Mission Name

TheFencesDataCard

History Background

Claire and Ethan are in Asuncion (Paraguay) with she (The Fence). Claire must analyse The Fence´s data card in order to get any relationship among The Fence and SHAX community.

Technical High-Level Overview

The aim is to analyse in depth to locate any clue that allow Claire to identify SHAX community. In this scenario, an iPhone evidence will be provided which contains the final clue to link The Fence with SHAX Community.

Short Description

You´re going to analyse The Fence´s iPhone. Your goal is to locate any clue related to SHAX, if you find it, please give us the ID Citizen linked to SHAX. This time, ID Citizen contains 12 numbers.

Mission Description

The Fence´s iPhone is provided. The aim is to analyse in depth to locate any clue that allow Claire to identify the link SHAX community and The Fences. Your goal is to analyse iPhone evidence provided deeply and locate the ID Citizen linked to SHAX. This time, ID Citizen contains 12 numbers.

Location

ASUNCION | PARAGUAY

Tools

- Autopsy
- SqliteStudio
- plistEditor
- iLEAP

Questions

What is UUID of the App which was investigated previously?

- 074D9D88-04F3-4504-A04D-EE7FF204619C0

Which database contains information about the digits used to lock the iPhone?

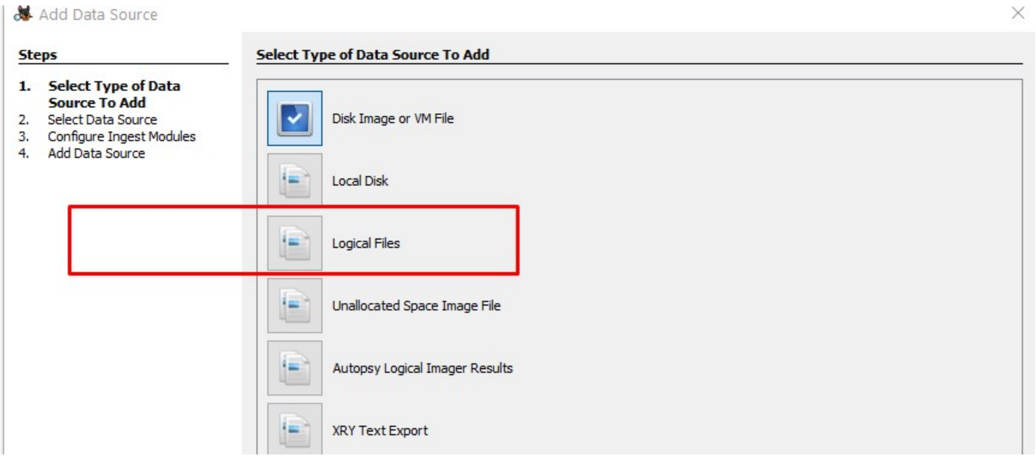
- ADDataStore.sqlitedb

Hints

1. Use Autopsy to analyse The Fences´s iPhone, and search the string "SHAX".
2. Check Apps Installed and iOS notification folder.
3. Check App snapshot (screenshots) folder related with App installed.

Write Up

First of all, player should unzip iPhone evidence provided, create a case on Autopsy tool and add the evidence extracted to the case, like the following picture:



