DiefVIP1

**Preliminary Investigative Summary**

I conducted a review of the three individuals identified in the subpoena, along with the associated alias email address. Based on the available data, the only countries with a potential nexus to these entities are China (linked to IDs submitted to OKX), Laos (via VPN usage), and Russia (identified through open-source intelligence).

It is plausible that individuals—potentially operating from a separate jurisdiction—acquired fraudulent Chinese identification documents through online marketplaces in order to open accounts on OKX and engage in digital asset transactions.

At this stage, without additional context on the broader fraud or scam, there is limited further research that can be conducted. The investigation is currently pending additional transaction data from other exchanges named in the subpoena. To advance this analysis, further tools—such as comprehensive identity verification reports—will be necessary to confirm the legitimacy and origin of the individuals or entities in question.

Names from Subpoena:

**FENG HUORONG**

ID used to open an account highly indicative of a fake Chinese ID most likely purchased online.

Similar profile picture from a LinkedIn account - possible match, medium confidence - Job Role is Huatai Century Holdings Limited - Deputy General Manager - <https://www.linkedin.com/in/%E8%80%80%E4%B8%9C-%E6%9D%A8-39a97317a/?originalSubdomain=cn>

Email - [yezi85460@gmail.com](mailto:yezi85460@gmail.com)

Sherlock (Social Media Username Search) Results:

* <https://www.rusfootball.info/user/yezi85460@gmail.com/> (Russian Football)
* <https://music.yandex/users/yezi85460@gmail.com/playlists> (Russian site)

Total Websites Username Detected On : 22. Removed links that resulted in 404 error

Most Common Wallets

#TGwY3p4sNpaVo7oEXGd9ipg1CwCuDBV19h

Recent Activity (UTC) 2023-04-17 11:16:54

Created on (UTC) 2022-05-12 08:29:00

Review - mainly tx with OKX Hot Wallet and various Deposit addresses

Small interactions with Deepcoin (investment platform)

#TWhpcJ86rBwDUW82X7sybVek6pvYFDB58Q

Recent Activity (UTC) 2023-10-17 11:01:45

Created on (UTC) 2023-03-31 09:56:21

#0x0f40Bc8345cFc8641627172b4eC402cd5Aa3Cd97 (Recent activity)

Recent Activity (UTC) Apr-30-2025 05:40:47 PM UTC

Created on (UTC) May-17-2023 12:05:47 PM UTC

Mostly received funds from OKX, and did swaps on Uniswap

Tx for Subpoena:

1. Deposits from 0x0f40Bc to Gate.io Deposit Address (0xc0DfA6B1a5ea0Dab9FB3803dA789EfD1B7aEc9ec)
   1. Tx Hash - 0x5cfcfebc4fc67ccdcff53fbfb5239613ddcd659f9e117598bd657e260c4586d5
2. Deposits from 0x0f40Bc to Kraken Deposit Address (0xE29c0D06810EcAf8f85edA82545f3a7DcFE9E3E1)
   1. Tx Hash - 0x6e1ae1a00fdc38a7b554932ac5b621231cfb510dbce33127b5458923de38c70a

**LU JUNLIN**

No photo ID used to open an account. Highly indicative of a fake Chinese ID most likely purchased online.  
Email - [247884267@qq.com](mailto:247884267@qq.com)

Sherlock (Social Media Username Search) Results:

* <https://www.rusfootball.info/user/247884267@qq.com/> (Russian Football)
* https://giphy.com/247884267@qq.com
* https://hackerearth.com/@247884267@qq.com
* https://cavalier.hudsonrock.com/api/json/v2/osint-tools/search-by-username?username=247884267@qq.com
* https://www.reddit.com/user/247884267@qq.com
* https://slideshare.net/247884267@qq.com
* https://trello.com/247884267@qq.com
* https://hosted.weblate.org/user/247884267@qq.com/
* https://music.yandex/users/247884267@qq.com/playlists
* https://chaos.social/@247884267@qq.com
* https://mastodon.cloud/@247884267@qq.com
* https://mastodon.social/@247884267@qq.com
* https://mastodon.xyz/@247884267@qq.com
* https://mstdn.io/@247884267@qq.com
* https://247884267@qq.com.omg.lol
* https://www.opennet.ru/~247884267@qq.com
* https://php.ru/forum/members/?username=247884267@qq.com
* https://social.tchncs.de/@247884267@qq.com
* https://www.threads.net/@247884267@qq.com

