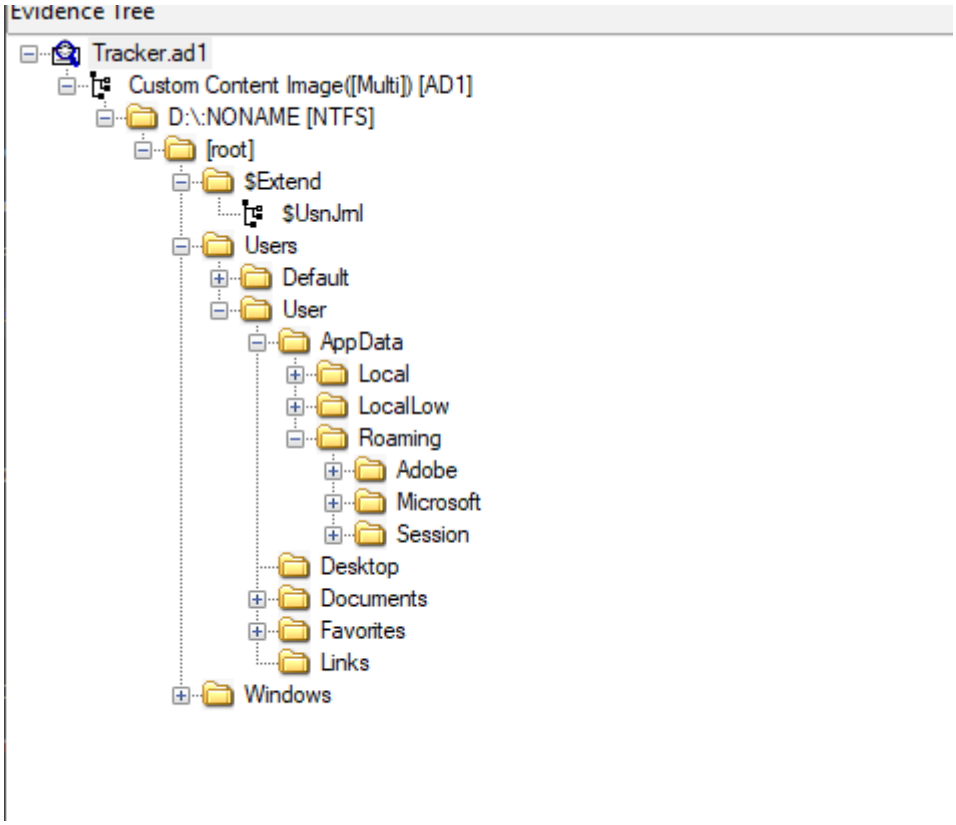
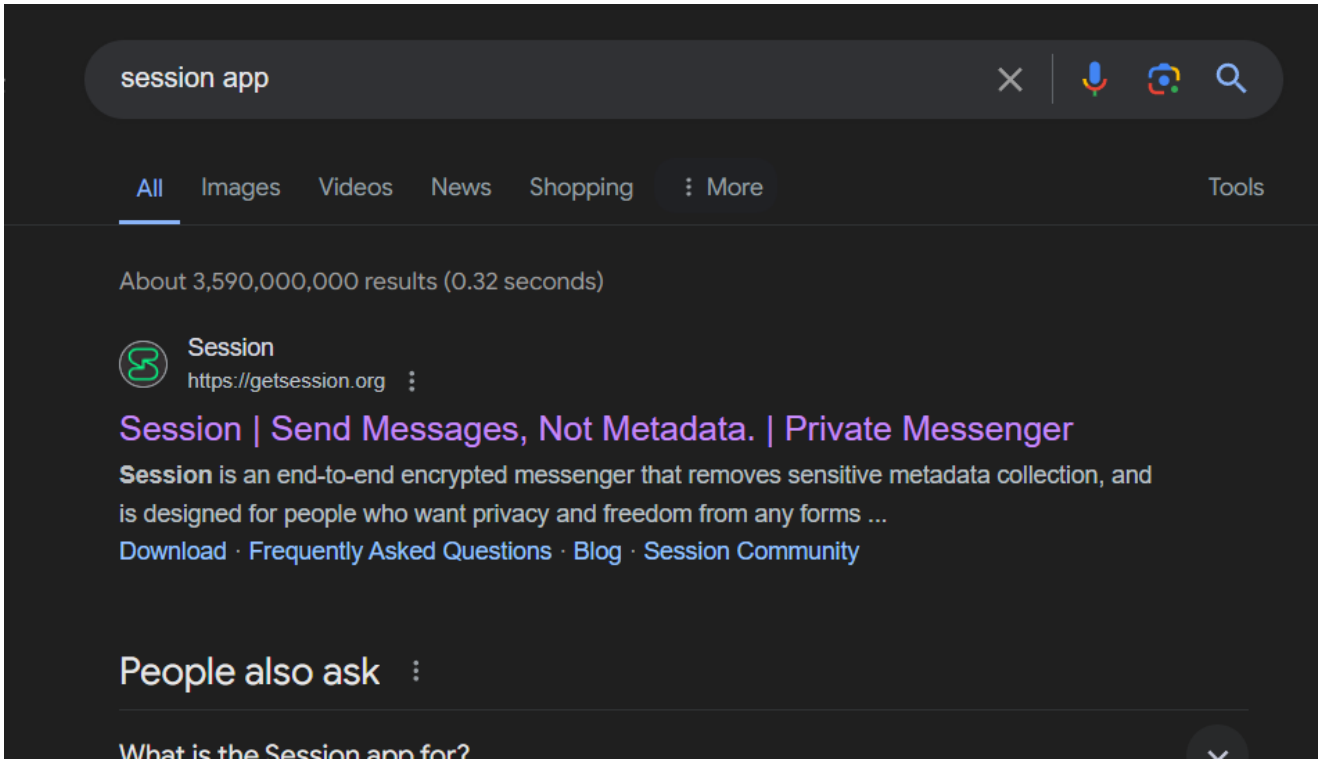
This is a DFIR challenge, we were given a AD1 file. The question ask for SNS ID of the drug dealer The first thing we need to look for, SNS app.



