MSAB BLOG

Traces for Deleted photo/video Under Apple Photos app



OSCAR CHOI
MSAB DIGITAL FORENSIC SPECIALIST

MSAB
Trusted Partner in Digital Forensics

Background

Establishing that a photograph or video was captured at a specific time can be crucial in a criminal investigation, particularly in cases involving offenses such as upskirting.

In many instances, by the time officers arrive at the scene or examine a suspect's device, the relevant photograph or video may already have been permanently deleted.

MSAB
Trusted Partner in Digital Forensics

01 — BACKGROUND

With modern mobile devices using file-based encryption (FBE), recovering permanently deleted photos or videos can be extremely difficult and, in many cases, may not be possible using current forensic techniques.

Apple iPhones also use file-based encryption, presenting similar challenges when attempting to recover deleted media.

However, even when the original photograph or video can no longer be recovered, other forensic traces may remain on the device. These artifacts can potentially provide evidence that a photograph or video was captured at a particular time, even though the media itself has been permanently deleted.

This blog explores forensic traces associated with photos and videos that have been permanently deleted by a user through the Apple Photos app, and how these artifacts may assist investigators in establishing that a capture event occurred.

MSAB
Trusted Partner in Digital Forensics

Conclusion

Even when a photo or video has been permanently deleted and the original media can no longer be recovered, this experiment demonstrates that multiple forensic traces may remain on the device. Importantly, useful evidence may be available even when the acquisition is limited to an iTunes backup, as the Photos.sqlite database and its associated data can provide valuable information about deleted media.

The traces identified during this experiment included evidence of the permanent deletion event, historical information relating to the creation of the media asset, recovered deleted ZASSET records, the original filename, and additional metadata such as camera information.

When these artifacts are correlated, they can help reconstruct the history of a deleted photo or video even when the media itself is no longer available.

A full file system extraction may provide further opportunities to identify supporting evidence from additional sources, including File System Events, Biome, and the Unified Log. Correlating information from these sources with artifacts recovered from Photos.sqlite may provide an even more complete picture of activity on the device.

The key takeaway for investigators is therefore simple:

where possible, acquire the device as soon as possible. Many of these forensic artifacts are transient and may be automatically purged, overwritten, or otherwise become unavailable over time.

The longer the delay between the relevant activity and acquisition, the greater the possibility that potentially valuable traces will be lost.

MSAB
Trusted Partner in Digital Forensics

Overview of the Apple Photos App

The Apple Photos app is the central location for managing photos and videos across Apple devices, including iPhone, iPad, and Mac. Users can browse, organize, edit, share, and delete photos and videos through the app.

At the heart of the Photos app is the Photos.sqlite database. This is the primary database used to store metadata and organizational information relating to the user's photo and video library.

From a digital forensic perspective, this database can provide valuable information about media stored on the device and how it has been managed by the user.



MSAB
Trusted Partner in Digital Forensics

How Apple Photos Handles Deleted Items

The deletion process can broadly be divided into three stages:

1. Soft deletion

When a user deletes a photo or video through the Photos app, the item is not immediately permanently removed. Instead:

- The item is moved to the Recently Deleted collection.
- The associated media file remains on the device.
- The Photos database continues to maintain information and references relating to the deleted item.

2. Retention period

Items within Recently Deleted are normally retained for up to 30 days, giving the user an opportunity to recover them. During this period:

- The photo or video remains recoverable through the Photos app.
- The underlying media file remains available in storage.
- Relevant metadata and database references continue to exist.

MSAB
Trusted Partner in Digital Forensics

3. Permanent deletion

An item can be permanently deleted either when its retention period expires or when the user manually deletes it from Recently Deleted. At this point:

- The item is removed from the user's Photos library.
- Associated database records and references may be removed or altered.
- The underlying media file is deleted, and its storage may subsequently become available for reuse.

For a forensic examiner, this final stage presents the greatest challenge.

On modern iOS devices using file-based encryption, recovery of the original media file after permanent deletion may not be possible.

However, the deletion of the media and its primary database record does not necessarily mean that every trace of the original capture has disappeared.

Other artifacts may remain elsewhere on the device, potentially providing evidence that a photo or video was captured even when the original media can no longer be recovered.

MSAB
Trusted Partner in Digital Forensics



03 — EXPERIMENT

Experiment

To better understand what happens within the **Photos.sqlite** database when a photo is permanently deleted, some validation was carried out.

MSAB
Trusted Partner in Digital Forensics

Two extractions of the same device were performed: one **before** and one **after** a selected photo was permanently deleted from the Apple Photos app. The resulting **Photos.sqlite** databases were then compared, focusing initially on changes in the number of records within each database table.

By comparing the database before and after permanent deletion, we can identify which tables are affected by the deletion process and determine whether any potentially useful forensic traces remain.

Device:	Apple iPhone 12 mini
Operating System:	18.7 (22H20)
Extraction Tool & Method:	MSAB XRY Pro version 11.2.1 (Full File System with optimized)
Decoding Tool:	MSAB XRY Pro version 11.3

MSAB
Trusted Partner in Digital Forensics

Figure 1.0 - Analysis Tool: XAMN Pro version 8.4 and DB Browser for SQLite Version 3.13.1

/private/var/mobile/Media/PhotoData/Photos.sqlite database BEFORE deleted a photo (part 1)

ACHANGE	6536
ATRANSACTION	1040
ATRANSACTIONSTRING	174
sqlite_master	558
Z_1KEYWORDS	0
Z_20CLUSTERREJECTEDPERSONS	0
Z_20REJECTEDPERSONS	0
Z_20REJECTEDPERSONSNEEDINGFACECROPS	0
Z_29ALBUMLISTS	37
Z_29KEYASSETS	0
Z_30ASSETS	0
Z_3MEMORIESBEINGCURATEDASSETS	26
Z_3MEMORIESBEINGCUSTOMUSERASSETS	0
Z_3MEMORIESBEINGEXTENDEDCURATEDASSETS	26
Z_3MEMORIESBEINGMOVIECURATEDASSETS	0
Z_3MEMORIESBEINGREPRESENTATIVEASSETS	26
Z_3MEMORIESBEINGUSERCURATEDASSETS	0
Z_3MEMORIESBEINGUSERREMOVEDASSETS	0
Z_3SUGGESTIONSBEINGKEYASSETS	10
Z_3SUGGESTIONSBEINGREPRESENTATIVEASSETS	0
Z_41LABELS	1
Z_43NODESBEINGADDITIONALLABEL	0
Z_54INVALIDMERGECANDIDATES	0
Z_54MERGECANDIDATES	0
Z_54MERGECANDIDATESWITHCONFIDENCE	0
Z_METADATA	1
Z_MODELCACHE	1
Z_PRIMARYKEY	71
Z_RT_Asset_boundedByRect_node	1
Z_RT_Asset_boundedByRect_parent	0
Z_RT_Asset_boundedByRect_rowid	2
ZADDITIONALASSETATTRIBUTES	51
ZALBUMLIST	7
ZASSET	51
ZASSETANALYSISSTATE	0
ZASSETCONTRIBUTOR	0
ZASSETDESCRIPTION	0
ZBACKGROUNDJOBWORKITEM	22
ZCHARACTERRECOGNITIONATTRIBUTES	51
ZCLOUDFEEDENTRY	0