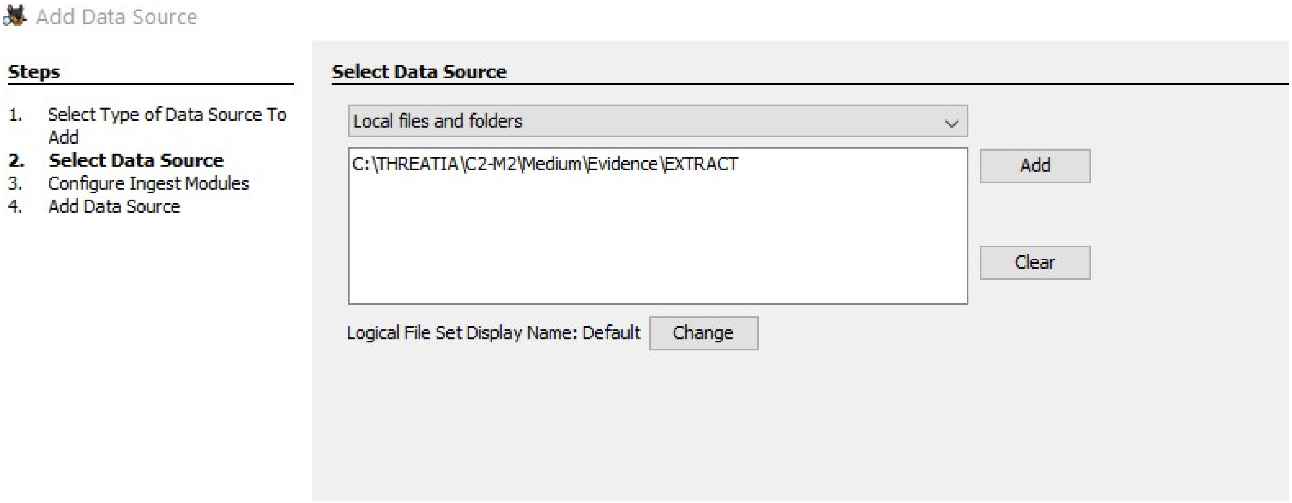
Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

Figure 1



Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

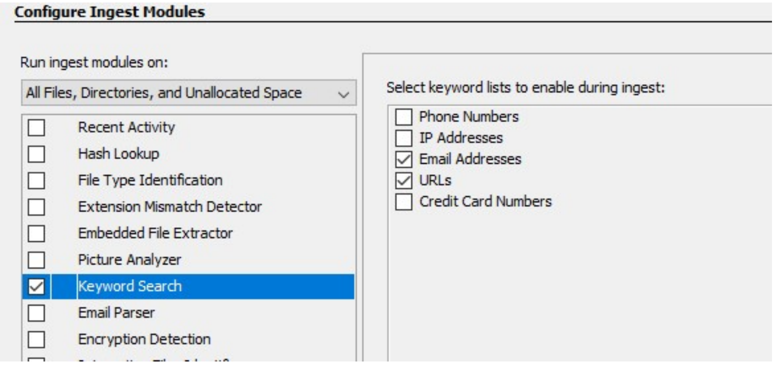
Local files and folders

C:\THREATIA\C2-M2\Medium\Evidence\EXTRACT

Logical File Set Display Name: Default

Figure 2

The key to analyse is "SHAX", so keeping in mind this, player must select on Autopsy "keyword search" on Ingest Modules:



Configure Ingest Modules

Run ingest modules on:

All Files, Directories, and Unallocated Space

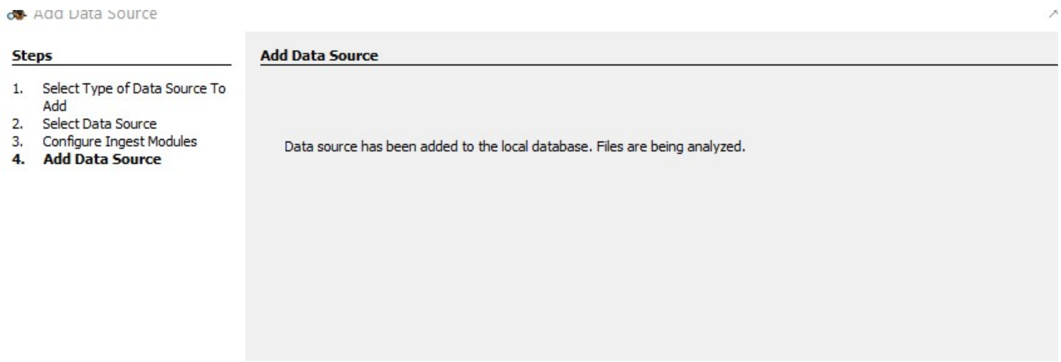
- □ Recent Activity
- □ Hash Lookup
- □ File Type Identification
- □ Extension Mismatch Detector
- □ Embedded File Extractor
- □ Picture Analyzer
- ☑ Keyword Search
- □ Email Parser
- □ Encryption Detection

