mift

A mobile image forensic toolkit

GitHub: https://github.com/controlf/mift

Version: 1.0
Last updated: 2022-07-19

Author: Mike Bangham

Control-F
DIGITAL FORENSICS

Contents

1 ABOUT MIFT

"**mift**" is a **mobile image forensics toolkit** designed to harvest media files, and associated metadata from the file system of an Android or iOS device. It presents which may not be fully decoded or exploited by commercial forensic tools. The latest release can be downloaded from: https://github.com/controlf/mift

At the time of writing, **mift** supports six forensic functions (FIGURE 1), namely:

1. iOS Photos
2. iOS Snapshots
3. Huawei Gallery Cache
4. Samsung File Cache
5. Sony Picnic Cache
6. Samsung Gallery

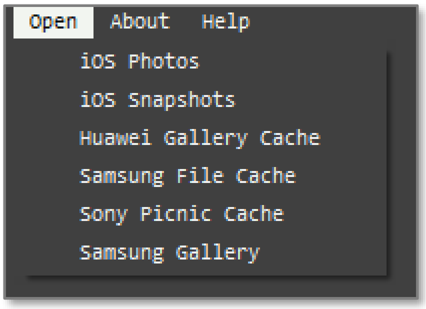
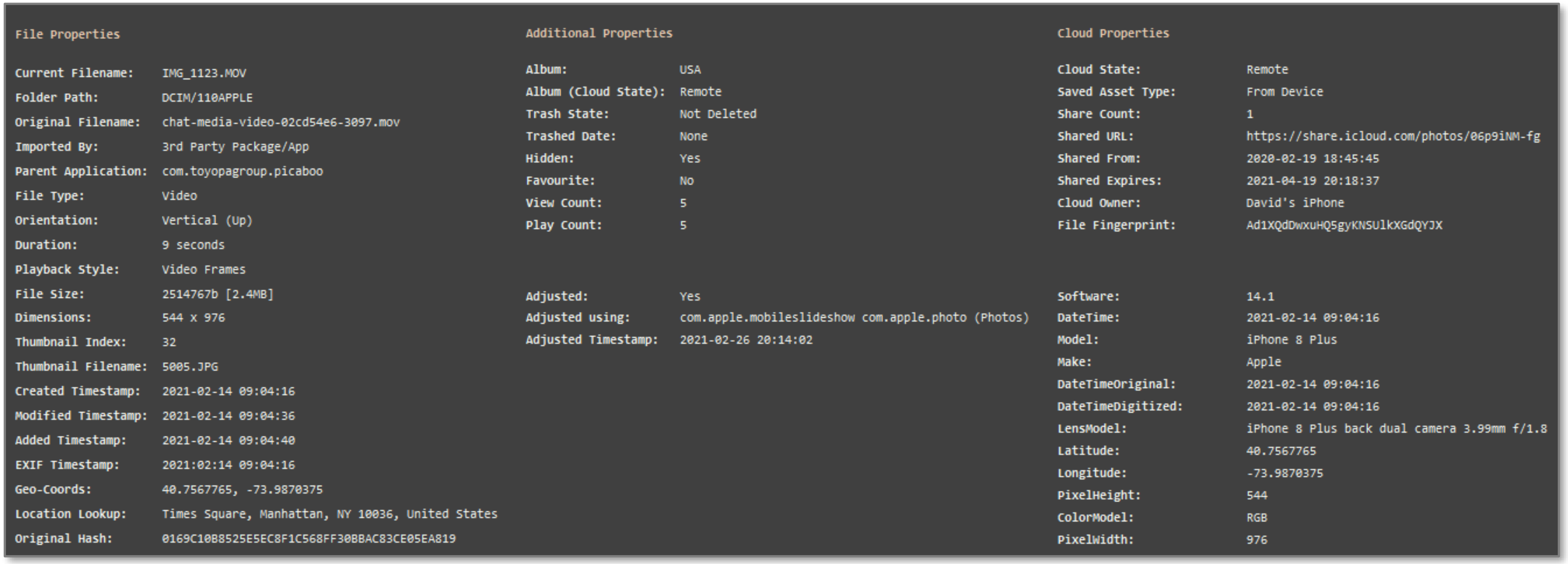


Figure 1

While media files are typically parsed and presented to an investigator via commercial forensic tools or carving techniques, the context of said media files is often lost. Associated entries within a database, or metadata embedded in BLOB data, might not be extracted and associated back to any related media files. mift is able to give context to thumbnail images and link them to original ("primary") images. It can also identify cloud ownership of media files, identify whether they been tampered with or modified, and confirm timestamps for deleted primary images.