/private/var/mobile/Media/PhotoData/Photos.sqlite database AFTER deleted a photo (part 1)

ACHANGE	6561
ATRANSACTION	1049
ATRANSACTIONSTRING	174
sqlite_master	558
Z_1KEYWORDS	0
Z_20CLUSTERREJECTEDPERSONS	0
Z_20REJECTEDPERSONS	0
Z_20REJECTEDPERSONSNEEDINGFACECROPS	0
Z_29ALBUMLISTS	37
Z_29KEYASSETS	0
Z_30ASSETS	0
Z_3MEMORIESBEINGCURATEDASSETS	26
Z_3MEMORIESBEINGCUSTOMUSERASSETS	0
Z_3MEMORIESBEINGEXTENDEDCURATEDASSETS	26
Z_3MEMORIESBEINGMOVIECURATEDASSETS	0
Z_3MEMORIESBEINGREPRESENTATIVEASSETS	26
Z_3MEMORIESBEINGUSERCURATEDASSETS	0
Z_3MEMORIESBEINGUSERREMOVEDASSETS	0
Z_3SUGGESTIONSBEINGKEYASSETS	10
Z_3SUGGESTIONSBEINGREPRESENTATIVEASSETS	0
Z_41LABELS	1
Z_43NODESBEINGADDITIONALLABEL	0
Z_54INVALIDMERGECANDIDATES	0
Z_54MERGECANDIDATES	0
Z_54MERGECANDIDATESWITHCONFIDENCE	0
Z_METADATA	1
Z_MODELCACHE	1
Z_PRIMARYKEY	71
Z_RT_Asset_boundedByRect_node	1
Z_RT_Asset_boundedByRect_parent	0
Z_RT_Asset_boundedByRect_rowid	2
ZADDITIONALASSETATTRIBUTES	50
ZALBUMLIST	7
ZASSET	50
ZASSETANALYSISSTATE	0
ZASSETCONTRIBUTOR	0
ZASSETDESCRIPTION	0
ZBACKGROUNDJOBWORKITEM	21
ZCHARACTERRECOGNITIONATTRIBUTES	50
ZCLOUDFEEDENTRY	0

MSAB
Trusted Partner in Digital Forensics

Figure 1.0 - Analysis Tool: XAMN Pro version 8.4 and DB Browser for SQLite Version 3.13.1

/private/var/mobile/Media/PhotoData/Photos.sqlite database BEFORE deleted a photo (part 2)

ZCLOUDMASTER	51 (...)
ZCLOUDMASTERMEDIAMETADATA	51 (...)
ZCLOUDRESOURCE	0 (...)
ZCLOUDSHAREDALBUMINVITATIONRECORD	0 (...)
ZCLOUDSHAREDCOMMENT	0 (...)
ZCOMPUTEDASSETATTRIBUTES	51 (...)
ZCOMPUTESYNCATTRIBUTES	49 (...)
ZDEFERREDREBUILDFACE	0 (...)
ZDETECTEDFACE	7 (...)
ZDETECTEDFACEGROUP	0 (...)
ZDETECTEDFACEPRINT	7 (...)
ZDETECTIONTRAIT	0 (...)
ZEDITEDIPTCATTRIBUTES	0 (...)
ZEXTENDEDATTRIBUTES	51 (...)
ZFACECROP	0 (...)
ZFILESYSTEMBOOKMARK	0 (...)
ZFILESYSTEMVOLUME	0 (...)
ZGENERICALBUM	47 (...)
ZGLOBALKEYVALUE	45 (...)
ZGRAPHEDGE	7 (...)
ZGRAPHEDGEVALUE	0 (...)
ZGRAPHLABEL	11 (...)
ZGRAPHNODE	32 (...)
ZGRAPHNODEVALUE	128 (...)
ZINTERNALRESOURCE	300 (...)
ZKEYWORD	0 (...)
ZLEGACYFACE	0 (...)
ZLIMITEDLIBRARYFETCHFILTER	0 (...)
ZMEDIAANALYSISASSETATTRIBUTES	51 (...)
ZMEMORY	1 (...)
ZMIGRATIONHISTORY	6 (...)
ZMOMENT	10 (...)
ZPERSON	9 (...)
ZPERSONREFERENCE	0 (...)
ZPHOTOANALYSISASSETATTRIBUTES	51 (...)
ZPHOTOSHIGHLIGHT	13 (...)
ZQUESTION	0 (...)
ZSCENECLASSIFICATION	2260 (...)
ZSCENEPRINT	51 (...)
ZSHARE	0 (...)

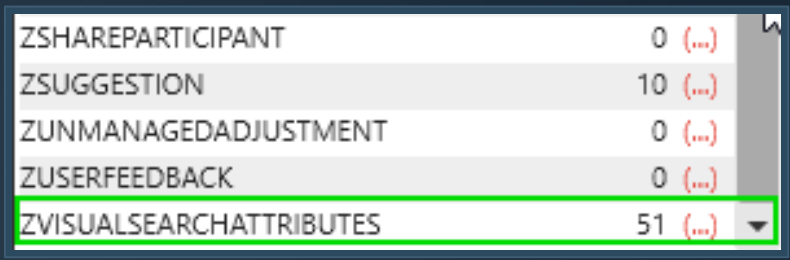
/private/var/mobile/Media/PhotoData/Photos.sqlite database AFTER deleted a photo (part 2)

ZCLOUDMASTER	50 (...)
ZCLOUDMASTERMEDIAMETADATA	50 (...)
ZCLOUDRESOURCE	0 (...)
ZCLOUDSHAREDALBUMINVITATIONRECORD	0 (...)
ZCLOUDSHAREDCOMMENT	0 (...)
ZCOMPUTEDASSETATTRIBUTES	50 (...)
ZCOMPUTESYNCATTRIBUTES	49 (...)
ZDEFERREDREBUILDFACE	0 (...)
ZDETECTEDFACE	7 (...)
ZDETECTEDFACEGROUP	0 (...)
ZDETECTEDFACEPRINT	7 (...)
ZDETECTIONTRAIT	0 (...)
ZEDITEDIPTCATTRIBUTES	0 (...)
ZEXTENDEDATTRIBUTES	50 (...)
ZFACECROP	0 (...)
ZFILESYSTEMBOOKMARK	0 (...)
ZFILESYSTEMVOLUME	0 (...)
ZGENERICALBUM	47 (...)
ZGLOBALKEYVALUE	45 (...)
ZGRAPHEDGE	7 (...)
ZGRAPHEDGEVALUE	0 (...)
ZGRAPHLABEL	11 (...)
ZGRAPHNODE	32 (...)
ZGRAPHNODEVALUE	128 (...)
ZINTERNALRESOURCE	298 (...)
ZKEYWORD	0 (...)
ZLEGACYFACE	0 (...)
ZLIMITEDLIBRARYFETCHFILTER	0 (...)
ZMEDIAANALYSISASSETATTRIBUTES	50 (...)
ZMEMORY	1 (...)
ZMIGRATIONHISTORY	6 (...)
ZMOMENT	10 (...)
ZPERSON	9 (...)
ZPERSONREFERENCE	0 (...)
ZPHOTOANALYSISASSETATTRIBUTES	50 (...)
ZPHOTOSHIGHLIGHT	13 (...)
ZQUESTION	0 (...)
ZSCENECLASSIFICATION	2252 (...)
ZSCENEPRINT	50 (...)
ZSHARE	0 (...)

