemDisplayName: 301 Roncesvalles Ave in Toronto`
`kMDItemFullyFormattedAddress: 301 Roncesvalles Ave, Toronto ON M6R 2M6, Canada`
`kMDItemLastUsedDate: 2018-03-24 16:22:20 +0000 UTC`
`kMDItemLatitude: 43.6482234`
`kMDItemLongitude: -79.4495759`
`kMDItemNamedLocation: 301 Roncesvalles Ave`
`kMDItemPostalCode: M6R 2M6`
`kMDItemStateOrProvince: ON`
`kMDItemSubThoroughfare: 301`
`kMDItemThoroughfare: Roncesvalles Ave`
`kMDItemUseCount: 3`
`kMDItemUsedDates: 2018-03-24 04:00:00 +0000 UTC`

iOS: Reminders

_kMDItemBundleID: com.apple.reminders
_kMDItemDomainIdentifier: com.apple.reminders.C0527568-B51C-4CB7-908D-...-3B6A-473D-B0DB-8A87E58F0FF3
_kMDItemExpirationDate: 2247-05-05 01:16:18.871345152 +0000 UTC
_kMDItemProviderDataTypes (3)
 com.apple.reminders.ics
 public.utf8-plain-text
 public.utf16-plain-text
_kMDItemStorageSize: 212
kMDItemAccountHandles: jbennett_mac@me.com
kMDItemAccountIdentifier: C0527568-B51C-4CB7-908D-F97CBFAD9BFD
kMDItemCompletionDate: 2016-07-26 17:22:13 +0000 UTC
kMDItemContentType: public.to-do-item
kMDItemContentTypeTree: public.to-do-item
kMDItemDueDate: 2016-07-22 21:00:00 +0000 UTC
kMDItemTitle: [Ask Linda about the Belleville](#)

iOS: Calendar Events

_kMDItemBundleID: com.apple.mobilecal
_kMDItemDomainIdentifier: com.apple.mobilecal.9A07B074-...C7.877CEFC9-C058-4C32-A8C2-BA243AA41101
_kMDItemExpirationDate: 2247-05-05 01:16:18.871345152 +0000 UTC
kMDItemAccountHandles: a.donnie01@icloud.com
kMDItemAccountIdentifier: 9A07B074-C355-432F-9BFE-FBE4CA007C8E
kMDItemContentType: public.calendar-event
kMDItemContentTypeTree: public.calendar-event
kMDItemEndDate: 2020-02-13 03:00:00 +0000 UTC
kMDItemIdentifier: E409AF1B-567A-43C0-B3D8-FE62C242F3B3
kMDItemIsAllDay: false
kMDItemKind: calendar event
kMDItemStartDate: 2020-02-13 02:00:00 +0000 UTC
kMDItemTitle: [Check in with Taz](#)

iOS: Contact

_kMDItemBundleID: com.apple.MobileAddressBook
_kMDItemDomainIdentifier: contact
_kMDItemExternalID: E610F58F-2A1D-4FE8-BFFE-DC77B4A8AF0F
_kMDItemProviderDataTypes (4)
 CNContactIdentifiersPboardType
 CNLinkedContactsIdentifiersPboardType
 public.vcard
 com.apple.contacts.vCardDisplayNames
kMDItemAccountHandles: 1 (202) 465-2197
kMDItemAlternateNames (2)
 Eddie
 V
kMDItemContentCreationDate: 2010-01-24 02:47:43 +0000 UTC
kMDItemContentType: public.contact
kMDItemDisplayName: Eddie V
kMDItemKind: contact information
kMDItemPhoneNumbers: 1 (202) 465-2197

iOS: Email Mailbox

_kMDItemBundleID: com.apple.mobilemail

_kMDItemExpirationDate: 2018-09-05 20:20:50 +0000 UTC

_kMDItemUserActivityRequiredString:

v1.0/com.apple.mail.mailbox/t='Inbox'&u={'focusedMessageID'='message:%253C3b4825136de99b67ad61f368d10595a8@2d4a6334d2f2bb73c1c106ccaf5b5e83c5a47abe274260dad6a33286199d452%253E','mailActivityType'='com.apple.mail.mailbox','remoteMailboxURL'='x-apple-mail-mailboxurl:%2F%2Fa%252Edonnie01%2540gmail%252Ecom@imap.gmail.com%2FINBOX'}

