

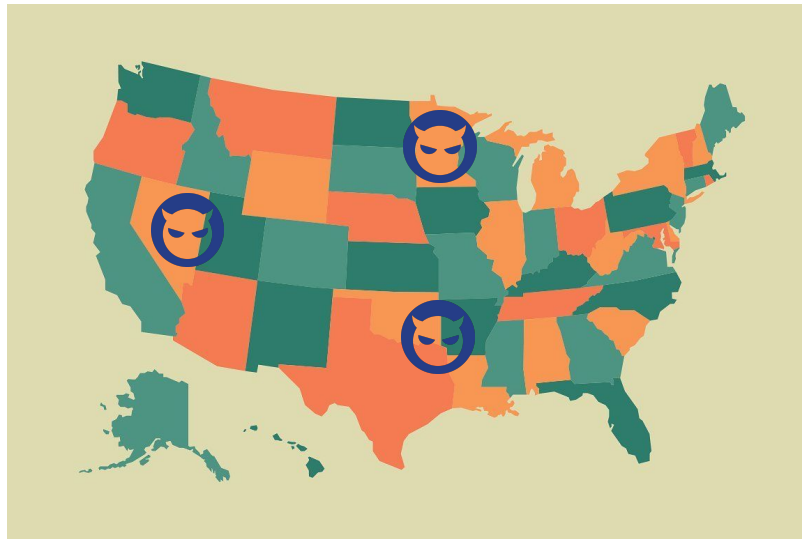
Digital Forensic Analysis of Facebook Marketplace Chat Messages and Facebook Notifications

Jonathan Chao

Intelligence and Cyber Operations, BA

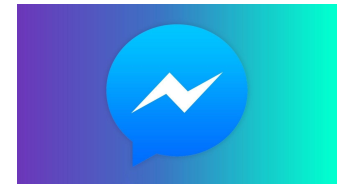
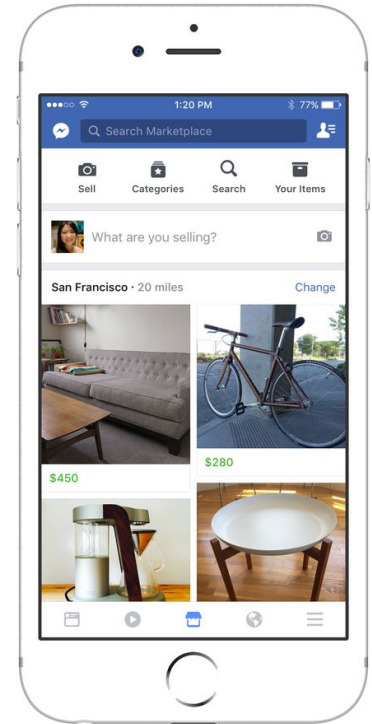
An Example Scenario...

- Criminal organization (possibly stationed internationally)
- Several unknown operatives spread out
- Need centralized way to reach out and contact



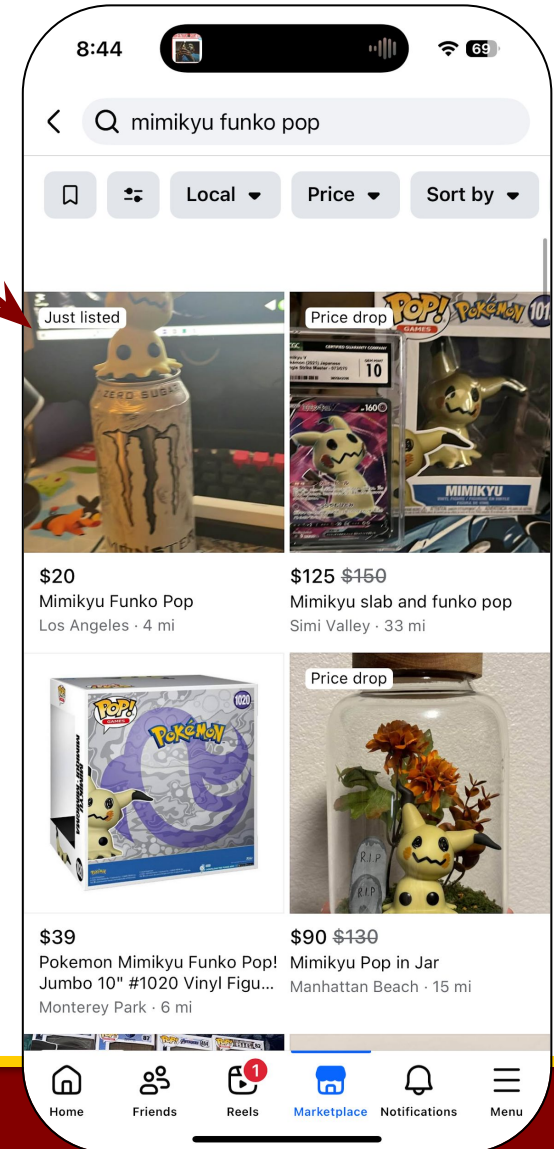
A potential solution?