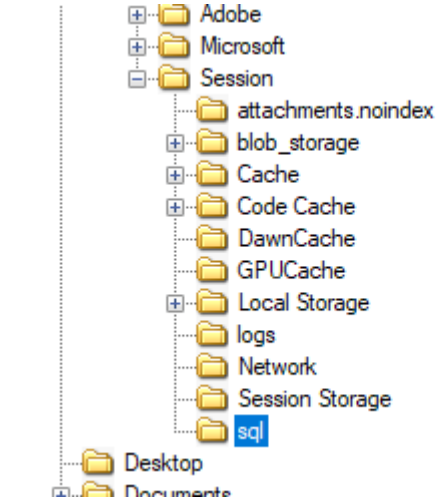
Navigating FTK Imager, we can see that theres ADOBE (a pdf reader), Microsoft (definitely not SNS), and Session. First time i heard session, lets do a quick googling.

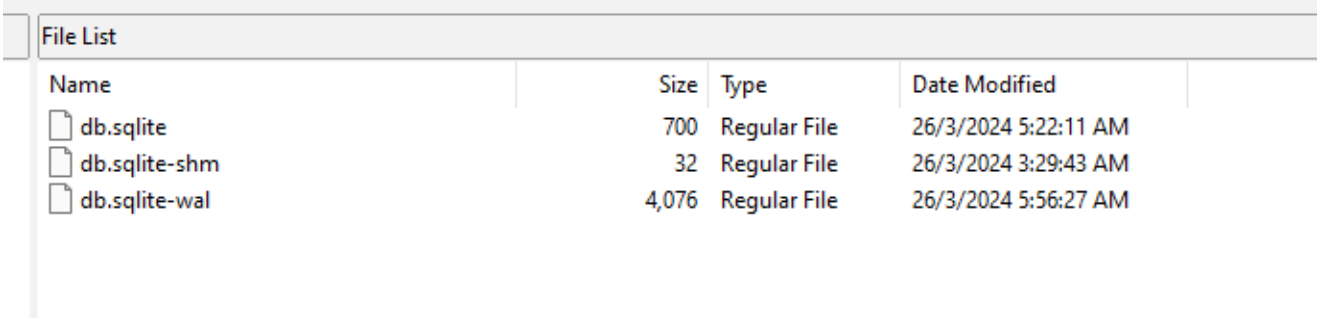


yesss, a private messenger, something a drug dealer would love.