_kMDItemUserActivityType: com.apple.mail.mailbox

kMDItemContentCreationDate: 2018-08-06 20:20:50 +0000 UTC

kMDItemContentType: public.item

kMDItemDisplayName: Inbox

kMDItemLastUsedDate: 2018-08-06 20:20:50 +0000 UTC

kMDItemTitle: Inbox

kMDItemUseCount: 1

kMDItemUsedDates: 2018-08-06 14:00:00 +0000 UTC

iOS: Twitter

_kMDItemBundleID: com.atebits.Tweetie2
_kMDItemDomainIdentifier: TwitterTweet
_kMDItemExpirationDate: 2018-03-31 16:04:52 +0000 UTC
_kMDItemExternalID: <https://twitter.com/cultofmac/status/976980416182833152>
_kMDItemGroupId: 15
_kMDItemStorageSize: 222
kMDItemContentType: public.utf8-plain-text
kMDItemDescription: ICYMI: Apple vows to zip Siri's loose lips in future update <https://t.co/pliTcrXA86>
<https://t.co/mEpiAvQu5k>
kMDItemKeywords (3)
Tweets
Cult of Mac <U+2066><U+202A>@cultofmac<U+202C><U+2069>
ICYMI: Apple vows to zip Siri's loose lips in future update <https://t.co/pliTcrXA86> <https://t.co/mEpiAvQu5k>
kMDItemKind: text
kMDItemTitle: Cult of Mac <U+2066><U+202A>@cultofmac<U+202C><U+2069>

How can we get the stuff

CMDLine Tools

- **mdutil**
 - Manages spotlight metadata stores
- **mdimport**
 - Imports a file's metadata into Spotlight
- **mdfind**
 - Finds files matching a query
- **mdls**
 - Lists the metadata attributes for a file

But iOS?


```
mdfind -0 "kMDItemKind == *" | xargs -0 mdls -name kMDItemPath -name kMDItemKind
```

```
kMDItemKind = "Document"
```

```
kMDItemPath = "/Users/vico/Library/.../-BA76-02A5390B5690.olk15ExchangeSyncMap"
```

```
kMDItemKind = "Document"
```

```
kMDItemPath = "/Users/vico/Library/Group Containers/.../-228C5465DCB8.olk15Folder"
```

```
kMDItemKind = "XML Document"
```

```
kMDItemPath = "/Users/vico/Library/Containers/.../microsoft word_Rules.xml"
```

```
kMDItemKind = "ICS file"
```

```
kMDItemPath = "/Users/vico/Library/.../521d5820-2bac-3dc0-9dc6-0e194c55cd01.ics"
```

spotlight_parser

https://github.com/ydkhatri/spotlight_parser

“This script will process individual Spotlight database files. These files are found under the volume at location /.Spotlight-V100/Store-V2/<UUID> where <UUID> represents a store id. In that folder you should find files named store and .store which are the Spotlight databases. Provide these as input to this script.”

```
spotlight_parser.py [-p OUTPUT_PREFIX] <path_to_database>  
<output_folder>
```

Example: `python spotlight_parser.py c:\spot\store c:\output`

Introducing: Illuminate

- Free cmdline tools for parsing Spotlight thingies
- Parses
 - Full /.Spotlight-V100, with extracted text cache
 - Volume-level store.db
 - User-level store.db
 - iOS NSProtect... directory
- Carves on raw blobs for store files
- Windows and macOS
- No external dependencies
- Beta! (designed as a research tool)

Illuminate Usage Overview

./illuminate -h

Usage of ./illuminate:

- a with -c, carve all files with a valid header regardless of if there is likely no metadata content
- c carve the supplied blob for Spotlight stores
- d string
write carved files to the specified directory (default "FLASHLIGHT")
- debug int
print debugging output to stderr, valid values 0-3; higher means more info
- i string
input to parse: [.]store.db from volume-level or user-level,
CoreSpotlight/NSFileProtection[...]/index.spotlightV2 for iOS, or
/.Spotlight-V100 for macOS installation
- p parse the paths for records; this only works when -i points to volume-level stores

Illuminate Examples

All of the text output we've seen previously snipped from flashlight

Basic usage examples:

./illuminate -i <some store.db>

./illuminate -i <some /.Spotlight-V100 directory>

**./illuminate -i <some NSFileProtectionComplete or NSFileProtectionCompleteUnlessOpen or
NSFileProtectionCompleteUntilFirstUserAuthentication directory>**

./illuminate -i <some blob> -c

./illuminate -i <some blob> -c -d <some output directory>

Illuminate Paths Example

./illuminate -p -i .../.Spotlight-V100/Store-V2/CC48CF65-F311-...-FDB1A25B5C78/.store.db

oid: 402503, parentOID: 402497, len: 267, flags: 0, itemID: 262, dateUpdated: 2018-12-11 09:12:55 - 0800 PST

path: </Users/josh/Documents/About Stacks.pdf>

_kMDItemFileName: About Stacks.pdf

_kMDItemOwnerGroupID: 20

_kMDItemOwnerUserID: 501

kMDItemContentCreationDate: 2009-06-17 22:23:51 ...

kMDItemContentModificationDate: 2009-09-10 21:05:54 ...