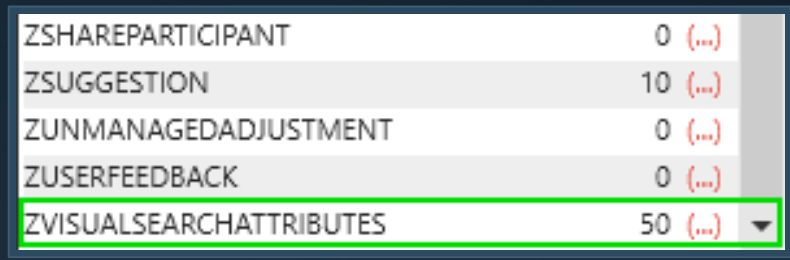
MSAB
Trusted Partner in Digital Forensics

Figure 1.0 - Analysis Tool: XAMN Pro version 8.4 and DB Browser for SQLite Version 3.13.1

/private/var/mobile/Media/PhotoData/Photos.sqlite database BEFORE deleted a photo (part 3)



/private/var/mobile/Media/PhotoData/Photos.sqlite database AFTER deleted a photo (part 3)



After comparing the number of records in each table, the results are as follows:

Table 1 - Where the number of records increased

Table Name	Number of records increased
ACHANGE	25
ATRANSACTION	9

MSAB
Trusted Partner in Digital Forensics

Table 2 - Where the number of records decreased

Table Name	Number of records decreased
ZADDITIONALASSETATTRIBUTES	1
ZASSET	1
ZBACKGROUNDJOBWORKITEM	1
ZCHARACTERRECOGNITIONATTRIBUTES	1
ZCLOUDMASTER	1
ZCLOUDMASTERMEDIAMETADATA	1
ZCOMPUTEDASSETATTRIBUTES	1
ZEXTENDEDATTRIBUTES	1
ZINTERNALRESOURCE	2
ZMEDIAANALYSISASSETATTRIBUTES	1
ZPHOTOANALYSISASSETATTRIBUTES	1
ZSCENECLASSIFICATION	8
ZSCENEPRINT	1
ZVISUALSEARCHATTRIBUTES	1

Interestingly, after the photo was permanently deleted, the number of records in some database tables actually **increased**.

This may initially seem unexpected, as we might assume that deleting an item would result only in records being removed.

To understand why this happens, let's take a closer look at each of the affected tables and examine what changes occur during the permanent deletion process.

MSAB
Trusted Partner in Digital Forensics

ACHANGE and ATRANSACTION

The ACHANGE table and ATRANSACTION table are parts of the Apple's Core Data for Persistent History Tracking. In Core Data, when the storage format is SQLite and the persistent history tracking function is enabled, any changes like insert, update and delete of the data in database will trigger a system notification and register on those tables.

For more details, please refer to
https://fatbobman.com/en/posts/tables_and_fields_of_coredata/

The ACHANGE table is a transaction log/changelog table within Photos.sqlite that tracks modifications for synchronization purposes.

MSAB
Trusted Partner in Digital Forensics

Based on analysis, this table contains:

Column	Purpose	Example
ZCHANGETYPE	Type of change	0 – insert 1 – update 2 - delete
ZENTITY	Table affected	Link with Z_PRIMARYKEY table. To understand which table is affected, can match by ACHANGE.ZENTITY = Z_PRIMARYKEY.Z_ENT and Z_PRIMARYKEY.Z_SUPER = 0, if Z_PRIMARYKEY.Z_Super != 0, then need to base on the Z_Super value to locate the corresponding table within Z_PRIMARYKEY table
ZENTITYPK	Record affected	Link with the affected table. To understand which record is affected, can match by ACHANGE.ZENTITYPK = AffectedTable.Z_PK
ZCOLUMNS	Column affected	It is using bit masking method to represent each column, need to map with corresponding mapping table
ZTRANSACTIONID	SQLite transaction details	Link with ATRANSACTION table and ATRANSACTIONSTING table. To understand the transaction details, can match by ACHANGE.ZTRANSACTIONID = ATRANSACTION.Z_PK and ATRANSACTION.ZCONTEXTNAMETS = ATRANSACTIONSTRING.Z_PK

Table 3 – Explanation on columns found in ACHANGE table

MSAB
Trusted Partner in Digital Forensics

When a photo or video file is permanently deleted, the corresponding entries under the Photos.sqlite database will be erased, and the Persistent History Tracking will be triggered to record the delete action on the ACHANGE table. This is because this table will monitor the delete action of the Photos.sqlite table.