A typical example of mift's iOS Photos report for a single media file will produce metadata as seen in FIGURE 2.



```
File Properties

Current Filename:     IMG_1123.MOV
Folder Path:          DCIM/110APPLE
Original Filename:    chat-media-video-02cd54e6-3097.mov
Imported By:          3rd Party Package/App
Parent Application:   com.toyopagroup.picaboo
File Type:            Video
Orientation:          Vertical (Up)
Duration:             9 seconds
Playback Style:       Video Frames
File Size:            2514767b [2.4MB]
Dimensions:           544 x 976
Thumbnail Index:      32
Thumbnail Filename:   5005.JPG
Created Timestamp:    2021-02-14 09:04:16
Modified Timestamp:   2021-02-14 09:04:36
Added Timestamp:      2021-02-14 09:04:40
EXIF Timestamp:       2021:02:14 09:04:16
Geo-Coords:           40.7567765, -73.9870375
Location Lookup:      Times Square, Manhattan, NY 10036, United States
Original Hash:        0169C10B8525E5EC8F1C568FF30BBAC83CE05EA819
```

```
Additional Properties

Album:                USA
Album (Cloud State):  Remote
Trash State:          Not Deleted
Trashed Date:         None
Hidden:               Yes
Favourite:            No
View Count:           5
Play Count:           5


Adjusted:             Yes
Adjusted using:       com.apple.mobileslideshow com.apple.photo (Photos)
Adjusted Timestamp:   2021-02-26 20:14:02
```

```
Cloud Properties

Cloud State:          Remote
Saved Asset Type:     From Device
Share Count:          1
Shared URL:           https://share.icloud.com/photos/06p9iNM-fg
Shared From:          2020-02-19 18:45:45
Shared Expires:       2021-04-19 20:18:37
Cloud Owner:          David's iPhone
File Fingerprint:     Ad1XQdDwxuHQ5gyKNSUlkXGdQYJX


Software:             14.1
DateTime:             2021-02-14 09:04:16
Model:                iPhone 8 Plus
Make:                 Apple
DateTimeOriginal:     2021-02-14 09:04:16
DateTimeDigitized:    2021-02-14 09:04:16
LensModel:            iPhone 8 Plus back dual camera 3.99mm f/1.8
Latitude:             40.7567765
Longitude:            -73.9870375
PixelHeight:          544
ColorModel:           RGB
PixelWidth:           976
```