- Facebook Marketplace/ Marketplace apps in general
- Fake listings get little traffic
- These listings draw little attention but can be seen from all over
- Chat logs are inconspicuous, and encrypted through facebook
- Less clear than traditional communications (messenger)



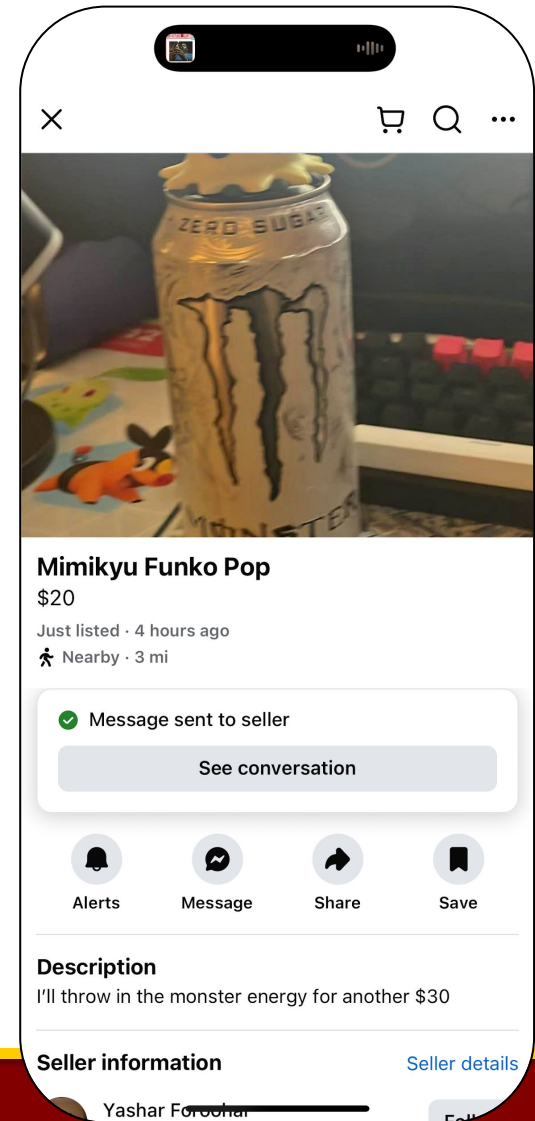
Example Interaction

- FB Marketplace listing for item few people would search for
- Burner facebook account on iOS device reaches out for contact
- Think niche and off-putting!