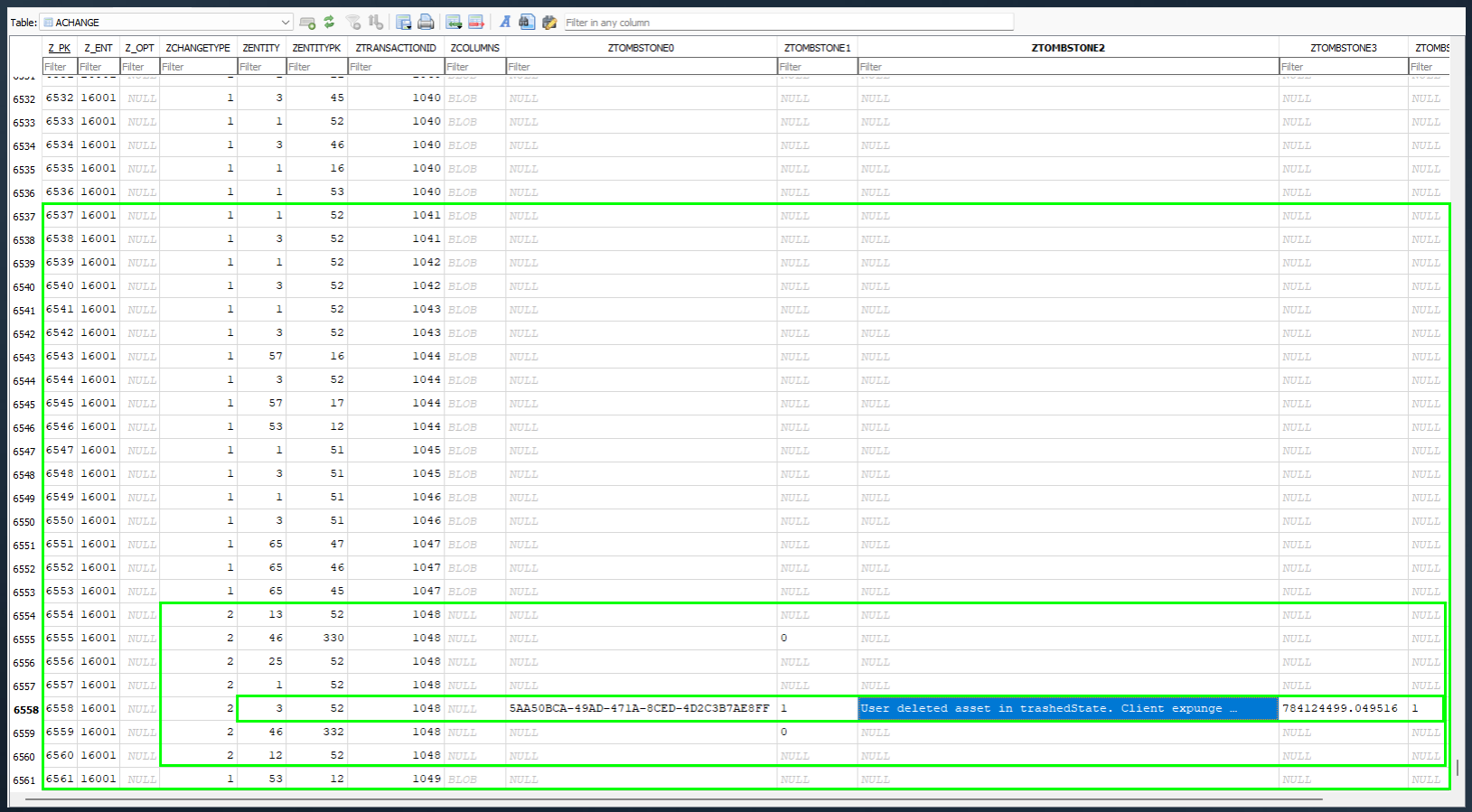


Table: ACHANGE

Filter in any column

	Z_PK	Z_ENT	Z_OPT	ZCHANGETYPE	ZENTITY	ZENTITYPK	ZTRANSACTIONID	ZCOLUMNS	ZTOMBSTONE0	ZTOMBSTONE1	ZTOMBSTONE2	ZTOMBSTONE3	ZTOMBS
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
6532	6532	16001	NULL	1	3	45	1040	BLOB	NULL	NULL	NULL	NULL	NULL
6533	6533	16001	NULL	1	1	52	1040	BLOB	NULL	NULL	NULL	NULL	NULL
6534	6534	16001	NULL	1	3	46	1040	BLOB	NULL	NULL	NULL	NULL	NULL
6535	6535	16001	NULL	1	1	16	1040	BLOB	NULL	NULL	NULL	NULL	NULL
6536	6536	16001	NULL	1	1	53	1040	BLOB	NULL	NULL	NULL	NULL	NULL
6537	6537	16001	NULL	1	1	52	1041	BLOB	NULL	NULL	NULL	NULL	NULL
6538	6538	16001	NULL	1	3	52	1041	BLOB	NULL	NULL	NULL	NULL	NULL
6539	6539	16001	NULL	1	1	52	1042	BLOB	NULL	NULL	NULL	NULL	NULL
6540	6540	16001	NULL	1	3	52	1042	BLOB	NULL	NULL	NULL	NULL	NULL
6541	6541	16001	NULL	1	1	52	1043	BLOB	NULL	NULL	NULL	NULL	NULL
6542	6542	16001	NULL	1	3	52	1043	BLOB	NULL	NULL	NULL	NULL	NULL
6543	6543	16001	NULL	1	57	16	1044	BLOB	NULL	NULL	NULL	NULL	NULL
6544	6544	16001	NULL	1	3	52	1044	BLOB	NULL	NULL	NULL	NULL	NULL
6545	6545	16001	NULL	1	57	17	1044	BLOB	NULL	NULL	NULL	NULL	NULL
6546	6546	16001	NULL	1	53	12	1044	BLOB	NULL	NULL	NULL	NULL	NULL
6547	6547	16001	NULL	1	1	51	1045	BLOB	NULL	NULL	NULL	NULL	NULL
6548	6548	16001	NULL	1	3	51	1045	BLOB	NULL	NULL	NULL	NULL	NULL
6549	6549	16001	NULL	1	1	51	1046	BLOB	NULL	NULL	NULL	NULL	NULL
6550	6550	16001	NULL	1	3	51	1046	BLOB	NULL	NULL	NULL	NULL	NULL
6551	6551	16001	NULL	1	65	47	1047	BLOB	NULL	NULL	NULL	NULL	NULL
6552	6552	16001	NULL	1	65	46	1047	BLOB	NULL	NULL	NULL	NULL	NULL
6553	6553	16001	NULL	1	65	45	1047	BLOB	NULL	NULL	NULL	NULL	NULL
6554	6554	16001	NULL	2	13	52	1048	NULL	NULL	NULL	NULL	NULL	NULL
6555	6555	16001	NULL	2	46	330	1048	NULL	NULL	0	NULL	NULL	NULL
6556	6556	16001	NULL	2	25	52	1048	NULL	NULL	NULL	NULL	NULL	NULL
6557	6557	16001	NULL	2	1	52	1048	NULL	NULL	NULL	NULL	NULL	NULL
6558	6558	16001	NULL	2	3	52	1048	NULL	5AA50BCA-49AD-471A-8CED-4D2C3B7AE8FF	1	User deleted asset in trashedState. Client expunge …	784124499.049516	1
6559	6559	16001	NULL	2	46	332	1048	NULL	NULL	0	NULL	NULL	NULL
6560	6560	16001	NULL	2	12	52	1048	NULL	NULL	NULL	NULL	NULL	NULL
6561	6561	16001	NULL	1	53	12	1049	BLOB	NULL	NULL	NULL	NULL	NULL

MSAB
Trusted Partner in Digital Forensics

When examining the additional records made on the ACHANGE table after deleting a photo, there are seven records related to deletion. When trying to match those tables I found the number of records decreased, as seen below.

Table 4 – In total 6 tables are synced with the ACHANGE table deletion records

Table Name	Number of records decreased	ZENTITY
ZADDITIONALASSETATTRIBUTES	**1**	**1**
ZASSET	**1**	**3**
ZBACKGROUNDJOBWORKITEM	1	7
ZCHARACTERRECOGNITIONATTRIBUTES	1	8
ZCLOUDMASTER	**1**	**12**
ZCLOUDMASTERMEDIAMETADATA	**1**	**13**
ZCOMPUTEDASSETATTRIBUTES	1	17
ZEXTENDEDATTRIBUTES	**1**	**25**
ZINTERNALRESOURCE	**2**	**46**
ZMEDIAANALYSISASSETATTRIBUTES	1	50
ZPHOTOANALYSISASSETATTRIBUTES	1	56
ZSCENECLASSIFICATION	8	59
ZSCENEPRINT	1	60
ZVISUALSEARCHATTRIBUTES	1	68

MSAB
Trusted Partner in Digital Forensics

The ZASSET table

The ZASSET table is the central, most important table in Photos.sqlite database. It serves as the master catalog for every photo and video in Apple Photos app library.

Within the ACHANGE table, a record can be identified that represents a deletion event associated with the ZASSET table.

This record contains potentially valuable forensic information, including the UUID of the corresponding media asset, the reason for permanent deletion, and the timestamp indicating when the asset was moved to the trash.

This is particularly significant from a forensic perspective, as it demonstrates that even after the original media and its associated asset record have been permanently deleted, information relating to the deletion event may still remain within the Photos database.

MSAB
Trusted Partner in Digital Forensics

04 — FORENSIC TRACES

Try to filter ACHANGE table by ZCHANGETYPE = 2 (delete action) and ZENTITY = 3 (ZASSET table) and link with ATRANSACTION table, all the deleted media file(s) can be easily listed out. Below is an example of how this filtering was applied to the sample data.