Figure 2

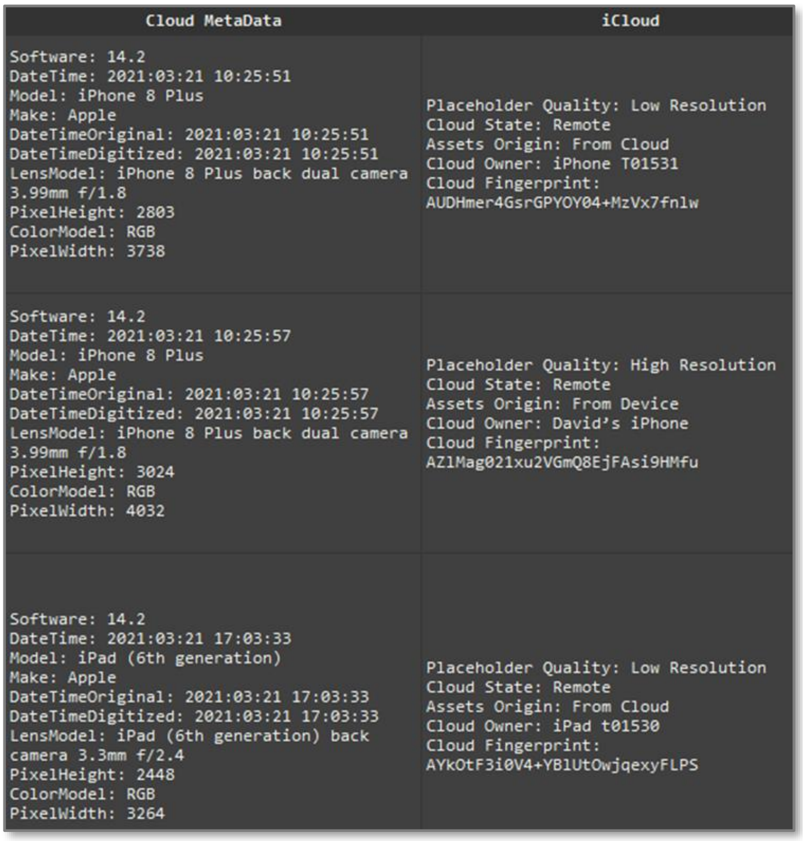
2 iOS Cloud

With iOS, multiple devices can share the same iOS cloud account and, therefore, share the same files that are backed up to the cloud. If two devices have uploaded different files to the cloud and the files have been shared across both devices, mift will report both the direction of any sharing, and cloud ownership.

2.1 Direction and Ownership

The screenshot in Figure 3 shows the iOS Cloud metadata for 3 image files extracted from an iOS device named ‘**David’s iPhone**’. Other columns are included in mift’s report table but not shown in the screenshot.

From the screenshot we can see there are 2 other devices connected to the same iCloud account as David’s iPhone, each of which have ownership of a file that is synced with the cloud (‘**iPhone T01531**’ for the first row, ‘**iPad t01530**’ for the third). The second row in the screenshot indicates that specific file has originated from the device, ‘**David’s iPhone**’. The ‘*Cloud Owner*’ field helps to affirm this. The ‘*Cloud State*’ shows the file is saved remotely on the cloud (so accessible to other cloud devices) due to the state of “Remote”. It is also worth noting that, since the file has come from this device, the file’s ‘Placeholder Quality’ is high resolution.



Cloud MetaData	iCloud
Software: 14.2 DateTime: 2021:03:21 10:25:51 Model: iPhone 8 Plus Make: Apple DateTimeOriginal: 2021:03:21 10:25:51 DateTimeDigitized: 2021:03:21 10:25:51 LensModel: iPhone 8 Plus back dual camera 3.99mm f/1.8 PixelHeight: 2803 ColorModel: RGB PixelWidth: 3738	Placeholder Quality: Low Resolution Cloud State: Remote Assets Origin: From Cloud Cloud Owner: iPhone T01531 Cloud Fingerprint: AUDHmer4GsrGPYOY04+MzVx7fnlw
Software: 14.2 DateTime: 2021:03:21 10:25:57 Model: iPhone 8 Plus Make: Apple DateTimeOriginal: 2021:03:21 10:25:57 DateTimeDigitized: 2021:03:21 10:25:57 LensModel: iPhone 8 Plus back dual camera 3.99mm f/1.8 PixelHeight: 3024 ColorModel: RGB PixelWidth: 4032	Placeholder Quality: High Resolution Cloud State: Remote Assets Origin: From Device Cloud Owner: David's iPhone Cloud Fingerprint: AZ1Mag021xu2VGmQ8EjFAsi9HMfu
Software: 14.2 DateTime: 2021:03:21 17:03:33 Model: iPad (6th generation) Make: Apple DateTimeOriginal: 2021:03:21 17:03:33 DateTimeDigitized: 2021:03:21 17:03:33 LensModel: iPad (6th generation) back camera 3.3mm f/2.4 PixelHeight: 2448 ColorModel: RGB PixelWidth: 3264	Placeholder Quality: Low Resolution Cloud State: Remote Assets Origin: From Cloud Cloud Owner: iPad t01530 Cloud Fingerprint: AYkOtF3i0V4+YB1UtOwjqexyFLPS

Figure 3

The first and third rows are files that have originated from two other devices. Since the file has been synced from the cloud, the default settings on iOS have synced a low-resolution placeholder (users can enable high resolution placeholders if they wish). These pieces of metadata all assist in building up a picture of where the files have originated from inside the cloud network.