Select keyword lists to enable during ingest:

- □ Phone Numbers
- □ IP Addresses
- ☑ Email Addresses
- ☑ URLs
- □ Credit Card Numbers

Figure 3

Eventually, data source has been added to the Autopsy case:



Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. **Add Data Source**

Add Data Source

Data source has been added to the local database. Files are being analyzed.

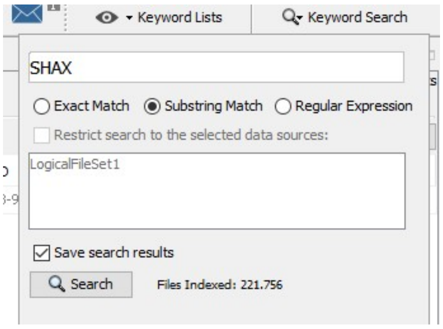
Figure 4

Autopsy will last a few hours to complete the "ingest module", so take it easy…

Starting ingest

Figure 5

Once, Autopsy has been finished, player must search on the keyword search tab: SHAX



SHAX

○ Exact Match ● Substring Match ○ Regular Expression

□ Restrict search to the selected data sources:

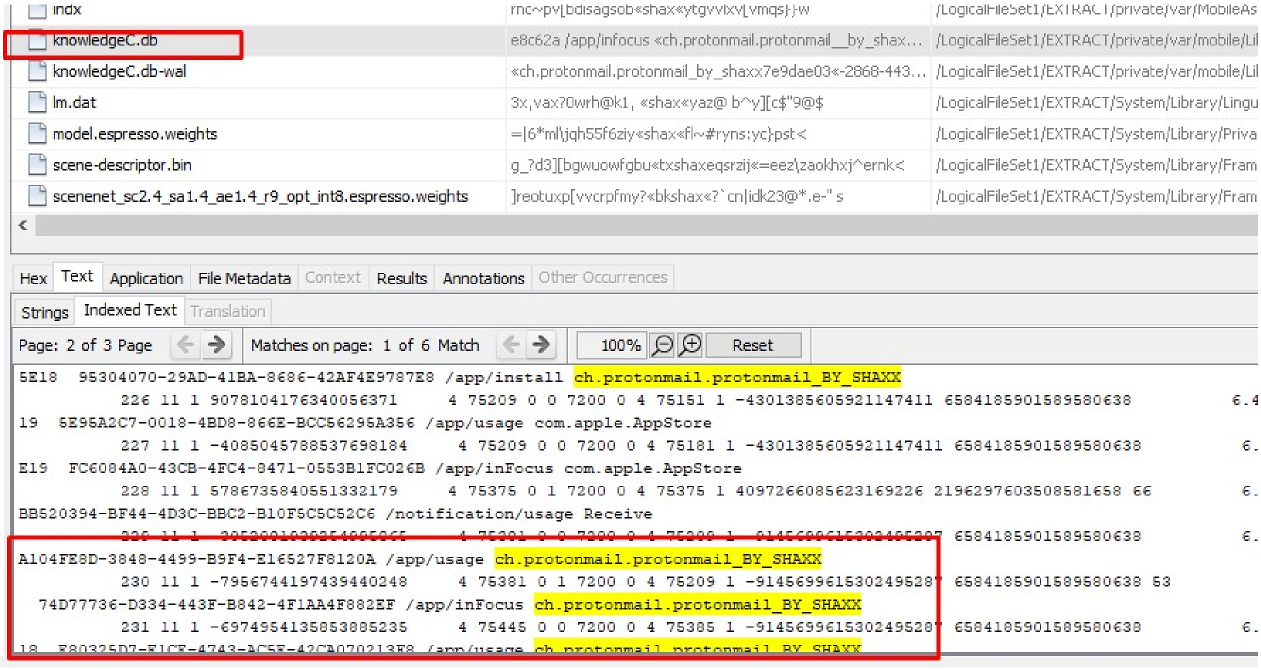
LogicalFileSet1

☑ Save search results

Files Indexed: 221.756

Figure 6

There are many results based on the string "SHAX" but the most important result is the database **knowledgeC.db located on private/var/mobile/Library/CoreDuet/Knowledge:**



