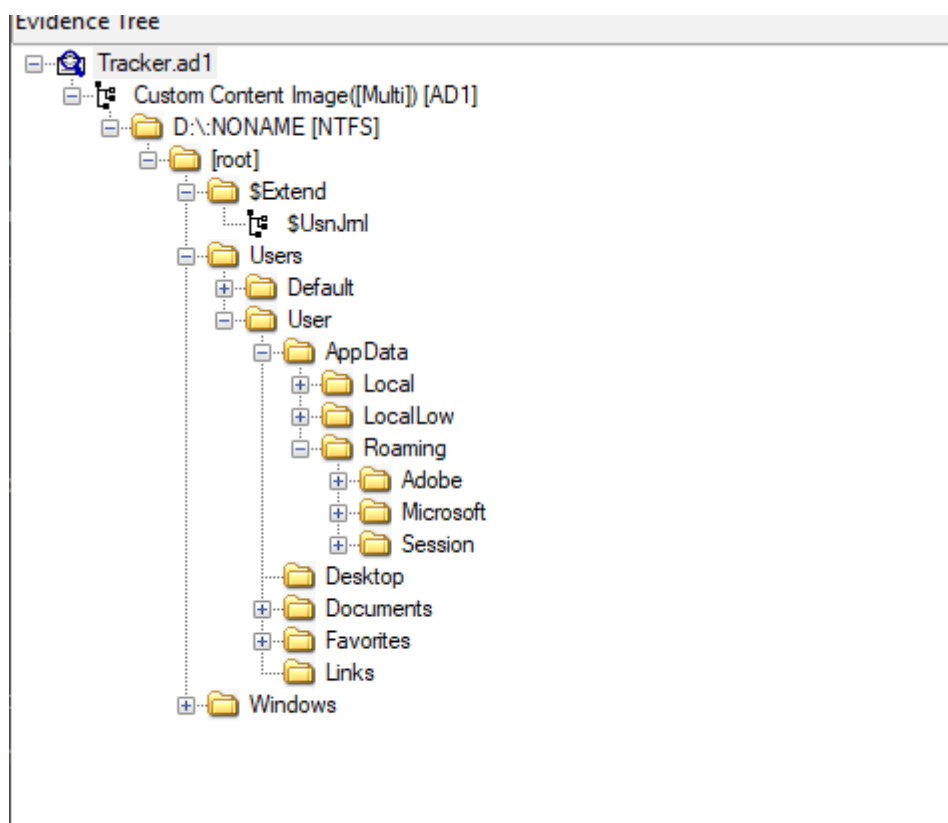
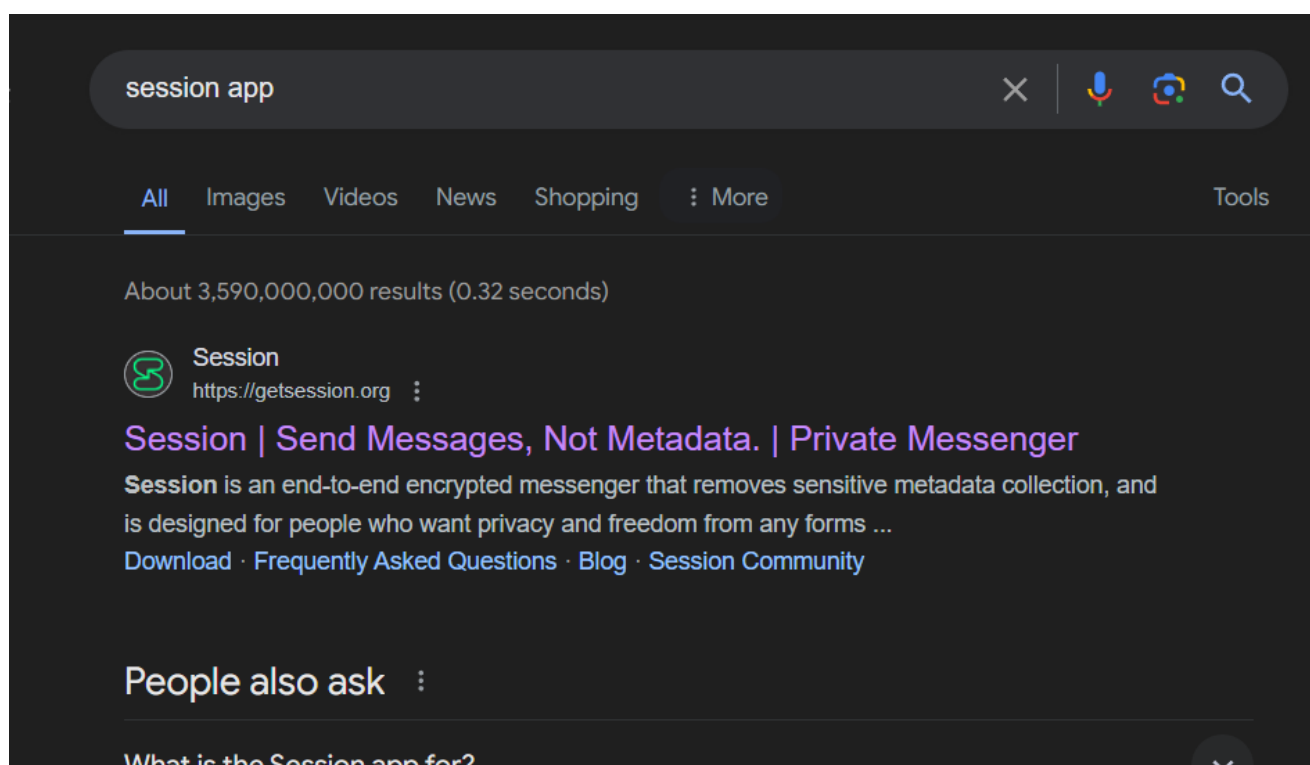


This is a DFIR challenge, we were given a AD1 file. The question ask for SNS ID of the drug dealer
The first thing we need to look for, SNS app.