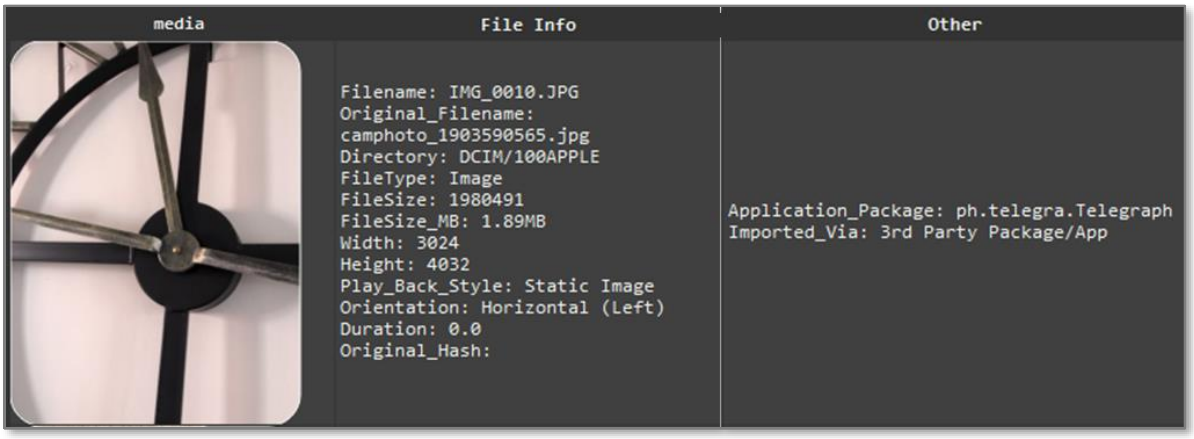
In the '*Cloud MetaData*' column we have details scraped from available Exif data, at the time of syncing. These details are retained in the cloud for each file and can provide both additional context, and assistance with attribution.

3 iOS Package Metadata

Sometimes an investigator needs to know which application or package has generated, or been involved with, a media file found on an iOS device. Using mift we can obtain useful metadata that can assist with both attributing a file to an application, and also identify whether or not it has been sent or received (i.e. its direction).

3.1 Package ownership and direction

In the screenshot in Figure 4, the photo in question (as seen in the '*media*' column) has been captured using the camera function inside the application "Telegram". The original filename is an important factor in proving this was the case. The file name of the image within `DCIM/100APPLE` (presented under "Filename") would not have given this much insight on its own, whereas the "*Original_Filename*" attribute provides far greater insight. We have some useful metadata in the "*Other"* column attributing the file to Telegram and, as expected, the file is logged as being imported to iOS Photos via a 3rd party app.



media | File Info | Other

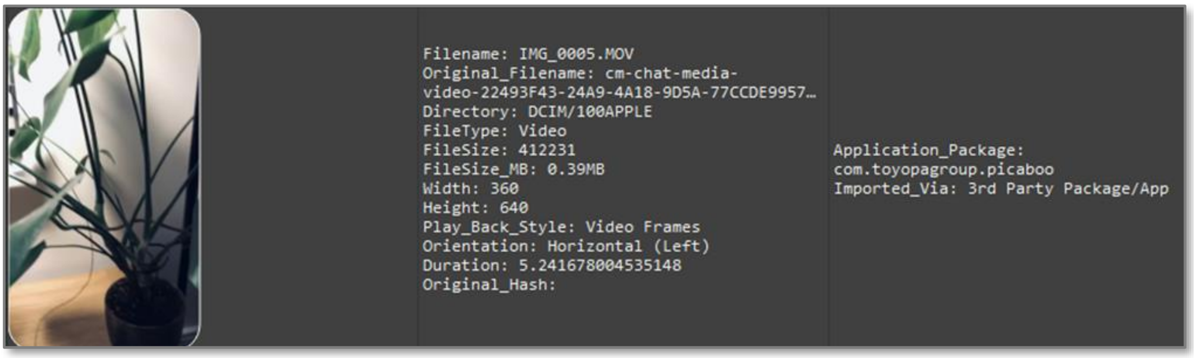
```
Filename: IMG_0010.JPG
Original_Filename:
camphoto_1903590565.jpg
Directory: DCIM/100APPLE
FileType: Image
FileSize: 1980491
FileSize_MB: 1.89MB
Width: 3024
Height: 4032
Play_Back_Style: Static Image
Orientation: Horizontal (Left)
Duration: 0.0
Original_Hash:
```

```
Application_Package: ph.telegra.Telegraph
Imported_Via: 3rd Party Package/App
```