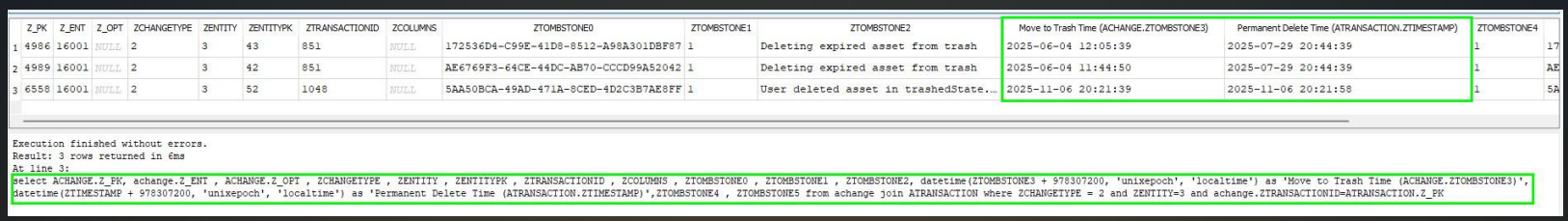
There are three media files (42, 43, 52) that have been deleted, 52 is the one deleted for this experiment. It can clearly show the two permanent delete methods, one is automatically deleted by the system when the retention period is expired (Deleting expired asset from trash), and one is manually deleted by phone user (User deleted asset in trashedState.

Within the ACHANGE table, a record can be identified that represents a deletion event associated with the ZASSET table. This record contains potentially valuable forensic information, including the UUID of the corresponding media asset, the permanent deletion reason, and the timestamp indicating when the asset was moved to the trash.

In this example, the Client Expunge Reason is recorded as “UI expunge from recently deleted”, indicating that the media was permanently deleted through the user interface from the Recently Deleted collection.

FORENSIC TRACE 01

This provides the first forensic trace of the permanently deleted media. Although the original photo is no longer available, the ACHANGE table retains information linking the deletion event to a specific asset UUID and provides context about how the item was permanently deleted.



	Z_PK	Z_ENT	Z_OPT	ZCHANGETYPE	ZENTITY	ZENTITYPK	ZTRANSACTIONID	ZCOLUMNS	ZTOMBSTONE0	ZTOMBSTONE1	ZTOMBSTONE2	Move to Trash Time (ACHANGE.ZTOMBSTONE3)	Permanent Delete Time (ATRANSACTION.ZTIMESTAMP)	ZTOMBSTONE4	
1	4986	16001	NULL	2	3	43	851	NULL	172536D4-C99E-41D8-8512-A98A301DBF87	1	Deleting expired asset from trash	2025-06-04 12:05:39	2025-07-29 20:44:39	1	17
2	4989	16001	NULL	2	3	42	851	NULL	AE6769F3-64CE-44DC-AB70-CCCD99A52042	1	Deleting expired asset from trash	2025-06-04 11:44:50	2025-07-29 20:44:39	1	AE
3	6558	16001	NULL	2	3	52	1048	NULL	5AA50BCA-49AD-471A-8CED-4D2C3B7AE8FF	1	User deleted asset in trashedState.…	2025-11-06 20:21:39	2025-11-06 20:21:58	1	5A

```
Execution finished without errors.
Result: 3 rows returned in 6ms
At line 3:
select ACHANGE.Z_PK, achange.Z_ENT , ACHANGE.Z_OPT , ZCHANGETYPE , ZENTITY , ZENTITYPK , ZTRANSACTIONID , ZCOLUMNS , ZTOMBSTONE0 , ZTOMBSTONE1 , ZTOMBSTONE2, datetime(ZTOMBSTONE3 + 978307200, 'unixepoch', 'localtime') as 'Move to Trash Time (ACHANGE.ZTOMBSTONE3)',
datetime(ZTIMESTAMP + 978307200, 'unixepoch', 'localtime') as 'Permanent Delete Time (ATRANSACTION.ZTIMESTAMP)',ZTOMBSTONE4 , ZTOMBSTONE5 from achange join ATRANSACTION where ZCHANGETYPE = 2 and ZENTITY=3 and achange.ZTRANSACTIONID=ATRANSACTION.Z_PK
```


MSAB
Trusted Partner in Digital Forensics

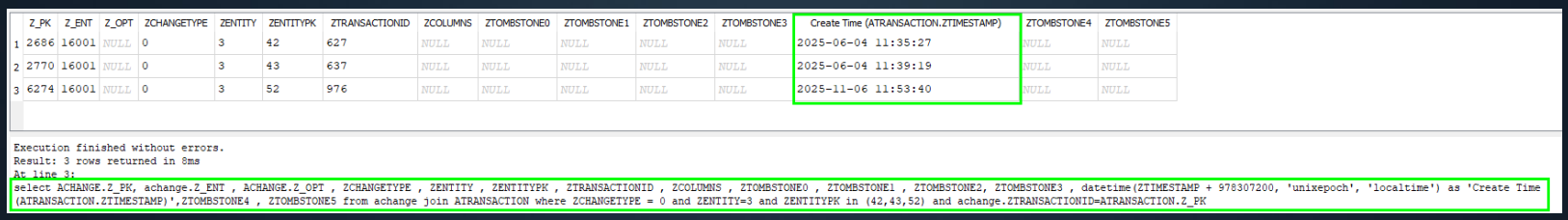
04 — FORENSIC TRACES

Identifying when the media file was deleted provides valuable information, but establishing when the media was originally created can be even more significant to an investigation.

As the ACHANGE and ATRANSACTION tables provide persistent history tracking, the creation of the original media record within Photos.sqlite may also be captured within this history. By correlating these historical records using the asset UUID, it may be possible to identify information relating to when the media asset was first created.

FORENSIC TRACE 02

This provides the second forensic trace. Even though the original photo or video and its primary database record have been permanently deleted, the persistent history may retain evidence relating to the original creation of that asset.



Z_PK	Z_ENT	Z_OPT	ZCHANGETYPE	ZENTITY	ZENTITYPK	ZTRANSACTIONID	ZCOLUMNS	ZTOMBSTONE0	ZTOMBSTONE1	ZTOMBSTONE2	ZTOMBSTONE3	Create Time (ATRANSACTION.ZTIMESTAMP)	ZTOMBSTONE4	ZTOMBSTONE5
1 2686	16001	NULL	0	3	42	627	NULL	NULL	NULL	NULL	NULL	2025-06-04 11:35:27	NULL	NULL
2 2770	16001	NULL	0	3	43	637	NULL	NULL	NULL	NULL	NULL	2025-06-04 11:39:19	NULL	NULL
3 6274	16001	NULL	0	3	52	976	NULL	NULL	NULL	NULL	NULL	2025-11-06 11:53:40	NULL	NULL

Execution finished without errors.
Result: 3 rows returned in 8ms
At line 3:

```
select ACHANGE.Z_PK, achange.Z_ENT , ACHANGE.Z_OPT , ZCHANGETYPE , ZENTITY , ZENTITYPK , ZTRANSACTIONID , ZCOLUMNS , ZTOMBSTONE0 , ZTOMBSTONE1 , ZTOMBSTONE2, ZTOMBSTONE3 , datetime(ZTIMESTAMP + 978307200, 'unixepoch', 'localtime') as 'Create Time (ATRANSACTION.ZTIMESTAMP)',ZTOMBSTONE4 , ZTOMBSTONE5 from achange join ATRANSACTION where ZCHANGETYPE = 0 and ZENTITY=3 and ZENTITYPK in (42,43,52) and achange.ZTRANSACTIONID=ATRANSACTION.Z_PK
```