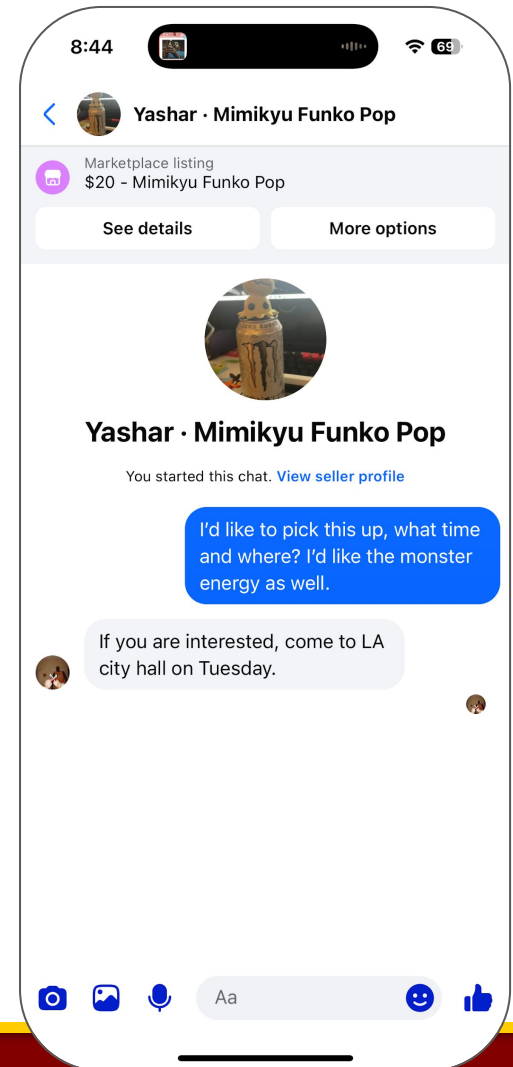
Example Interaction

- FB Marketplace listing for item few people would search for
- Burner facebook account on iOS device reaches out for contact
- Think niche and off-putting!



Example Interaction cont.

- Code could be used, chat logs provide direct communication
- More than 1 billion monthly Marketplace users (last official Meta figure, 2021)
- Would a message like this stand out in an investigation?



Artifact 1: User Creation Date

- com.facebook.Facebook plist
- key fb-msys-<USER ACCOUNT ID>.db_first_created_timestamp → Unix Epoch time
- Establish connection → 61583507053152
- Sunday, November 16, 2025 1:54:13 AM.

com.facebook.Facebook.plist

key	Type	Value
Root	dict	(205 items)
FBAppOpenAfterFreshInstallKey	boolean	true
kCaaLoxAutoLogin	boolean	
fb-msys-61583507053152.db_first_created_timestamp	number	1763258053

Artifact 2: Notification Files

- Notifications are cached locally in an AppDomainGroup folder directory, as a sequence of 99 to 100 byte files
- AppDomainGroup-group.com.facebook.Facebook/PushNotifClientSyncDisplayedDirectory/*

 U1U645000f923455G3802870fda60G6450059283727G79+1764547693296334+122102122401116901+1764717665864086

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	55	31	55	36	34	35	30	30	30	66	39	32	33	34	35	35	U1U645000f923455
00000010	47	33	38	30	32	38	37	30	66	64	61	36	30	47	36	34	G3802870fda60G64
00000020	35	30	30	35	39	32	38	33	37	32	37	47	37	39	2B	31	50059283727G79+1
00000030	37	36	34	35	34	37	36	39	33	32	39	36	33	33	34	2B	764547693296334+
00000040	31	32	32	31	30	32	31	32	32	34	30	31	31	31	36	39	1221021224011169
00000050	30	31	2B	31	37	36	34	37	31	37	36	36	35	38	36	34	01+1764717665864
00000060	30	38	36														086

Parsing Notification Files

Our String:

U1U645000f923455G3802870fda60G6450059283727G79+1764
547693296334+122102122401116901+1764717665864086

Compare our plaintext with the next available notification file, and reference existing information to deduce the general shape of Facebook's storage system.

Next String:

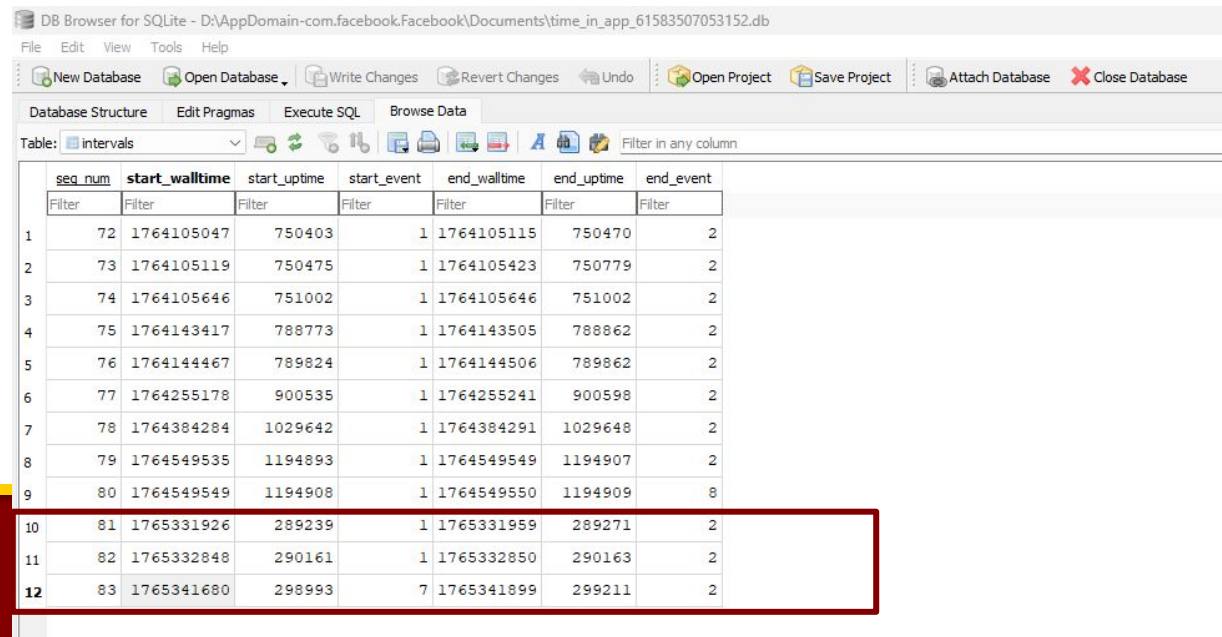
U1U644fbc10e8c9aG3802870fda60G644fc0aa48f6cG114+1764
374430423936+122102122401116901+1764699185060117

Parsing Notification Files

Character Set	Rough Meaning
U1U	user-related notification
645000f923455	Primary ID
3802870fda60	user ID
6450059283727	Secondary ID
79	notification type
1764547693296334	Unix time → Monday, December 1, 2025 12:08:13.296 AM
12210212240111690 1	Tertiary ID
1764717665864086	Unix time (Creation date of file) → Tuesday, December 2, 2025 11:21:05.864 PM

Artifact 3: time_in_app DB

- Figure: SQL file showing a sequence of user activity, with start and end times displayed in Unix Epoch Time.
- AppDomain-com.facebook.Facebook/Documents/time_in_app_<USER ACCOUNT ID>.db



The screenshot shows the DB Browser for SQLite interface. The title bar indicates the database path: D:\AppDomain-com.facebook.Facebook\Documents\time_in_app_61583507053152.db. The table 'intervals' is selected, and its data is displayed in a grid. The table has seven columns: seq_num, start_walltime, start_uptime, start_event, end_walltime, end_uptime, and end_event. The data shows a sequence of 12 intervals, with the last interval (seq_num 83) highlighted by a red box.

	seq_num	start_walltime	start_uptime	start_event	end_walltime	end_uptime	end_event
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	72	1764105047	750403	1	1764105115	750470	2
2	73	1764105119	750475	1	1764105423	750779	2
3	74	1764105646	751002	1	1764105646	751002	2
4	75	1764143417	788773	1	1764143505	788862	2
5	76	1764144467	789824	1	1764144506	789862	2
6	77	1764255178	900535	1	1764255241	900598	2
7	78	1764384284	1029642	1	1764384291	1029648	2
8	79	1764549535	1194893	1	1764549549	1194907	2
9	80	1764549549	1194908	1	1764549550	1194909	8
10	81	1765331926	289239	1	1765331959	289271	2
11	82	1765332848	290161	1	1765332850	290163	2
12	83	1765341680	298993	7	1765341899	299211	2