Figure 4

A second file (Figure 5) and third file (Figure 6) below have some useful metadata relating to videos being sent and received via Snapchat, respectively. The original filename is useful here for determining the **received or sent** status of the media files. This would be the case even if the Snapchat application has been deleted, or it cannot be accessed manually using the device itself (such as for a manual examination).

In the screenshot presented in Figure 5, mift provides us with the original filename. Note the upper-case text of the GUID identifier section of the filename. From testing this shows the video has been sent from this device via Snapchat.

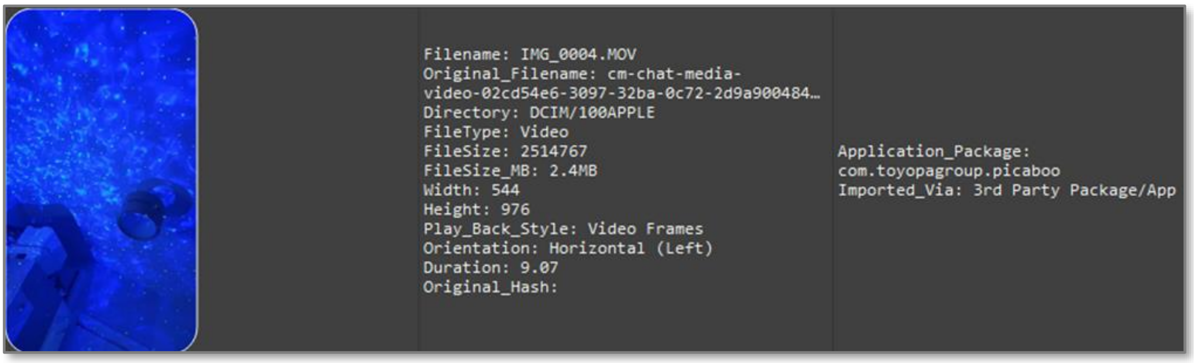


```
Filename: IMG_0005.MOV
Original_Filename: cm-chat-media-
video-22493F43-24A9-4A18-9D5A-77CCDE9957…
Directory: DCIM/100APPLE
FileType: Video
FileSize: 412231
FileSize_MB: 0.39MB
Width: 360
Height: 640
Play_Back_Style: Video Frames
Orientation: Horizontal (Left)
Duration: 5.241678004535148
Original_Hash:
```

```
Application_Package:
com.toyopagroup.picaboo
Imported_Via: 3rd Party Package/App
```

Figure 5

Note the lower case GUID identifier in the original filename presented in the screenshot in FIGURE 6. From testing, lower case GUID file names indicate that the file has been received by the device via Snapchat.



```
Filename: IMG_0004.MOV
Original_Filename: cm-chat-media-
video-02cd54e6-3097-32ba-0c72-2d9a900484…
Directory: DCIM/100APPLE
FileType: Video
FileSize: 2514767
FileSize_MB: 2.4MB
Width: 544
Height: 976
Play_Back_Style: Video Frames
Orientation: Horizontal (Left)
Duration: 9.07
Original_Hash:
```

```
Application_Package:
com.toyopagroup.picaboo
Imported_Via: 3rd Party Package/App
```

Figure 6

> ***Note:*** *You can learn more about this type of file attribution and deriving context from metadata on the Control-F Smartphone App Forensics (SAF) course.*

