

OS X SPOTLIGHT QUERIES

SARAH EDWARDS | @iamevltwin | oompa@csh.rit.edu

SPOTLIGHT ESSENTIALS

- **Root of Each Volume: HFS+, ExFAT, FATx, etc**
 - `/.Spotlight-V100/`
- **Index Metadata**
 - Various File Types (Docs, Apps, Media, Email, Calendar, Chat, etc)
 - Various Data Types (File System, App Specific, EXIF, OS X Specific)
- **OS X Tools**
 - `mdimport -A`, `mdimport -X`
 - Metadata types & structures
 - `mdfind`
 - Find a particular data type
 - `mdls`
 - List the metadata for a particular file

TOOL:

mdimport -A

mdimport -X

'kMDItemAuthors'	'Authors'	'Authors of the item'
'kMDItemBitsPerSample'	'Bits per sample'	'Number of bits per sample'
'kMDItemCFBundleIdentifier'	'(null)'	'(null)'
'kMDItemCity'	'City'	'City of the item'
'kMDItemCodecs'	'Codecs'	'Codecs used to encode the item'
'kMDItemColorSpace'	'Color space'	'Color space of the item'
'kMDItemComment'	'Comment'	'Comments about the item'
'kMDItemComposer'	'Composer'	'Composer of the item'
'kMDItemContactKeywords'	'Contact keywords'	'Contact keywords of the item'
'kMDItemContentCreationDate'	'Content created'	'Date when content was created'
'kMDItemContentModificationDate'	'Content modified'	'Date when content was modified'
'kMDItemContentType'	'(null)'	'(null)'
'kMDItemContentTypeTree'	'(null)'	'(null)'
'kMDItemContributors'	'Contributors'	'People or organizations that contributed to the item'
'kMDItemCopyright'	'Copyright'	'Copyright information for the item'
'kMDItemCountry'	'Country'	'Country of origin for the item'
'kMDItemCoverage'	'Coverage'	'Extent of coverage for the item'
'kMDItemCreator'	'Content Creator'	'Author of the content'
'kMDItemDateAdded'	'Date added'	'Date when item was added to the library'
'kMDItemDeliveryType'	'Delivery type'	'Method used to deliver the item'
'kMDItemDescription'	'Description'	'Description of the item'
'kMDItemDestinationRecipients'	'(null)'	'(null)'
'kMDItemDirector'	'Director'	'Director of the item'
'kMDItemDisplayName'	'Display name'	'Localized display name of the item'

```
"public.movie" = {
    allattrs = (
        kMDItemAcquisitionMake,
        kMDItemAcquisitionModel,
        kMDItemAudioBitRate,
        kMDItemCodecs,
        kMDItemColorSpace,
        kMDItemDeliveryType,
        kMDItemLayerNames,
        kMDItemMediaTypes,
        kMDItemPixelHeight,
        kMDItemPixelWidth,
        kMDItemStreamable,
        kMDItemTotalBitRate,
        kMDItemVideoBitRate,
        kMDItemProfileName
    );
    displayattrs = (
        kMDItemPixelHeight,
        kMDItemPixelWidth,
        kMDItemCodecs,
        kMDItemProfileName
    );
    name = "public.movie";
    previewattrs = (
        kMDItemPixelHeight,
        kMDItemPixelWidth,
        kMDItemDurationSeconds,
        kMDItemLastUsedDate
    );
    readonlyattrs = (
        kMDItemPixelHeight,
        kMDItemPixelWidth,
        kMDItemDurationSeconds
    );
    relatedattrs = (
        kMDItemCopyright,
        kMDItemAuthors,
        kMDItemTitle
    );
};
```