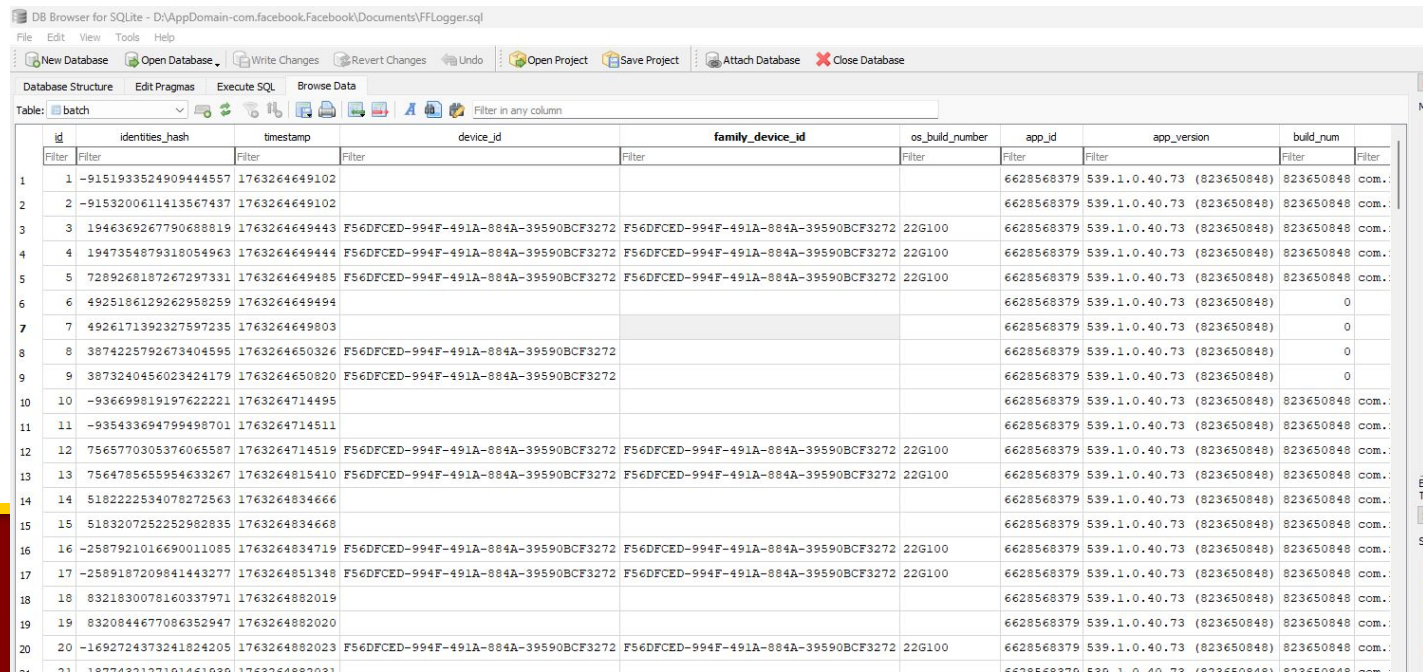
Parsing the time_in_app File

- user with id 61583507053152 had a session from 1765341680 to 1765341899
- This corresponds to Wednesday, December 10, 2025 4:41:20 AM to Wednesday, December 10, 2025 4:44:59 AM

10	81	1765331926	289239	1	1765331959	289271	2
11	82	1765332848	290161	1	1765332850	290163	2
12	83	1765341680	298993	7	1765341899	299211	2

Artifact 4: FFLogger Files

- Figure: FFLogger SQL file, which updates regularly and maintains continuity for the Facebook backend. It tracks app version, device hardware ID, build number, and hashes the state of the app for logging.
- File Location:
AppDomain-com.facebook.Facebook/Documents/FFLogger.sql