indx	rnc~pv[bdisagsob«shax«ytgvvlxv[vmqs}}w	/LogicalFileSet1/EXTRACT/private/var/MobileAs
knowledgeC.db	e8c62a /app/infocus «ch.protonmail.protonmail__by_shax...	/LogicalFileSet1/EXTRACT/private/var/mobile/Lil
knowledgeC.db-wal	«ch.protonmail.protonmail_by_shaxx7e9dae03«-2868-443...	/LogicalFileSet1/EXTRACT/private/var/mobile/Lil
lm.dat	3x,vax?0wrh@k1, «shax«yaz@ b^y][c$"9@$	/LogicalFileSet1/EXTRACT/System/Library/Lingu
model.espresso.weights	=|6*ml\jqh55f6ziy«shax«fl~#ryns:yc}pst<	/LogicalFileSet1/EXTRACT/System/Library/Priva
scene-descriptor.bin	g_?d3][bgwuowfgbu«txshaxeqsrzij«=eez\zaokhxj^ernk<	/LogicalFileSet1/EXTRACT/System/Library/Fram
scenenet_sc2.4_sa1.4_ae1.4_r9_opt_int8.espresso.weights	]reotuxp[vvcrpfmy?«bkshax«?`cn|idk23@*.e-" s	/LogicalFileSet1/EXTRACT/System/Library/Fram