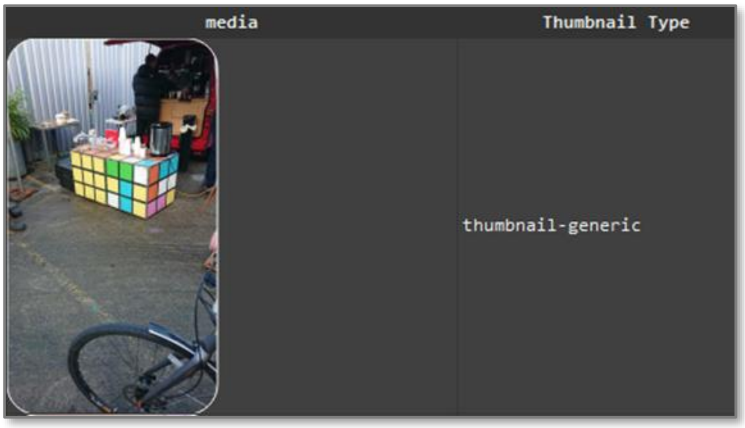
4 SONY PICNIC THUMBNAIL CACHE

Sony devices often store thumbnail copies of media files, many of which may still reside on the device even where the original image is no longer present (i.e. has been deleted). Details of the original files and the thumbnail versions are recorded in a SQLite database which has the unusual name of "**picnic**" (no file extension). This file acts as the media database for the Sony gallery app. mift is capable of providing context to these thumbnail files regardless of whether the original file is still present on the device.

4.1 THUMBNAIL METADATA

In order to improve readability of this document we have split the columns and their values for a single mift media file record (row). We have broken the record into several screenshots to provide a clear breakdown of context and meaning.

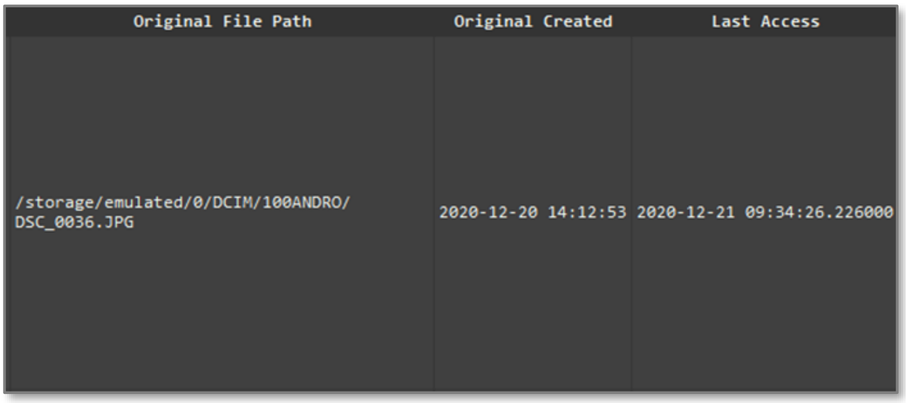
In FIGURE 7 we see a thumbnail media file record relating to a still image. The original has been deleted, yet a high-resolution thumbnail is still present within the file system.



media	Thumbnail Type
	thumbnail-generic

Figure 7

As we look at some of the other columns of recorded data, as within FIGURE 8, we can see the file path of the original image, which is still present in this database, despite the original having been deleted. We also have a created time and date of that original image, which could prove useful.