so we can conclude that SNS app is SESSION

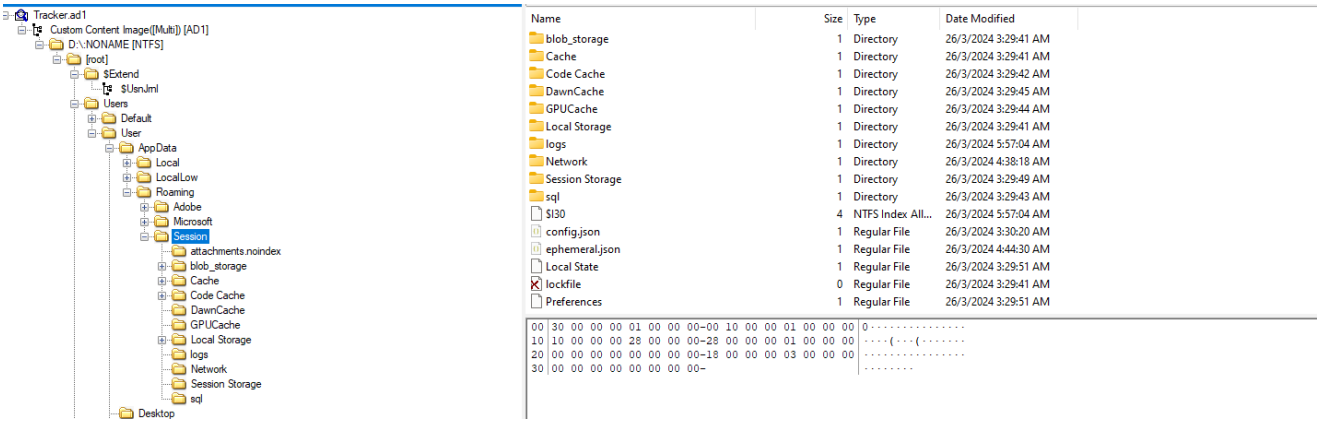
moving on into finding the ID.