UUID	Create Time (UTC+8)	Move to Trash Time (UTC+8)	Permanent Delete Time (UTC+8)	Permanent Delete Reason
172536D4-C99E-41D8-8512-A98A301DBF87 (record 43)	4 Jun 2025 11:35:27	4 Jun 2025 12:05:39	29 Jul 2025 20:44:39	Deleting expired asset from trash
AE6769F3-64CE-44DC-AB70-CCCD99A52042 (record 42)	4 Jun 2025 11:39:19	4 Jun 2025 11:44:50	29 Jul 2025 20:44:39	Deleting expired asset from trash
5AA50BCA-49AD-471A-8CED-4D2C3B7AE8FF (record 52)	**6 Nov 2025 11:53:40**	**6 Nov 2025 20:21:39**	**6 Nov 2025 20:21:58**	**User deleted asset in trashedState. Client expunge reason: UI expunge from recently deleted**

Write-Ahead Logging (WAL)

The Photos.sqlite database uses SQLite's Write-Ahead Logging (WAL) mechanism. Rather than writing every database change directly to the main database file, SQLite can first record changes within the associated WAL file.

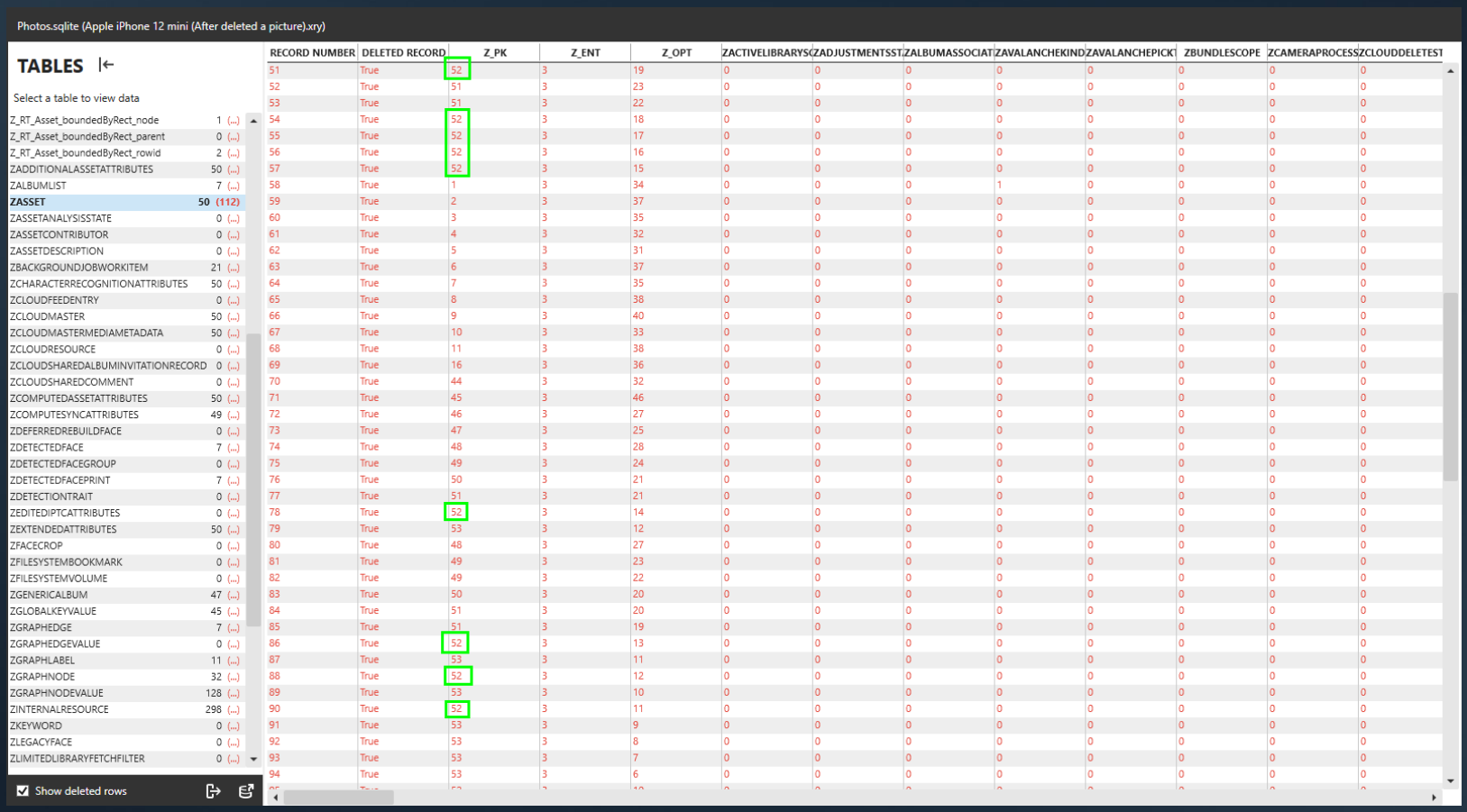
Importantly for forensic examination, both full file system extractions and iTunes backup extractions can include the WAL file associated with Photos.sqlite.

Depending on the state of the database and WAL at the time of acquisition, this may provide an additional opportunity to identify records or data relating to previously deleted assets.