TOOL: mdls

```
word:Downloads ompa$ mdls IMG_2292.JPG
_kTimeMachineIsCreationMarker      = 1
_kTimeMachineNewestSnapshot        = 4001-01-01 00:00:00 +0000
_kTimeMachineOldestSnapshot        = 2015-09-17 15:42:57 +0000
kMDItemAcquisitionMake             = "Apple"
kMDItemAcquisitionModel            = "iPhone 6"
kMDItemAperture                    = 2.275007124536905
kMDItemBitsPerSample                = 32
kMDItemColorSpace                  = "RGB"
kMDItemContentCreationDate          = 2015-09-17 00:38:44 +0000
kMDItemContentModificationDate      = 2015-09-17 00:38:44 +0000
kMDItemContentType                 = "public.jpeg"
kMDItemContentTypeTree              = (
    "public.jpeg",
    "public.image",
    "public.data",
    "public.item",
    "public.content"
)
kMDItemCreator                     = "8.4"
kMDItemDateAdded                   = 2015-09-17 15:50:07 +0000
kMDItemDisplayName                  = "IMG_2292.JPG"
kMDItemEXIFVersion                  = "2.2.1"
kMDItemExposureMode                 = 0
kMDItemExposureProgram              = 2
kMDItemExposureTimeSeconds          = 0.03333333333333333
kMDItemFlashOnOff                   = 0
kMDItemFNumber                      = 2.2
kMDItemFocalLength                  = 4.15
kMDItemFSContentChangeDate          = 2015-09-17 00:38:44 +0000
kMDItemFSCreationDate               = 2015-09-17 00:38:44 +0000
kMDItemFSCreatorCode                = ""
kMDItemFSFinderFlags                = 0
kMDItemFSHasCustomIcon              = (null)
kMDItemFSInvisible                  = 0
kMDItemFSIsExtensionHidden          = 0
```

TOOL:

mdfind

- `mdfind <string>` = String Search
- `-onlyin` – Search only in a particular directory/volume
- `<datatype> == "*" – Search for items containing a specific metadata type`

```
word:/ oompa$ mdfind forensic
/Users/oompa/Library/Mail/V2/IMAP-oompa@mail.csh.rit.edu/Sent Messages.mbox/267B3751-EF3A-49D8-8B3B-07F98C077049/Data/
5/7/1/Messages/175844.emlx
/Users/oompa/Library/Mail/V2/IMAP-oompa@mail.csh.rit.edu/INBOX.mbox/267B3751-EF3A-49D8-8B3B-07F98C077049/Data/5/7/1/Me
ssages/175621.emlx
```

```
word:/ oompa$ mdfind kMDItemPixelHeight == '*' -onlyin ~/Downloads/
/Users/oompa/Downloads/IMG_2292.JPG
/Users/oompa/Downloads/IMG_2290.PNG
/Users/oompa/Downloads/IMG_2294.JPG
/Users/oompa/Downloads/IMG_2293.JPG
```


PROCESS:

Mount Image

Acquire a Forensic Image of an OS X System (E01, DD, DMG)



Mount Image (ewfmount/
xmount/etc) - /Volumes/
<MountedImage>



Query Using Host OS X System
Utilities (mdfind/mdls)

QUERY: GPS LOCATIONAL DATA

```
mdfind -0 -onlyin / "kMDItemLatitude == *" | xargs -0  
mdls -name kMDItemDisplayName -name kMDItemPath -name  
kMDItemLatitude -name kMDItemLongitude -name  
kMDItemGPSDateStamp
```

```
kMDItemDisplayName = "IMG_0200.JPG"  
kMDItemGPSDateStamp = "2014:07:21"  
kMDItemLatitude = 55.68493666666667  
kMDItemLongitude = 13.0907805  
kMDItemPath = "/Users/oempa/Library/Containers/com.apple.cloudphotosd/Data/Library/Application Support/com.apple.cloudphotosd/services/com.apple.photo.icloud.sharedstreams/assets/13836496-E555-4241-8F83-F99700ADA7A9/2FD53558-8BDF-487A-9D54-2AE827FDCDF5/IMG_0200.JPG"  
kMDItemDisplayName = "IMG_0214.JPG"  
kMDItemGPSDateStamp = "2014:07:21"  
kMDItemLatitude = 59.33048833333334  
kMDItemLongitude = 18.05945283333334  
kMDItemPath = "/Users/oempa/Library/Containers/com.apple.cloudphotosd/Data/Library/Application Support/com.apple.cloudphotosd/services/com.apple.photo.icloud.sharedstreams/assets/13836496-E555-4241-8F83-F99700ADA7A9/78DB70E1-7E2D-4A4E-868C-CF3E0C18D001/IMG_0214.JPG"
```