Page: 2 of 3 Page

Matches on page: 1 of 6 Match

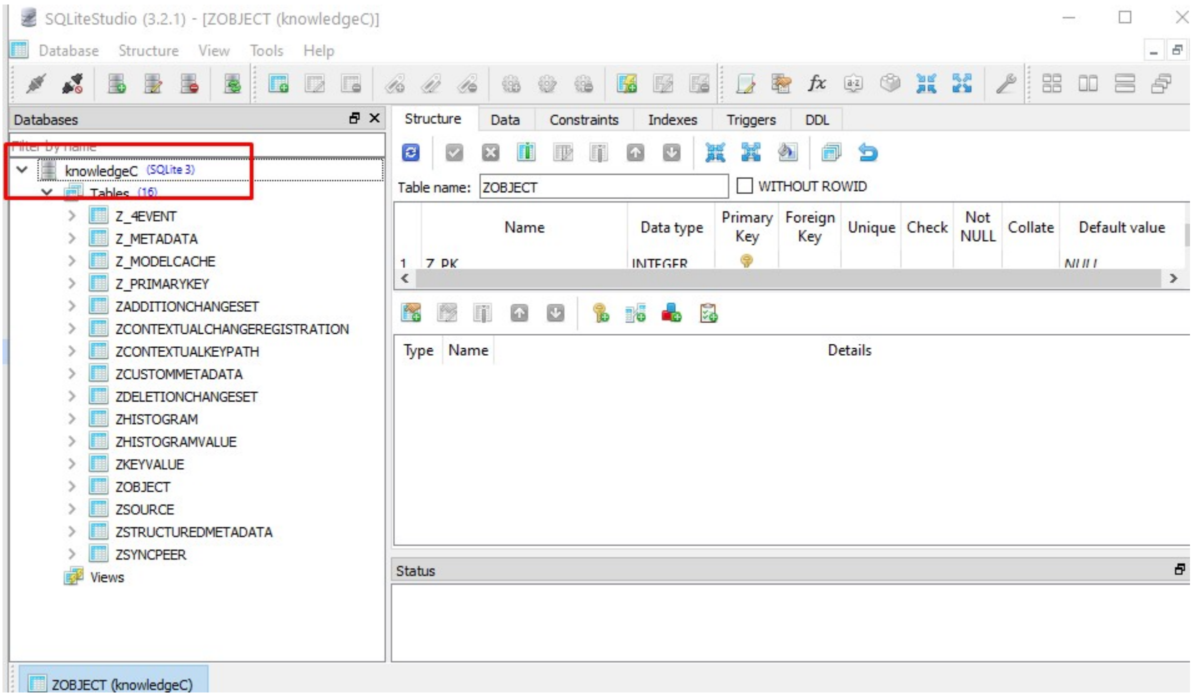
100%

```
5E18  95304070-29AD-41BA-8686-42AF4E9787E8 /app/install ch.protonmail.protonmail_BY_SHAXX
          226 11 1 9078104176340056371      4 75209 0 0 7200 0 4 75151 1 -4301385605921147411 6584185901589580638         6.4
19  5E95A2C7-0018-4BD8-866E-BCC56295A356 /app/usage com.apple.AppStore
          227 11 1 -4085045788537698184      4 75209 0 0 7200 0 4 75181 1 -4301385605921147411 6584185901589580638         6.
E19  FC6084A0-43CB-4FC4-8471-0553B1FC026B /app/inFocus com.apple.AppStore
          228 11 1 5786735840551332179      4 75375 0 1 7200 0 4 75375 1 4097266085623169226 2196297603508581658 66         6.
BB520394-BF44-4D3C-BBC2-B10F5C5C52C6 /notification/usage Receive
          229 11 1 -3052001030254095065      4 75201 0 0 7200 0 4 75209 1 -9145699615302495287 6584185901589580638         6.
A104FE8D-3848-4499-B9F4-E16527F8120A /app/usage ch.protonmail.protonmail_BY_SHAXX
          230 11 1 -7956744197439440248      4 75381 0 1 7200 0 4 75209 1 -9145699615302495287 6584185901589580638 53
  74D77736-D334-443F-B842-4F1AA4F882EF /app/inFocus ch.protonmail.protonmail_BY_SHAXX
          231 11 1 -6974954135853885235      4 75445 0 0 7200 0 4 75385 1 -9145699615302495287 6584185901589580638         6.
18  F80325D7-F1CF-4743-AC5F-42CA070213F8 /app/usage ch.protonmail.protonmail_BY_SHAXX
```

Figure 7

This database contains apps installed on the iPhone Device and other information related to TheFences activity.

Player must analyse deeply, using another tool to open the SQLite database and then, locate where SHAX it´s located.



SQLiteStudio (3.2.1) - [ZOBJECT (knowledgeC)]

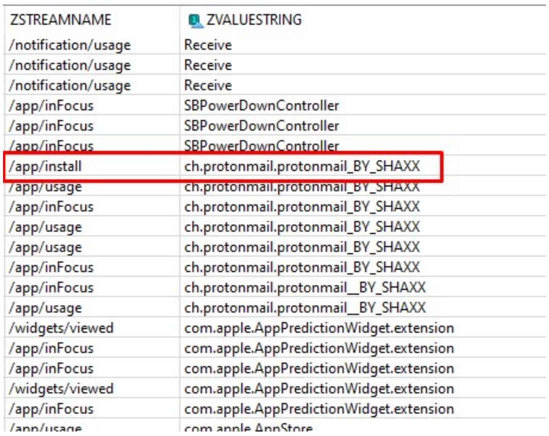
Table name: ZOBJECT

□ WITHOUT ROWID

	Name	Data type	Primary Key	Foreign Key	Unique	Check	Not NULL	Collate	Default value
1	Z_PK	INTEGER							NULL

Figure 8

Installed Apps can be found on ZOBJECT table, and ZVALUESTRING column:



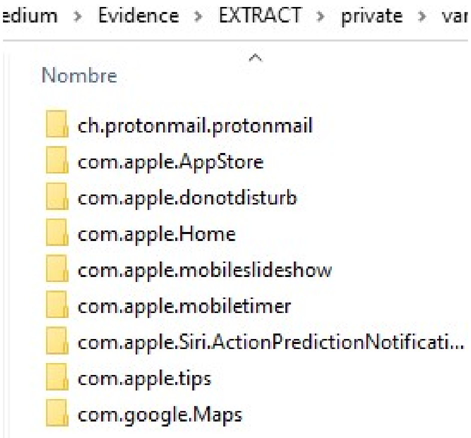
ZSTREAMNAME	ZVALUESTRING
/notification/usage	Receive
/notification/usage	Receive
/notification/usage	Receive
/app/inFocus	SBPowerDownController
/app/inFocus	SBPowerDownController
/app/inFocus	SBPowerDownController
/app/install	ch.protonmail.protonmail_BY_SHAXX
/app/usage	ch.protonmail.protonmail_BY_SHAXX
/app/inFocus	ch.protonmail.protonmail_BY_SHAXX
/app/usage	ch.protonmail.protonmail_BY_SHAXX
/app/usage	ch.protonmail.protonmail_BY_SHAXX
/app/inFocus	ch.protonmail.protonmail_BY_SHAXX
/app/inFocus	ch.protonmail.protonmail__BY_SHAXX
/app/usage	ch.protonmail.protonmail__BY_SHAXX
/widgets/viewed	com.apple.AppPredictionWidget.extension
/app/inFocus	com.apple.AppPredictionWidget.extension
/app/inFocus	com.apple.AppPredictionWidget.extension
/widgets/viewed	com.apple.AppPredictionWidget.extension
/app/inFocus	com.apple.AppPredictionWidget.extension
/app/usage	com.apple.AppStore

Figure 9

As you can see, SHAX has tampered the app, adding a new name to the proton mail APP.

On this phase of the investigation, player must analyse all related to the ProtonMail App. If player does not know anything about iOS forensics artifacts, it will be a complicated task for him. The key of this case it´s an interesting artifact “iOS notifications” folder located at:

- /private/var/mobile/Library/UserNotifications/



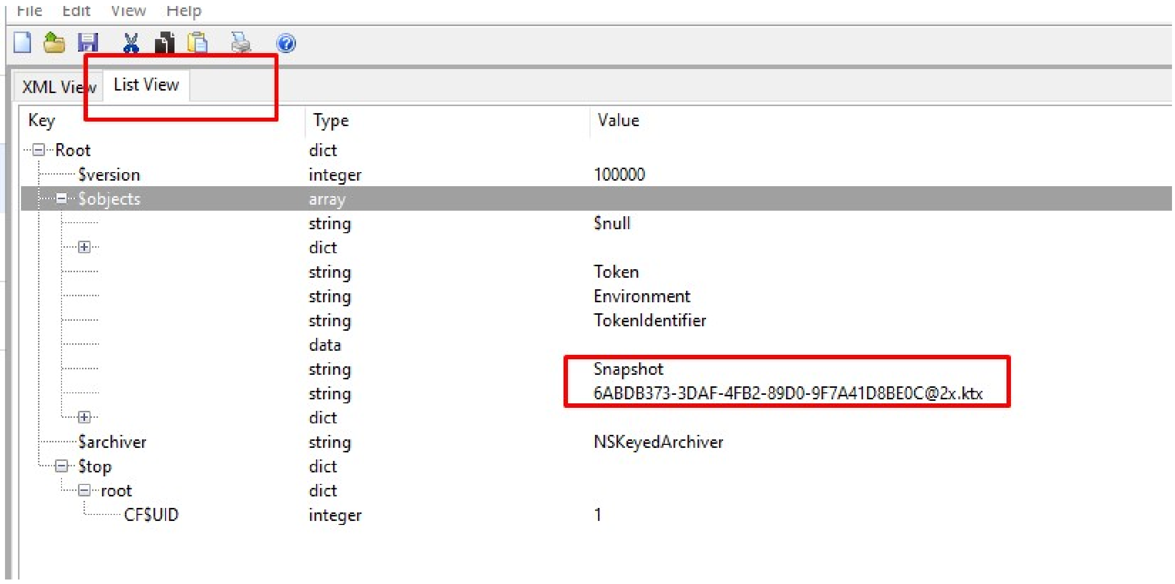
edium > Evidence > EXTRACT > private > var