Total Websites Username Detected On : 24

Most Common Wallets

#TA1NyPWjruSfKLyDcH5S7Uj2C5Mj1raFKf

Recent Activity (UTC) 2025-01-18 15:22:24

Created on (UTC) 2023-05-23 10:27:27

Transactions with Binance

#TAhGc6ZuYxPxej9rfcX9oEvEzR7SQPjW3T

Recent Activity (UTC) 2025-05-30 12:40:06

Created on (UTC) 2022-11-24 02:53:36

Transactions with Binance

#TAFhTqAQyHVxw1bhVf4WxtF7X6MwSmPDWg (OKX label)

Recent Activity (UTC) 2024-08-10 06:41:24

Created on (UTC) 2022-08-09 13:19:21

Tx activity indicates selling of USDT for fiat on OKX

#TAj9drKdfYeJfGynzGTNqeMbkfLBipquxp

Recent Activity (UTC) 2024-01-20 05:20:18

Created on (UTC) 2023-08-16 19:41:21

Moved USDT and TRX to other tron addresses and OKX

#TAViKdErjhfechR6N3k2SNW77FuSUAV4pQ

Recent Activity (UTC) 2025-05-16 01:56:51

Created on (UTC) 2023-11-01 06:40:00

Deposit $1k USDT to Bybit address (TGfapmmAF223honB4wXTtcZyaBBGQAUBNv)

Receive from HitBTC Hot Wallet

#TB2TKHJQqrXYXMDWZzegkiYoadskPbhWwd

Recent Activity (UTC) 2025-04-25 17:57:21

Created on (UTC) 2023-07-16 20:04:15

Tx activity indicates selling of USDT for fiat on OKX

#TBhWiY7LZBsxhS6WdCgqdUnbFTdQhLc3c5

Recent Activity (UTC) 2024-08-02 08:07:03

Created on (UTC) 2024-07-02 02:20:30

Received several tx from Binance Hot Wallets

#TBQS1pvwCLEkYuz5t9ivtux6mgcfgZ5AZP

Recent Activity (UTC) 2025-05-30 05:38:57

Created on (UTC) 2023-09-03 18:18:36

Tx activity indicates address funds use move USDT and TRX around on TRON network

Deposits to Cryptomus Deposit addresses (2)

#TC1w4WMHX3zL1Gzu1NCnN3CCWWgPtnHqDH

Recent Activity (UTC) 2025-05-29 18:07:30

Created on (UTC) 2023-07-01 18:18:12

Received USDT from Binance Hot Wallet

Tx for Subpoena:

1. Deposits from TAViKd to Bybit address (TGfapmmAF223honB4wXTtcZyaBBGQAUBNv)
   1. Tx Hash - c3c68ac36059652b9157b58615b4dc2c4ae5327e6997ffcd08040d9f873a096
2. Deposit from TBQS1p to Cryptomus address (TK1TexmetyWbJjEDuLBCaYDxnr9nJeLqyy)
   1. Tx Hash - a458709da981ab3bdc9291111b3e72a14e70bb76f7d368772e99711a8b7e1bdb
3. Deposit from TBQS1p to Cryptomus address (TX1zPQvvw6nBVY1D68RZtzja8kk5jqAwpc)
   1. Tx Hash - ac12792ff92193e34b6c0683ec80ea7de0d54d49c69916f02eb974789d763f7f
4. [Can gather tx received from Binance, but best to prioritize deposits to exchanges.]

**SU XIAOHONG**

ID used to open an account highly indicative of a fake Chinese ID most likely purchased online.  
Email - [247884267@qq.com](mailto:247884267@qq.com)