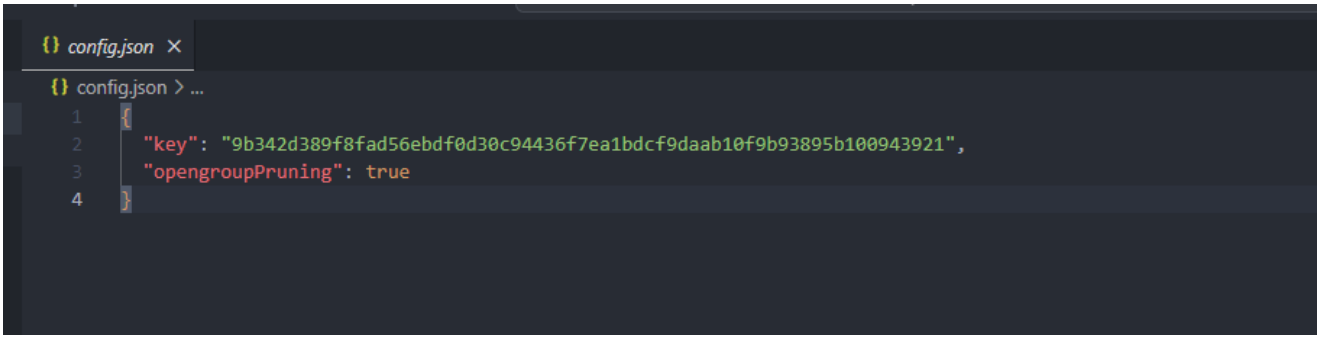




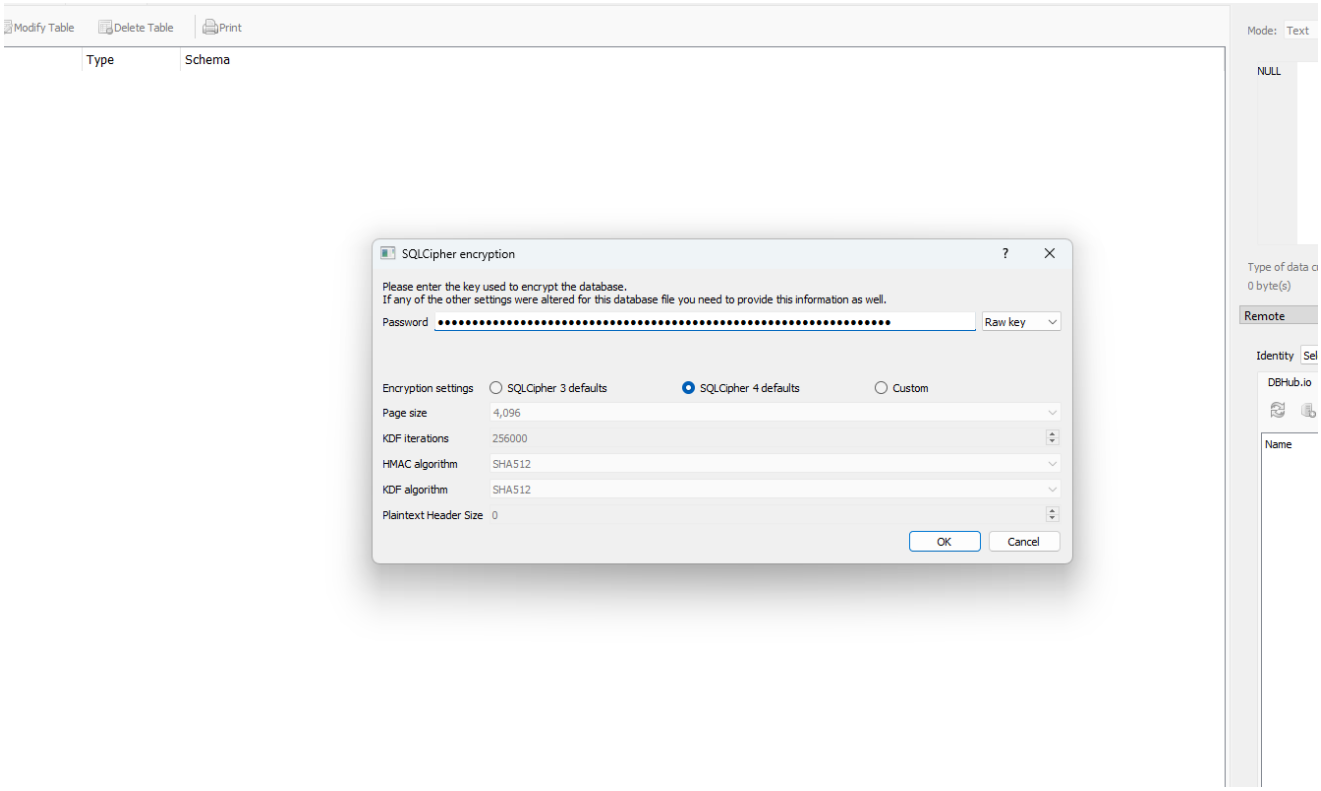
Found sqlite files.

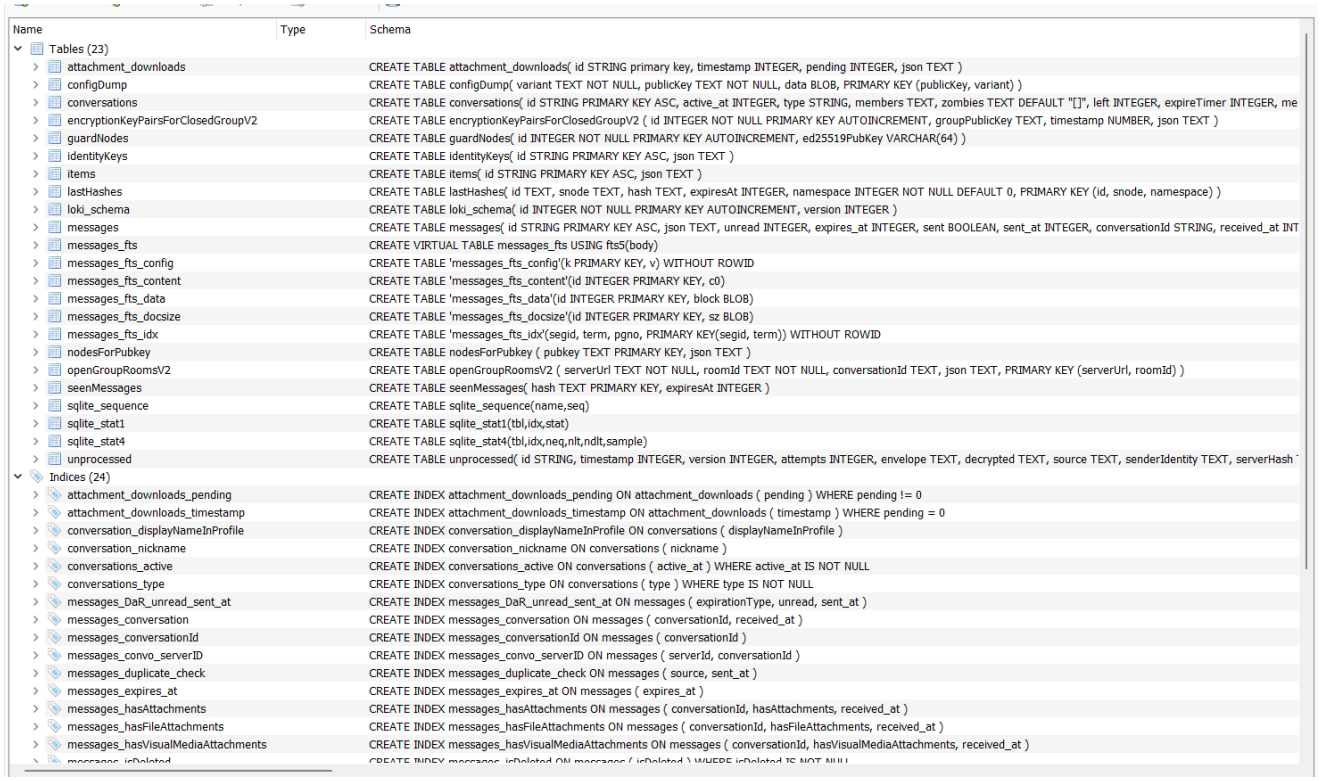
When tried to open it normally, it wont open thus I suspect there is some type of encryption. Encryption means there is a 'key'.