The screenshot shows a SQLite database browser interface with the following table structure:

id	identities_hash	timestamp	device_id	family_device_id	os_build_number	app_id	app_version	build_num
1	-9151933524909444557	1763264649102				6628568379	539.1.0.40.73 (823650848)	823650848
2	-9153200611413567437	1763264649102				6628568379	539.1.0.40.73 (823650848)	823650848
3	1946369267790688819	1763264649443	F56DFCED-994F-491A-884A-39590BCF3272	F56DFCED-994F-491A-884A-39590BCF3272	22G100	6628568379	539.1.0.40.73 (823650848)	823650848
4	1947354879318054963	1763264649444	F56DFCED-994F-491A-884A-39590BCF3272	F56DFCED-994F-491A-884A-39590BCF3272	22G100	6628568379	539.1.0.40.73 (823650848)	823650848
5	7289268187267297331	1763264649485	F56DFCED-994F-491A-884A-39590BCF3272	F56DFCED-994F-491A-884A-39590BCF3272	22G100	6628568379	539.1.0.40.73 (823650848)	823650848
6	4925186129262958259	1763264649494				6628568379	539.1.0.40.73 (823650848)	0
7	4926171392327597235	1763264649803				6628568379	539.1.0.40.73 (823650848)	0
8	3874225792673404595	1763264650326	F56DFCED-994F-491A-884A-39590BCF3272			6628568379	539.1.0.40.73 (823650848)	0
9	3873240456023424179	1763264650820	F56DFCED-994F-491A-884A-39590BCF3272			6628568379	539.1.0.40.73 (823650848)	0
10	-936699819197622221	1763264714495				6628568379	539.1.0.40.73 (823650848)	823650848
11	-935433694799498701	1763264714511				6628568379	539.1.0.40.73 (823650848)	823650848
12	7565770305376065587	1763264714519	F56DFCED-994F-491A-884A-39590BCF3272	F56DFCED-994F-491A-884A-39590BCF3272	22G100	6628568379	539.1.0.40.73 (823650848)	823650848
13	7564785655954633267	1763264815410	F56DFCED-994F-491A-884A-39590BCF3272	F56DFCED-994F-491A-884A-39590BCF3272	22G100	6628568379	539.1.0.40.73 (823650848)	823650848
14	5182222534078272563	1763264834666				6628568379	539.1.0.40.73 (823650848)	823650848
15	5183207252252982835	1763264834668				6628568379	539.1.0.40.73 (823650848)	823650848
16	-2587921016690011085	1763264834719	F56DFCED-994F-491A-884A-39590BCF3272	F56DFCED-994F-491A-884A-39590BCF3272	22G100	6628568379	539.1.0.40.73 (823650848)	823650848
17	-2589187209841443277	1763264851348	F56DFCED-994F-491A-884A-39590BCF3272	F56DFCED-994F-491A-884A-39590BCF3272	22G100	6628568379	539.1.0.40.73 (823650848)	823650848
18	8321830078160337971	1763264882019				6628568379	539.1.0.40.73 (823650848)	823650848
19	8320844677086352947	1763264882020				6628568379	539.1.0.40.73 (823650848)	823650848
20	-1692724373241824205	1763264882023	F56DFCED-994F-491A-884A-39590BCF3272	F56DFCED-994F-491A-884A-39590BCF3272	22G100	6628568379	539.1.0.40.73 (823650848)	823650848
21	1877432127181461838	1763264882031				6628568379	539.1.0.40.73 (823650848)	823650848