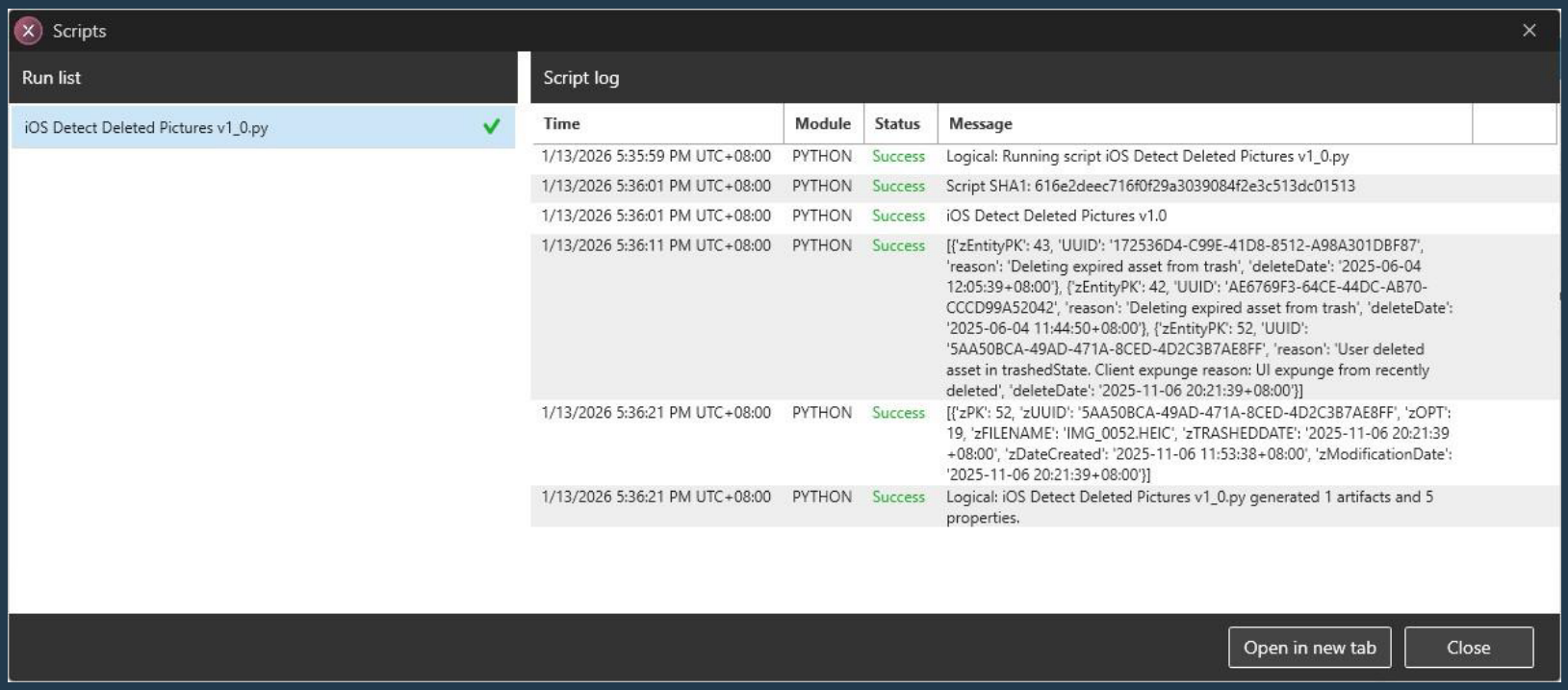
When examining Photos.sqlite using the SQLite Viewer in XAMN Pro, 112 deleted records were identified within the ZASSET table. Several of these records were associated with record 52, which corresponds to the photo that was permanently deleted during this experiment.

MSAB
Trusted Partner in Digital Forensics

This provides another potentially valuable source of forensic evidence. Although the active ZASSET record may no longer be present following permanent deletion, remnants of that record may still be recoverable and could contain information about the original media asset.



MSAB
Trusted Partner in Digital Forensics



Using the Python scripting module in XAMN Pro, SQL queries can be applied to the recovered deleted records, making it easier to identify and correlate records associated with a specific deleted media asset.

MSAB
Trusted Partner in Digital Forensics

In this test, a Python script was used to perform the following process:

1. Identify deletion records relating to the ZASSET table within the ZCHANGE table.
2. Extract the corresponding record numbers referenced by those deletion events.
3. Search the recovered deleted records within the ZASSET table for records matching those record numbers.
4. Return the matching results for further examination.

The results below show the output of this process. By correlating the deletion history in ZCHANGE with recovered records from ZASSET, it is possible to locate remnants associated with the permanently deleted media and examine the metadata that may still be available.

This approach significantly reduces the need to manually review large numbers of recovered deleted records and provides a more targeted method for identifying artifacts associated with permanently deleted photos or videos.

MSAB
Trusted Partner in Digital Forensics

Records found in ZCHANGE table in JSON format


```
[
  {
    "zEntityPK":43,
    "UUID":"172536D4-C99E-41D8-8512-A98A301DBF87",
    "reason":"Deleting expired asset from trash",
    "deleteDate":"2025-06-04 12:05:39+08:00"
  },
  {
    "zEntityPK":42,
    "UUID":"AE6769F3-64CE-44DC-AB70-CCCD99A52042",
    "reason":"Deleting expired asset from trash",
    "deleteDate":"2025-06-04 11:44:50+08:00"
  },
  {
    "zEntityPK":52,
    "UUID":"5AA50BCA-49AD-471A-8CED-4D2C3B7AE8FF",
    "reason":"User deleted asset in trashedState. Client
              expunge reason: UI expunge from recently deleted",
    "deleteDate":"2025-11-06 20:21:39+08:00"
  }
]
```


MSAB
Trusted Partner in Digital Forensics

Deleted record found in ZASSET table in JSON format


```
[
  {
    "zPK":52,
    "zUUID":"5AA50BCA-49AD-471A-8CED-4D2C3B7AE8FF",
    "zOPT":19,
    "zFILENAME":"IMG_0052.HEIC",
    "zTRASHEDDATE":"2025-11-06 20:21:39+08:00",
    "zDateCreated":"2025-11-06 11:53:38+08:00",
    "zModificationDate":"2025-11-06 20:21:39+08:00"
  }
]
```


In this experiment, only the deleted ZASSET record for item 52 could be recovered. The records associated with items 42 and 43 were no longer recoverable.

One possible explanation is that these records had already been overwritten following a WAL checkpoint, although this cannot be confirmed from the available data alone.

MSAB
Trusted Partner in Digital Forensics

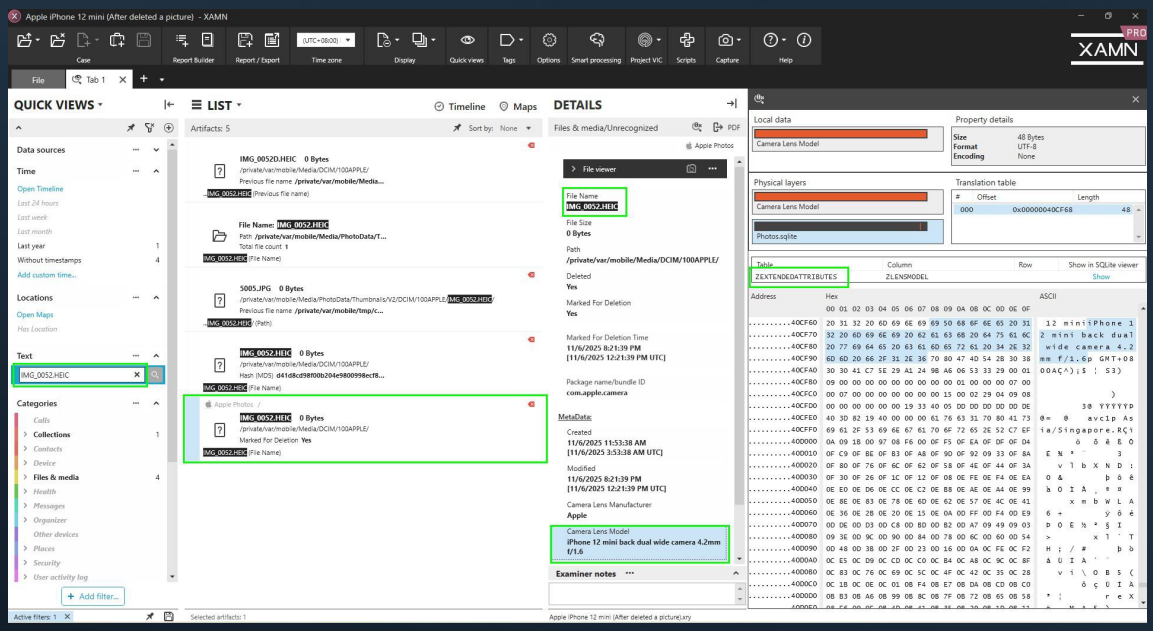
FORENSIC TRACE 03

This recovered ZASSET record provides the third forensic trace of the permanently deleted media.