Nombre

- ch.protonmail.protonmail
- com.apple.AppStore
- com.apple.donotdisturb
- com.apple.Home
- com.apple.mobileslideshow
- com.apple.mobiletimer
- com.apple.Siri.ActionPredictionNotificati...
- com.apple.tips
- com.google.Maps

Figure 10

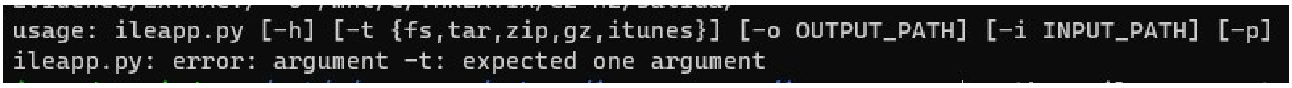
As we can see above, protonmail has User notifications: Categories.plist. Player should open this file with plist editor:



Key	Type	Value
Root	dict	
$version	integer	100000
$objects	array	
	string	$null
	dict	
	string	Token
	string	Environment
	string	TokenIdentifier
	data	
	string	Snapshot
	string	6ABDB373-3DAF-4FB2-89D0-9F7A41D8BE0C@2x.ktx
	dict	
$archiver	string	NSKeyedArchiver
$top	dict	
root	dict	
CF$UID	integer	1

Figure 11

On the List View tab, there is a clue relate to a Snapshot (screenshot). This said, player could find directly the file on Autopsy or launch iLEAPP tool to analyse Screenshots.

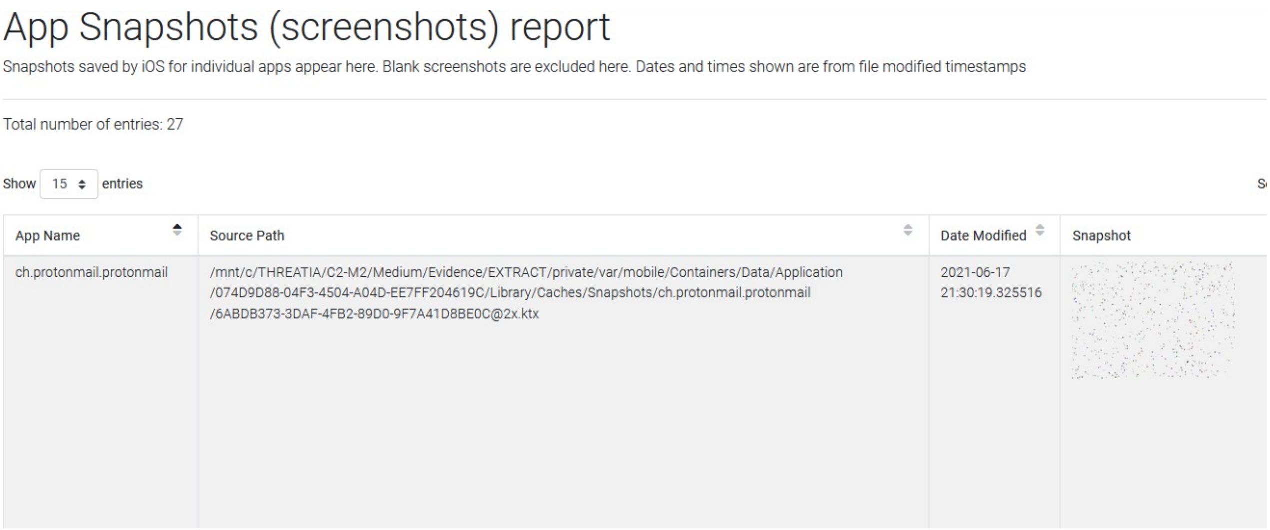


```
usage: ileapp.py [-h] [-t {fs,tar,zip,gz,itunes}] [-o OUTPUT_PATH] [-i INPUT_PATH] [-p]
ileapp.py: error: argument -t: expected one argument
```