QUERY: MEDIA

```
mdfind -0 "kMDItemContentTypeTree == *audiovisual*" |  
xargs -0 mdls -name kMDItemPath -name  
kMDItemPurchaseDate -name kMDItemTitle -name  
kMDItemRecordingYear -name kMDItemAuthors -name  
kMDItemAlbum -name kMDItemCopyright -name  
kMDItemDurationSeconds -name kMDItemContentType
```

```
kMDItemAlbum      = "Details"  
kMDItemAuthors    = (  
    "Frou Frou"  
)  
kMDItemContentType = "com.apple.protected-mpeg-4-audio"  
kMDItemCopyright  = "© 2002 Universal Island Records Ltd. A Universal Music Company."  
kMDItemDurationSeconds = 334.57333333333333  
kMDItemPath        = "/Users/oomba/Music/iTunes/iTunes Media/Music/Frou Frou/Details/07 Shh.m4p"  
kMDItemPurchaseDate = 2014-10-04 21:32:33 +0000  
kMDItemRecordingYear = 2002  
kMDItemTitle       = "Shh"
```

```
kMDItemAlbum      = (null)  
kMDItemAuthors    = (null)  
kMDItemContentType = "com.apple.quicktime-movie"  
kMDItemCopyright  = (null)  
kMDItemDurationSeconds = (null)  
kMDItemPath        = "/Users/oomba/Pictures/Photos Library.photoslibrary/Masters/2015/06/20/20150620-012628/IMG_2048.MOV"  
kMDItemPurchaseDate = (null)  
kMDItemRecordingYear = (null)  
kMDItemTitle       = "IMG_2048.MOV"
```


QUERY: ATTACHMENTS

```
mdfind -0 "kMDItemOriginSenderDisplayName == *" | xargs  
-0 mdls -name kMDItemPath -name  
kMDItemOriginSenderDisplayName -name  
kMDItemOriginSenderHandle -name kMDItemWhereFroms -name  
kMDItemUsedDates -name kMDItemOriginApplicationIdentifier  
-name kMDItemUseCount -name kMDItemCreator
```

```
kMDItemCreator = "8.4"  
kMDItemOriginApplicationIdentifier = "com.apple.mobileslideshow"  
kMDItemOriginSenderDisplayName = "iPhone"  
kMDItemOriginSenderHandle = "oompa@csh.rit.edu"  
kMDItemPath = "/Users/oompa/Downloads/IMG_2292.JPG"  
kMDItemUseCount = 6  
kMDItemUsedDates = (  
    "2015-09-17 04:00:00 +0000",  
    "2015-09-18 04:00:00 +0000",  
    "2015-10-08 04:00:00 +0000"  
)  
kMDItemWhereFroms = (  
    iPhone,  
    miPhone6  
)
```

```
kMDItemCreator = "Microsoft® Word 2010"  
kMDItemOriginApplicationIdentifier = "com.apple.mail"  
kMDItemOriginSenderDisplayName = "Jennifer Santiago"  
kMDItemOriginSenderHandle = "Jennifer Santiago <jsantiago@sans.org>"  
kMDItemPath = "/Users/oompa/Library/Containers/com.apple.mail/Data/Library/Mail Downloads/054CF  
850-8809-4B9F-B2B6-5A416F0EA499/Agenda Prague 6-18-15.pdf"  
kMDItemUseCount = (null)  
kMDItemUsedDates = (null)  
kMDItemWhereFroms = (  
    "Jennifer Santiago <jsantiago@sans.org>",  
    "SANS DFIR Europe Summit - speaker confirmation details",  
    "message:%3Cf9caf18f.000026f0.00000013@BPVQF12%3E"  
)
```

QUERY: PHOTOS

```
mdfind -0 "kMDItemAcquisitionMake == *" | xargs -0  
mdls -name kMDItemPath -name kMDItemAcquisitionMake -  
name kMDItemAcquisitionModel -name kMDItemCreator -  
name kMDItemFSCreationDate
```

```
kMDItemAcquisitionMake = "Apple"  
kMDItemAcquisitionModel = "iPod touch"  
kMDItemCreator = "6.1.6"  
kMDItemFSCreationDate = 2014-10-26 18:56:18 +0000  
kMDItemPath = "/Users/oomba/Library/Mail/V2/IMAP-oomba@mail.csh.rit.edu/INBOX.mbox/267B3751-EF3A-49D8-8B3B-07F98C077049/Data/3/Attachments/3674/2/photo.JPG"  
kMDItemAcquisitionMake = "HTC"  
kMDItemAcquisitionModel = "HTC6500LVW"  
kMDItemCreator = (null)  
kMDItemFSCreationDate = 2014-10-26 18:56:18 +0000  
kMDItemPath = "/Users/oomba/Library/Mail/V2/IMAP-oomba@mail.csh.rit.edu/INBOX.mbox/267B3751-EF3A-49D8-8B3B-07F98C077049/Data/3/Attachments/3764/2/IMAG0079.jpg"  
kMDItemAcquisitionMake = "Apple"  
kMDItemAcquisitionModel = "iPhone 5s"  
kMDItemCreator = "7.1"  
kMDItemFSCreationDate = 2014-10-26 18:56:18 +0000  
kMDItemPath = "/Users/oomba/Library/Mail/V2/IMAP-oomba@mail.csh.rit.edu/INBOX.mbox/267B3751-EF3A-49D8-8B3B-07F98C077049/Data/3/Attachments/3639/2/IMG_0010.jpeg"
```

