Key Twitter and Facebook Metadata Fields Forensic Investigators Need to be Aware of

Authentication of social media evidence can present significant challenges. This is just one reason why social media data must be properly collected, preserved, searched and produced in a manner consistent with best practices. When social media is collected with a proper chain of custody and all associated metadata is preserved, authenticity can be much easier to establish.

The following are key metadata field examples for individual Twitter items that provide important information to establish authenticity of the tweet, if properly collected and preserved:

Metadata Field:	**Description:**
created_at	UTC timestamp for tweet creation
user_id	The ID of the poster of a tweet
handle	User's screen name (different from user name)
retweet_id	The post ID of a retweet
retweet_user	The username of the user who retweeted
Reply	Indicates if this tweet is a reply
direct_message	Indicates if this tweet is a direct message
Hashtags	List of all hashtags in the tweet
Description	Up to 160 characters describing the tweet
geo_enabled	If the user has enabled geo-location (optional)
Place	Geo-location from where user tweeted from
Coordinates	Geo-location coordinates where tweet sent
in_reply_to_user_id	unique id for the user that replied
profile_image_url	location to a user's avatar file
recipient_id	unique id of direct message recipient
recipient_screen_name	display name of direct message sender
screen_name	display name for a user
sender_id	unique id of direct message sender

Source	application used to Tweet or direct message(i.e., from an iPhone or specific Twitter app)
time_zone	a user's time zone
utc_offset	time between user's time zone and UTC time
follow_request_sent	Indicates request to follow the user
Truncated	If the post is truncated due to excessive length

Any one or combination of these fields can be key circumstantial data to authenticate a single or group of social media items. US Federal Rule of Evidence 901(b)(4) provides that a party can authenticate electronically stored information ("ESI") with circumstantial evidence that reflects the "contents, substance, internal patterns, or other distinctive characteristics" of the evidence. Many cases have applied Rule 901(b)(4) to metadata associated with emails and other ESI. Facebook and LinkedIn items have their own unique, but generally comparable metadata fields.

Following are some key metadata fields for each Facebook entry. These fields provide important evidence, investigation context and circumstantial evidence to establish authenticity, if properly collected and preserved.

Metadata Field	Description
Uri	Unified resource identifier of the subject item
fb_item_type	Identifies item as Wallitem, Newsitem, Photo, etc.
parent_itemnum	Parent item number-sub item are tracked to parent
thread_id	Unique identifier of a message thread
recipients	All recipients of a message listed by name
recipients_id	All recipients of a message listed by user id.
album_id	Unique id number of a photo or video item
post_id	Unique id number of a wall post
application	application used to post to Facebook (i.e, from an iPhone or social media client)
user_img	url where user profile image is located
user_id	Unique id of the poster/author of a Facebook item
account_id	unique id of a users account
user_name	display name of poster/author of a Facebook item
created_time	When a post or message was created
updated_time	When a post or message was revised/updated

To	Name of user whom a wall post is directed to
to_id	Unique id of user whom a wall post is directed to
Link	url of any included links
comments_num	Number of comments to a post
picture_url	url where picture is located