kMDItemContentType: com.adobe.pdf

kMDItemContentTypeTree (6)

com.adobe.pdf

...

public.content

kMDItemCreator: Preview

kMDItemDateAdded: 2015-06-11 23:27:33 +0000 UTC

kMDItemDisplayName: About Stacks.pdf

kMDItemEncodingApplications: Mac OS X 10.6 Quartz PDFContext

kMDItemKind: Portable Document Format (PDF)

kMDItemLogicalSize: 466028

kMDItemNumberOfPages: 1

kMDItemPageHeight: 792

kMDItemPageWidth: 612

kMDItemPhysicalSize: 466944

kMDItemSecurityMethod: None

kMDItemTitle: About Stacks

kMDItemVersion: 1.4

Illuminate Installation Example

`./illuminate -i .../.Spotlight-V100 -p`

Parses the VolumeConfiguration.plist

Parses all [.]store.db files under the Store-V2 directory

Parses the Cache directories, and attaches the cache text to the records in the output (capped at 256 bytes – some cache files can be > 1MB)

And parses file paths since we specified "-p"

```
...
"ConfigurationCreationDate": "2015-06-11T22:55:11Z",
"ConfigurationCreationVersion": "Version 10.10 (Build 14A389)",
"ConfigurationModificationDate": "2019-02-25T14:17:23Z",
"ConfigurationModificationVersion": "Version 10.14.3 (Build 18D109)",
"ConfigurationVolumeUUID": "E77D8F66-98C2-3957-9F8A-
C5483A4A565E",
```

```
"Exclusions": [
  "/Users/josh/Dropbox",
```

```
...
],
```

```
...
```

VolumeConfiguration.plist contents

```
...
"Stores": {
  "CC48CF65-F311-448D-875B-FDB1A25B5C78": {
    "CreationDate": "2015-06-11T22:55:11Z",
    "CreationVersion": "Version 10.10 (Build 14A389)",
    "IndexVersion": 95,
    "PartialPath": "/",
    "PolicyDate": "2015-06-11T22:55:11Z",
    "PolicyLevel": "kMDConfigSearchLevelReadWrite",
    "PolicyProcess": "STORE_ADD",
    "PolicyVersion": "Version 10.10 (Build 14A389)"
  }
}
```

```
...
```


oid: 1217383, parentOID: 1217382, len: 208, flags: 0, itemID: 324184, dateUpdated: 2012-03-04 11:23:20 -0800 PST
path: racer/Users/josh/Library/Calendars/Attachments/BE0D91FF-304E-...-E6150944A412/tdct-merchantservices-fraud.pdf
kMDItemContentCreationDate: 2012-02-03 01:27:07 +0000 UTC
kMDItemContentModificationDate: 2012-02-03 01:27:07 +0000 UTC
kMDItemCreator: Adobe InDesign CS4 (6.0.4)
kMDItemDateAdded: 2012-02-05 16:52:44 +0000 UTC
kMDItemDisplayName: tdct-merchantservices-fraud.pdf
kMDItemEncodingApplications: Adobe PDF Library 9.0
kMDItemKind: Portable Document Format (PDF)
kMDItemLogicalSize: 442617
kMDItemNumberOfPages: 10
kMDItemPageHeight: 603
kMDItemPageWidth: 540
kMDItemPhysicalSize: 446464
kMDItemSecurityMethod: None
kMDItemVersion: 1.5

CACHE FILE (21478 bytes) at .../Store-V2/E817A452-6A1D-4567-B631-C4E6B774FE33/Cache/0000/0000/0012/1217383.txt
DATA : 581614(0810) Please immediately report any suspicious activity involving credit card or debit card use to TD Merchant Services at 1-800-363-1163 For more information, visit www.tdmerchantservices.com Merchant Services How to help protect your business X



Illuminate Carving

`./illuminate -c -i vicos_infected_windows_box_20140409.dd`

Carved 5 files:

Offset: 54138025472 length: 118784

Offset: 73720152064 length: 135168

Offset: 137784807424 length: 6361088

Offset: 142381200896 length: 135168

Offset: 155678443008 length: 741376

Illuminate Carving Aggressive Mode

```
./illuminate -c -i infected_windows.dd -d carved_files -a
```

Carved 104 files:

Offset: 1382490112 length: 69632

Offset: 54138025472 length: 118784

Offset: 73720152064 length: 135168

Offset: 74080333824 length: 53248

Offset: 179842232320 length: 4096

Offset: 227770216448 length: 4096

(many more 4k entries ...)



BlackBag[®]
TECHNOLOGIES

Questions
?

Dr. Vico Marziale
vico@blackbagtech.com
@vicomarziale

Go check out illuminate:
<https://offers.blackbagtech.com/spotlight>