QUERY: WHERE FROMS DATA

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

```
kMDItemPath      = "/Users/oomba/Downloads/TaiGjailbreak_V110.dmg"  
kMDItemWhereFroms = (  
    "http://res.taig.com/installer/mac/TaiGjailbreak_V110.dmg",  
    "http://www.taig.com/en/"  
)
```

```
kMDItemPath      = "/Users/oomba/Library/Mail/V2/IMAP-oomba@mail.csh.rit.edu/INBOX.mbox/267B3751-EF3A-49D8-8B3B-07F98  
C077049/Data/2/7/1/Attachments/172494/2/emailreceipt_20150918R1615054237.pdf"  
kMDItemWhereFroms = (  
    "theforumshops@apple.com",  
    "Your receipt from Apple Store, The Forum Shops",  
    "message:%3C586545993.228121442625143411.JavaMail.nexusp@nwk-nexusp-lapp38.corp.apple.com%3E"  
)
```

```
kMDItemPath      = "/Users/oomba/Downloads/IMG_2294.JPG"  
kMDItemWhereFroms = (  
    iPhone,  
    miPhone6  
)
```

```
kMDItemPath      = "/Users/oomba/IMG_1589.JPG"  
kMDItemWhereFroms = (  
    "+17039736397",  
    "Received via Messages file transfer"  
)
```

QUERY: APPLICATION USAGE

```
mdfind -0 -onlyin /Applications/ "kMDItemContentType ==  
com.apple.application-bundle" | xargs -0 mdls -name kMDItemPath -  
name kMDItemLastUsedDate -name kMDItemUseCount -name  
kMDItemUsedDates
```

```
kMDItemLastUsedDate = 2015-10-08 19:41:49 +0000  
kMDItemPath         = "/Applications/Utilities/Console.app"  
kMDItemUseCount      = 13  
kMDItemUsedDates     = (  
    "2015-08-17 04:00:00 +0000",  
    "2015-08-26 04:00:00 +0000",  
    "2015-08-30 04:00:00 +0000",  
    "2015-09-16 04:00:00 +0000",  
    "2015-09-17 04:00:00 +0000",  
    "2015-10-06 04:00:00 +0000",  
    "2015-10-07 04:00:00 +0000",  
    "2015-10-08 04:00:00 +0000"  
)  
kMDItemLastUsedDate = 2015-10-08 17:59:09 +0000  
kMDItemPath         = "/Applications/LittleSnapper.app"  
kMDItemUseCount      = 7  
kMDItemUsedDates     = (  
    "2015-08-17 04:00:00 +0000",  
    "2015-08-29 04:00:00 +0000",  
    "2015-09-28 04:00:00 +0000",  
    "2015-10-08 04:00:00 +0000"  
)  
kMDItemLastUsedDate = 2015-10-08 17:09:51 +0000  
kMDItemPath         = "/Applications/Mail.app"  
kMDItemUseCount      = 12  
kMDItemUsedDates     = (  
    "2015-08-17 04:00:00 +0000",  
    "2015-08-20 04:00:00 +0000",  
    "2015-09-01 04:00:00 +0000",  
    "2015-09-10 04:00:00 +0000",  
    "2015-09-15 04:00:00 +0000",  
    "2015-09-16 04:00:00 +0000",  
    "2015-09-17 04:00:00 +0000",  
    "2015-09-19 04:00:00 +0000",  
    "2015-10-06 04:00:00 +0000",  
    "2015-10-07 04:00:00 +0000",  
    "2015-10-08 04:00:00 +0000"  
)
```

OFFLINE ANALYSIS: SPOTLIGHT INSPECTOR

- 504ENSICS LABS
- <http://www.504ensics.com/tools/spotlight-inspector-digital-forensics-app-for-mac-osx/>
- store.db Database File
- Search / Report / Export