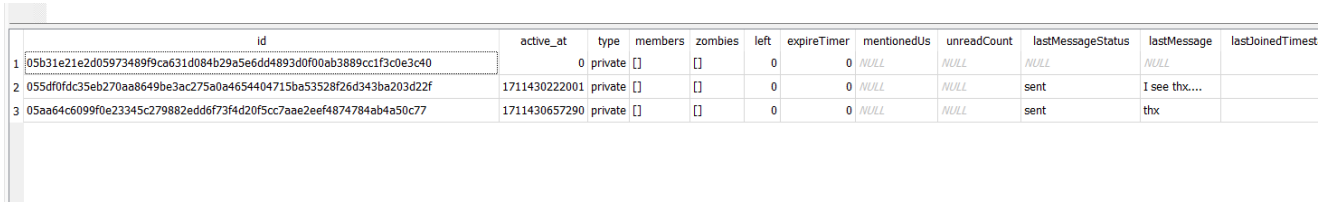


when we open the config.json we found the key. to open the sqlite3 file, I will be using DB Browser (SQLCipher) for this.



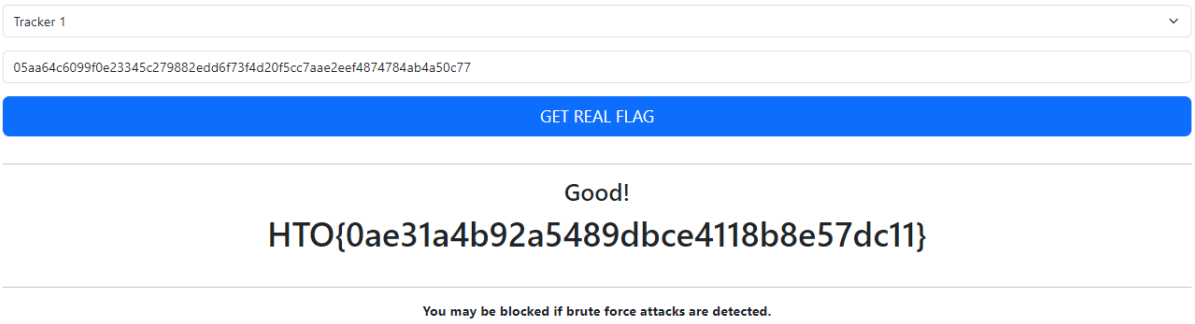


we got into the database. now time to find the id, conversations table seems like it.



	id	active_at	type	members	zombies	left	expireTimer	mentionedUs	unreadCount	lastMessageStatus	lastMessage	lastJoinedTimest
1	05b31e21e2d05973489f9ca631d084b29a5e6dd4893d0f00ab3889cc1f3c0e3c40	0	private	[]	[]	0	0	NULL	NULL	NULL	NULL	
2	055df0fdc35eb270aa8649be3ac275a0a4654404715ba53528f26d343ba203d22f	1711430222001	private	[]	[]	0	0	NULL	NULL	sent	I see thx....	
3	05aa64c6099f0e23345c279882edd6f73f4d20f5cc7aae2eef4874784ab4a50c77	1711430657290	private	[]	[]	0	0	NULL	NULL	sent	thx	

now we see 2 IDs with last message. If we think about it carefully, the id `05aa64c6099f0e23345c279882edd6f73f4d20f5cc7aae2eef4874784ab4a50c77` is the one.



`HTO{0ae31a4b92a5489dbce4118b8e57dc11}`