Artifact 5: Marketplace Item Notifs

- Unique to Facebook Marketplace is the JSON format in which listings are displayed. These listings include a vast array of information and are maintained long after initial viewing.

```
object ▶ items ▶ timeline ▶ item ▶ rows ▶ 3 ▶ reaction_icons undefined
▼ 3 {9}
  __typename : NotifPageWidgetBasicMediaCardRow
  cache_id : 8972924945716811773
  ▼ overlay_config {2}
    presentation : HORIZONTAL
    alignment : BOTTOM_LEADING
  ▼ reaction_icons [0]
    (empty array)
  tracking : {"extra_row_data":{"content_id":"25143233622035581","NotifPageWidgetBasicMediaCardRow","pos":2,"pg":6}}
  url : fb://marketplace/?
    hoistedStoryIDs=%5B%22UzpfSTeYMTU5MzQ0NzQ6Vks6MjUyNDk5NTQzMzEyOT
    ata=%7B%22productItemID%22%3A%22886320503819967%22%2C%22title%22
    73+Fender+Stratocaster.+It+has+the+original+tremolo+arm+and+the+
    22%3A1764612901%2C%22price%22%3A%22%246%2C500%22%2C%22groupID%22
    nly%29%22%2C%22isSold%22%3Afalse%2C%22isBasicListing%22%3Afalse%
    %22%3A%7B%22uri%22%3A%22https%3A%5C%2F%5C%2Fcontent-lax3-2.xx.f
    6%5C%2F593466093_10239771694209756_8521763610120346731_n.jpg%3F%
    7%26_nc_sid%3Daa7b47%26_nc_ohc%3DZ6ioUWKS_Q4Q7kNvwFpH80-%26_nc_c
    yH0omtBUwYPBL0EeEicIrSPWfycoT9z2a8CR33PZVeNzOLATRMvI3KmXOTv%26_
    2.xx%26oh%3D00_AfkbJDADdRk6vSXHeuy4qfvBZE6dJxpke5w4dxy8tSg1-
    A%26oe%3D69352104%22%2C%22width%22%3A810%2C%22height%22%3A540%7C
    content-lax7-1.xx.fbcdn.net%5C%2Fv%5C%2Ft39.30808-6%5C%2F5914071
```

Field	Value	Meaning
productItemID	886320503819967	Unique listing ID for the item
title	1973 Fender Stratocaster	Listing title
description	This is an all original vintage 1973 Fender Stratocaster. It has the original tremolo arm and the rare "ashtray" bridge cover. This is as close to min...	Item description (truncated in payload)
creationTimeInSeconds	1764612901	Unix Epoch Timestamp from Monday, December 1, 2025 6:15:01 PM
price	\$6,500	Display price
listingPriceAmount	6500	Numeric price
listingPriceAmountRaw	650000	Raw integer representation (price × 100)
listingPriceCurrency	USD	Currency
groupID	1573733789340857	Facebook group ID where listed
groupName		Group name
isSold	FALSE	Item not marked sold
isBasicListing	FALSE	Indicates full listing
isViewerSeller	FALSE	Viewer is not the seller
images	Multiple image objects with IDs and URIs	Photos
storyID	UzpfSTEyMTU5MzQ0NzQ6Vks6MjUyNDk5NTQzMzEyOTIxMzc=	Encoded story identifier
tracking.mf_story_key	25143233622035581	Tracking key for commerce ranking
profileImageURI	Facebook CDN link	Seller's profile picture
name		Seller's name
profileID		Seller's Facebook ID
profileTypeName	User	Seller account type
gender	2	Gender code (likely male)
location		Seller's location
categoryID	676772489112490	Marketplace category ID
buyerCTAType	INLINE_MESSAGING	Buyer call-to-action type
priceType	Fixed	Fixed-price listing
footer	BUY_SELL_GROUP_RELATED_ITEMS	Footer context

Parsing the JSON

Kidding!

title	1973 Fender Stratocaster	Listing title
description	This is an all original vintage 1973 Fender Stratocaster. It has the original tremolo arm and the rare "ashtray" bridge cover. This is as close to min...	Item description (truncated in payload)
creationTimeInSeconds	1764612901	Unix Epoch Timestamp from Monday, December 1, 2025 6:15:01 PM
price	\$6,500	Display price
profileID		Seller's Facebook ID
location		Seller's location

AppDomainGroup-group.com.facebook.Facebook/NotificationsWidgetV2.timeline.1.json

E2EE and Facebook

- End-to-End Encryption
- FB rolled out late, but in 2023 was rare for no-phone number sign up E2EE platform
- "Some products don't currently support end-to-end encryption, such as chats with businesses or accounts using business messaging tools, Marketplace chats and others." (2024, Facebook)
- App Domain Group, Messages Encrypted

What have we learned?

- A potential way to organize crimes
- Facebook has selective E2EE
- All your Marketplace listing and notifications are kept forever (or a long time, and location data IS included)
- Meta keeps track of when you log in and out
- We can use all these artifacts for a timeline, showing temporal correlation