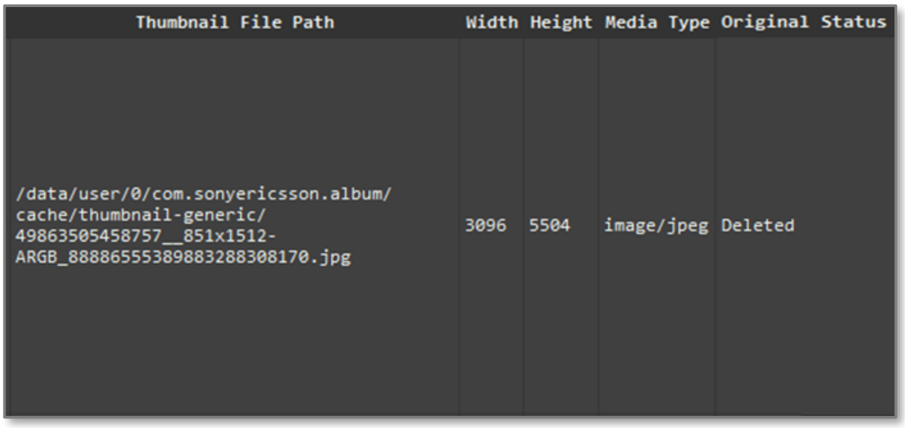


Original File Path	Original Created	Last Access
/storage/emulated/0/DCIM/100ANDRO/DSC_0036.JPG	2020-12-20 14:12:53	2020-12-21 09:34:26.226000

Figure 8

As is often the case with thumbnail images, their timestamps alone may not reflect the time at which the original image was taken. However, mift will recover and correlate records with identifiers found on the file system in order to link the original file metadata with its corresponding thumbnail image.

We can see in FIGURE 9 how we have also included the file path for the thumbnail image, along with the dimensions, media type, and status of the original image.



Thumbnail File Path	Width	Height	Media Type	Original Status
/data/user/0/com.sonyericsson.album/cache/thumbnail-generic/49863505458757__851x1512-ARGB_8888655538988328830817 0.jpg	3096	5504	image/jpeg	Deleted

Figure 9

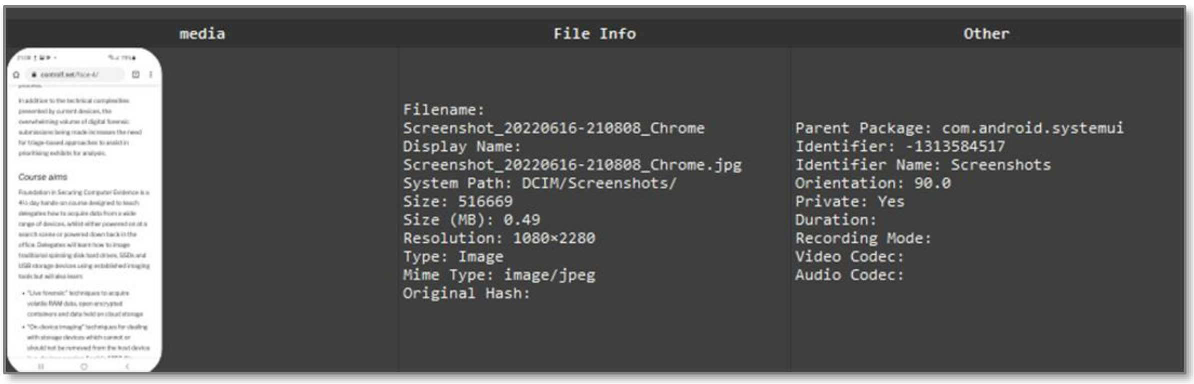
At the time of writing this report, the metadata attribution for deleted media from Sony devices was not found in a selection of commonly used commercial forensic tools.

5 SAMSUNG GALLERY

Much like Photos.sqlite on iOS, later revisions of the Samsung OS have stored increasing amounts of data relating to media generated by, or simply stored on, a given device. An example of mift's output for a file recovered from a Samsung device can be seen in the following screenshots and descriptions.

5.1 MEDIA

Here we can see an example of a media file record from mift, broken down into three separate screenshots, allowing us to look at each set of columns in stages. The media file in question relates to a screenshot taken of the Control-F website, while using the Samsung device.