Importantly, the recovered record contains another valuable piece of information: the original filename. The filename can help establish whether the deleted asset was a photo or video and provides an additional identifier that can be used to search for related artifacts elsewhere within the extraction.

As XRY Pro can recover deleted SQLite data, the identified filename can be used as a search term across the extraction to determine whether any additional records or artifacts reference the same media file.

Even where the original media itself cannot be recovered, locating references to its filename in other databases or artifacts may provide further evidence about the existence and activity associated with the deleted photo or video.



Searching the extraction using the recovered file name produces several additional results.

Significantly, some of these results contain further metadata associated with the deleted media, including information about the camera lens model.

MSAB
Trusted Partner in Digital Forensics

XRY Pro does not simply recover deleted data from an individual SQLite table.

Where relationships can be identified, it can correlate the recovered record with information from other relevant tables, allowing additional metadata associated with the deleted asset to be presented to the examiner.

FORENSIC TRACE 04

This provides the fourth forensic trace.

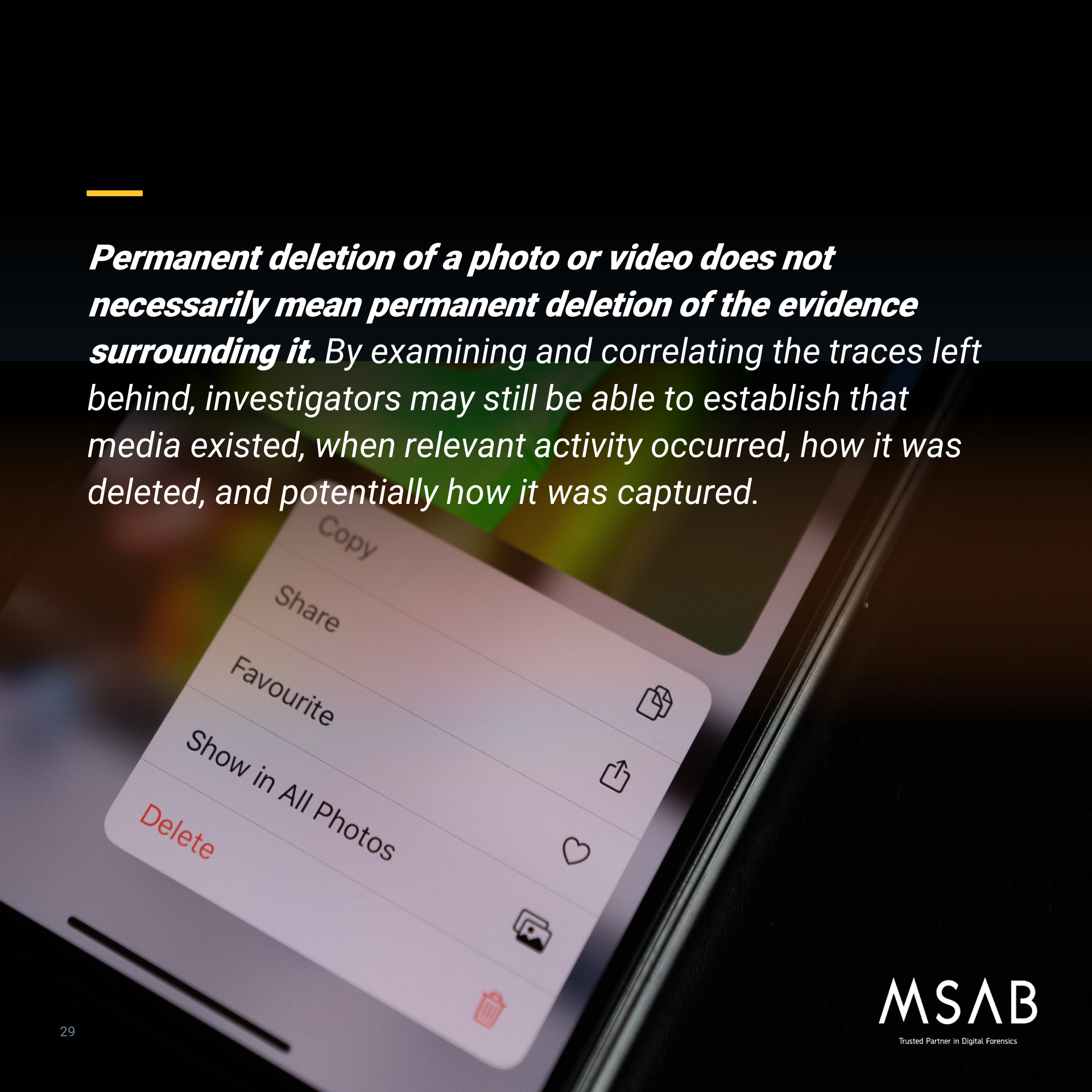
Camera information can be particularly valuable in investigations involving offenses such as upskirting. Depending on the metadata available, the camera or lens information may help establish whether the front-facing or rear-facing camera was used to capture the photo or video.

When considered alongside other recovered artifacts, this can provide important contextual evidence about how the deleted media was captured.

The original media may therefore be permanently deleted and unrecoverable, while metadata associated with its creation can still survive elsewhere within the extracted data.

MSAB
Trusted Partner in Digital Forensics

Permanent deletion of a photo or video does not necessarily mean permanent deletion of the evidence surrounding it. *By examining and correlating the traces left behind, investigators may still be able to establish that media existed, when relevant activity occurred, how it was deleted, and potentially how it was captured.*



MSAB
Trusted Partner in Digital Forensics

A final note on validation

The artefacts, database structures, fields and file locations described in this blog were accurate and observed during testing at the time of writing. Mobile operating systems, applications are constantly evolving, meaning that database schemas, storage locations and available artefacts may change between devices, software versions and extraction methods.

As with any digital forensic examination, never rely on a single artefact, database or forensic tool to support a conclusion. **Always** validate your findings against the underlying source data and, wherever possible, corroborate them using additional artefacts.



Tools parse the evidence.

The examiner validates it.

MSAB

Trusted Partner in Digital Forensics

Our Vision:

Mobile technology changes the world. There are billions of mobile devices such as phones, tablets, GPS units and watches. Even where there are no computers, people use mobiles: in the cities, in the countryside, in deserts and mountains. Wherever we go, whatever we do, we bring our mobile devices.

This is also true for people who break the rules of society. They use mobile devices and that can be a good thing. Mobile technology leaves traces, like digital footprints. These can reveal a hidden world — a fragmented world at times, but a world that points to the truth. It is our task to help our customers search for that truth, in order to make the world a safer place.

Our customers are passionate about their jobs. They truly believe in justice and peace. However, when it comes to mobile technology they meet tough challenges. There is a constant flow of new devices, new operating systems and new apps. Staying ahead of these challenges is absolutely critical for our customers.

MSAB takes responsibility for supporting our customers with the best possible solutions for mobile forensics. This means that we also need to stay ahead of the game; with our products and services, with our vision and energy, with our people and how we do things. We are the pioneers of our industry. Our vision is simple: MSAB – Exceeding the limits of technology to find the truth.

MSAB

Trusted Partner in Digital Forensics