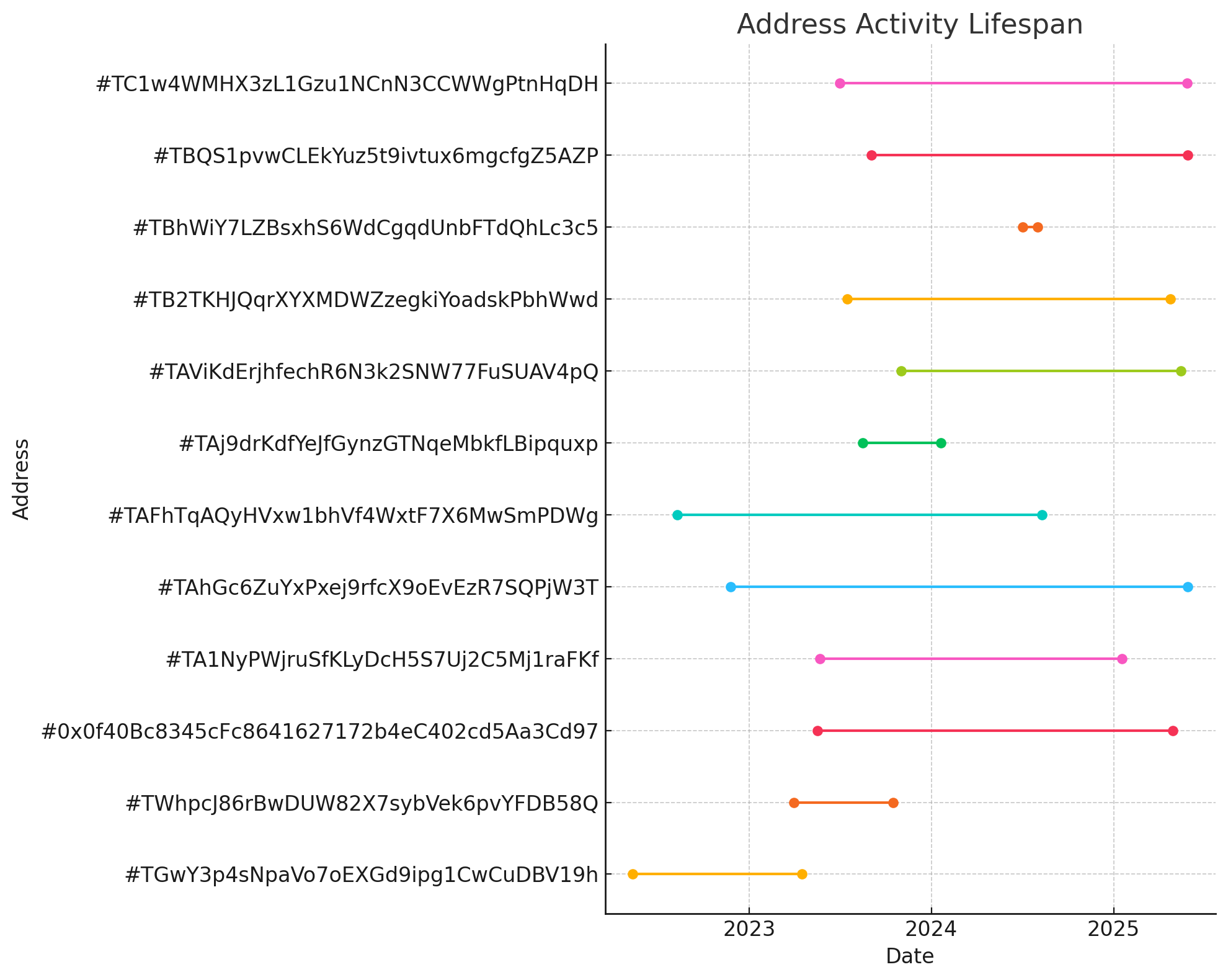
Sherlock (Social Media Username Search) Results:

* <https://www.rusfootball.info/user/247884267@qq.com/> (Russian Football)

Total Websites Username Detected On : 24

No address listed.

Address Activity Over Time:



[**mengzhi2005@gmail.com**](mailto:mengzhi2005@gmail.com)

Sherlock (Social Media Username Search) Results:

* <https://freelance.habr.com/freelancers/Mengzhi2005> (Russian freelance hub)
* https://gitlab.gnome.org/Mengzhi2005
* <https://hackerearth.com/@Mengzhi2005> (Hacker Forum)
* https://news.ycombinator.com/user?id=Mengzhi2005
* https://www.kaskus.co.id/@Mengzhi2005
* <https://www.smule.com/Mengzhi2005> (Music sharing site)
* https://torrentgalaxy.to/profile/Mengzhi2005
* https://x.com/Mengzhi2005
* https://hosted.weblate.org/user/Mengzhi2005/
* https://music.yandex/users/Mengzhi2005/playlists
* https://php.ru/forum/members/?username=Mengzhi2005
* https://www.threads.net/@Mengzhi2005

Total Websites Username Detected On : 12