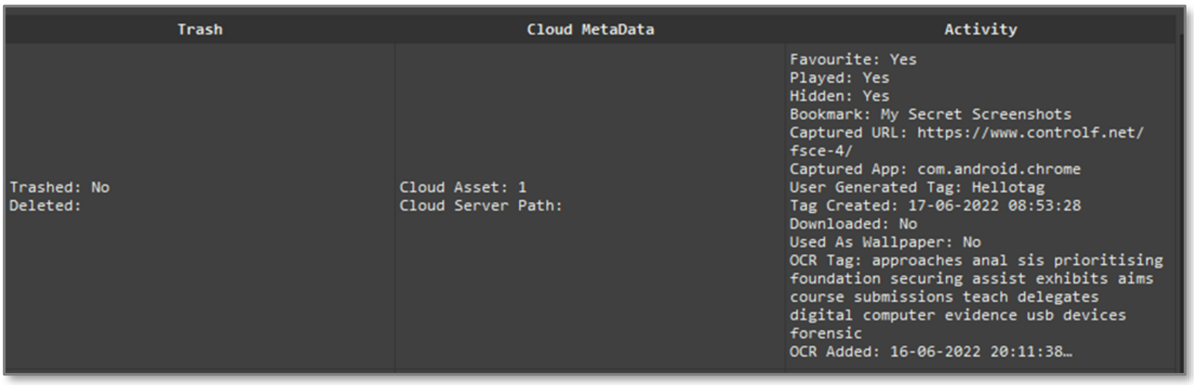
```
media
```

```
File Info

Filename:
Screenshot_20220616-210808_Chrome
Display Name:
Screenshot_20220616-210808_Chrome.jpg
System Path: DCIM/Screenshots/
Size: 516669
Size (MB): 0.49
Resolution: 1080×2280
Type: Image
Mime Type: image/jpeg
Original Hash:
```

```
Other

Parent Package: com.android.systemui
Identifier: -1313584517
Identifier Name: Screenshots
Orientation: 90.0
Private: Yes
Duration:
Recording Mode:
Video Codec:
Audio Codec:
```

Figure 10

We can identify useful metadata information, such as the original filename, resolution, and originating package information (in this case, identifying this to have been captured by the system user interface). Moving into FIGURE 11 we can see further activity has been recorded.



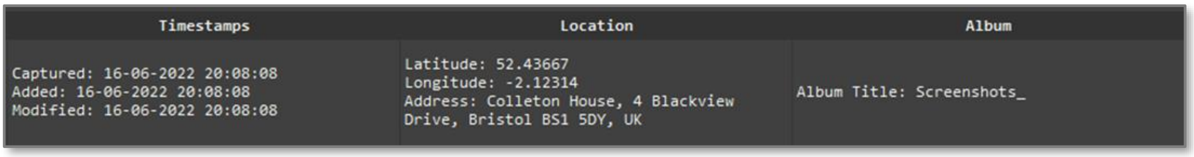
```
Trash

Trashed: No
Deleted:
```

```
Cloud MetaData

Cloud Asset: 1
Cloud Server Path:
```

```
Activity

Favourite: Yes
Played: Yes
Hidden: Yes
Bookmark: My Secret Screenshots
Captured URL: https://www.controlf.net/
fsce-4/
Captured App: com.android.chrome
User Generated Tag: Hellotag
Tag Created: 17-06-2022 08:53:28
Downloaded: No
Used As Wallpaper: No
OCR Tag: approaches anal sis prioritising
foundation securing assist exhibits aims
course submissions teach delegates
digital computer evidence usb devices
forensic
OCR Added: 16-06-2022 20:11:38…
```

Figure 11

mift has been able to locate, decode, and present a number of pattern-of-life (POL) properties, many of which have been collated within the "*Activity*" column. Other properties are captured within columns visible within FIGURE 12, as can be seen below.



Timestamps	Location	Album
Captured: 16-06-2022 20:08:08 Added: 16-06-2022 20:08:08 Modified: 16-06-2022 20:08:08	Latitude: 52.43667 Longitude: -2.12314 Address: Colleton House, 4 Blackview Drive, Bristol BS1 5DY, UK	Album Title: Screenshots_

Figure 12

Location data is visible in FIGURE 12 as well as a lookup that is conducted at the time of the image's generation. In FIGURE 11 we can see the URL of the page being viewed when the screenshot was captured and also whether the image has been viewed. Samsung appears to perform some OCR (optical character recognition) on the image to recover text from it and we can see from FIGURE 11 that the results are recorded and recoverable.

In addition to all the information and data already recovered, we can also see if the image was downloaded and if it has been used as a wallpaper, which may be relevant during an investigation.

Using mift we can provide far more context to the generation of a media file and any subsequent activity related to it.