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.

moving on into finding the ID.



Tracker ad1

- Custom Content Image([Multi]) [AD1]
- D:\NONAME [NTFS]
 - root
 - SExtend
 - SUser.ini
 - Users
 - Default
 - User
 - AppData
 - Local
 - LocalLow
 - Roaming
 - Adobe
 - Microsoft
 - Session
 - attachments noindex
 - blob_storage
 - Cache
 - Code Cache
 - DawnCache
 - GPUCache
 - Local Storage
 - logs
 - Network
 - Session Storage
 - sql

| Name | Size | Type | Date Modified |
|-----------------|------|-------------------|----------------------|
| blob_storage | 1 | Directory | 26/3/2024 3:29:41 AM |
| Cache | 1 | Directory | 26/3/2024 3:29:41 AM |
| Code Cache | 1 | Directory | 26/3/2024 3:29:42 AM |
| DawnCache | 1 | Directory | 26/3/2024 3:29:45 AM |
| GPUCache | 1 | Directory | 26/3/2024 3:29:44 AM |
| LocalStorage | 1 | Directory | 26/3/2024 3:29:41 AM |
| logs | 1 | Directory | 26/3/2024 5:57:04 AM |
| Network | 1 | Directory | 26/3/2024 4:38:18 AM |
| Session Storage | 1 | Directory | 26/3/2024 3:29:49 AM |
| sql | 1 | Directory | 26/3/2024 3:29:43 AM |
| \$I30 | 4 | NTFS Index All... | 26/3/2024 5:57:04 AM |
| config.json | 1 | Regular File | 26/3/2024 3:30:20 AM |
| ephemeral.json | 1 | Regular File | 26/3/2024 4:44:30 AM |
| Local State | 1 | Regular File | 26/3/2024 3:29:51 AM |
| lockfile | 0 | Regular File | 26/3/2024 3:29:41 AM |
| Preferences | 1 | Regular File | 26/3/2024 3:29:51 AM |

```

00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 | 0 .....
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00 | .....
20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00 | .....
30 00 00 00 00 00 00 00 00-00-

```

```
{} config.json x
{} config.json > ...
1 {
2   "key": "9b342d389f8fad56ebdf0d30c94436f7ea1bdcf9daab10f9b93895b100943921",
3   "opengroupPruning": true
4 }
```

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

The screenshot shows the DB Browser for SQLite interface. A modal dialog titled "SQLCipher encryption" is open, prompting the user to enter a password and select encryption settings. The dialog includes fields for "Password", "Raw key", "Encryption settings" (with radio buttons for "SQLCipher 3 defaults", "SQLCipher 4 defaults", and "Custom"), and various configuration options like "Page size", "KDF iterations", "HMAC algorithm", "KDF algorithm", and "Plaintext Header Size".

Below the dialog, the database schema is displayed, showing a list of tables and their corresponding CREATE TABLE statements. The tables include:

- attachment_downloads
- configDump
- conversations
- encryptionKeyPairsForClosedGroupV2
- guardNodes
- identityKeys
- items
- lastHashes
- loki_schema
- messages
- messages_fts
- messages_fts_config
- messages_fts_content
- messages_fts_data
- messages_fts_docsize
- messages_fts_idx
- nodesForPubkey
- openGroupRoomsV2
- seenMessages
- sqlite_sequence
- sqlite_stat1
- sqlite_stat4
- unprocessed

The schema also includes indices for various tables, such as attachment_downloads_pending, attachment_downloads_timestamp, conversation_displayNameInProfile, conversation_nickname, conversations_active, conversations_type, messages_DaR_unread_sent_at, messages_conversation, messages_convo_serverID, messages_duplicate_check, messages_expires_at, messages_hasAttachments, messages_hasFileAttachments, and messages_hasVisualMediaAttachments.

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 | lastJoinedTimestamp |
|---|---|---------------|---------|---------|---------|------|-------------|-------------|-------------|-------------------|---------------|---------------------|
| 1 | 05b31e21e2d05973489f9ca631d084b29a5e6dd4893d0f00ab3889ccf3c0e3c40 | 0 | private | | | 0 | 0 | NULL | NULL | NULL | NULL | |
| 2 | 055df0dc35eb270aa8649be3ac275a0a654404715ba53528f26d343ba203d22f | 1711430222001 | private | | | 0 | 0 | NULL | NULL | sent | I see thx.... | |
| 3 | 05aa64c6099f0e23345c279882edd6f73fd20f5cc7aae2eef4874784ab4a50c77 | 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.

Tracker 1

05aa64c6099f0e23345c279882edd6f73f4d20f5cc7aae2eef4874784ab4a50c77

GET REAL FLAG

Good!

HTO{0ae31a4b92a5489dbce4118b8e57dc11}

You may be blocked if brute force attacks are detected.

HTO{0ae31a4b92a5489dbce4118b8e57dc11}