Figure 12

- python3 ileapp.py -t fs -i /evidence_extracted/ -o /output_results/

Once iLEAPP finishes, player could locate one index HTML file, which contains all necessary information. On the App Snapshots (screenshots) section, we will see a ProtonMail Snapshot damaged:



App Snapshots (screenshots) report

Snapshots saved by iOS for individual apps appear here. Blank screenshots are excluded here. Dates and times shown are from file modified timestamps

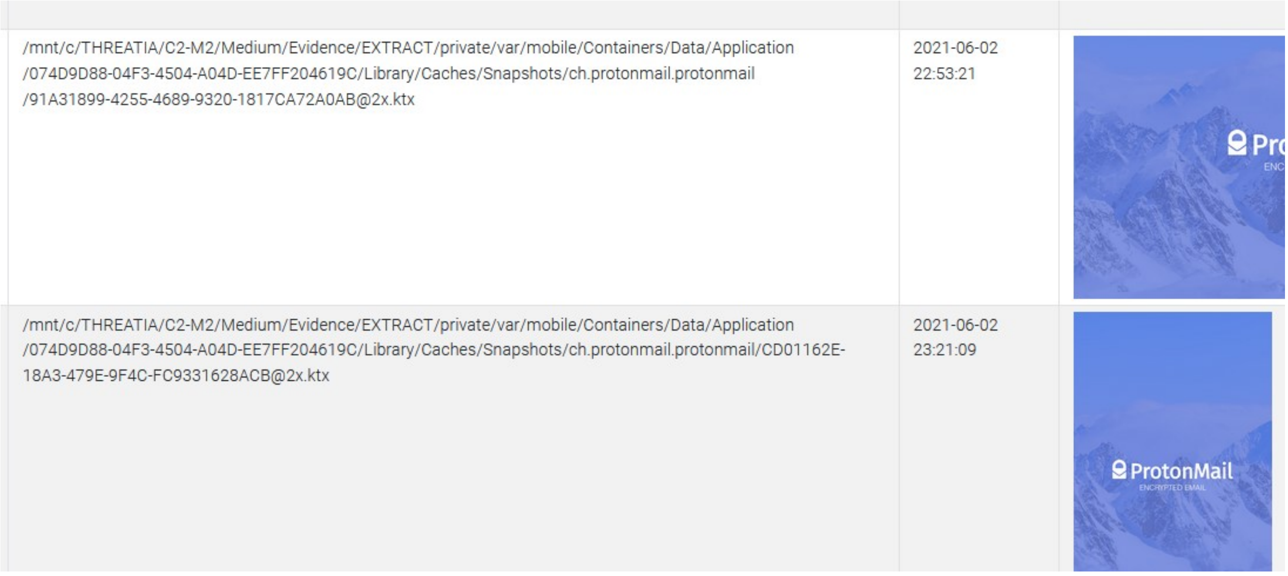
Total number of entries: 27

Show 15 entries

App Name	Source Path	Date Modified	Snapshot
ch.protonmail.protonmail	/mnt/c/THREATIA/C2-M2/Medium/Evidence/EXTRACT/private/var/mobile/Containers/Data/Application/074D9D88-04F3-4504-A04D-EE7FF204619C/Library/Caches/Snapshots/ch.protonmail.protonmail/6ABDB373-3DAF-4FB2-89D0-9F7A41D8BE0C@2x.ktx	2021-06-17 21:30:19.325516	

Figure 13

And the other screenshots could be checked perfectly:



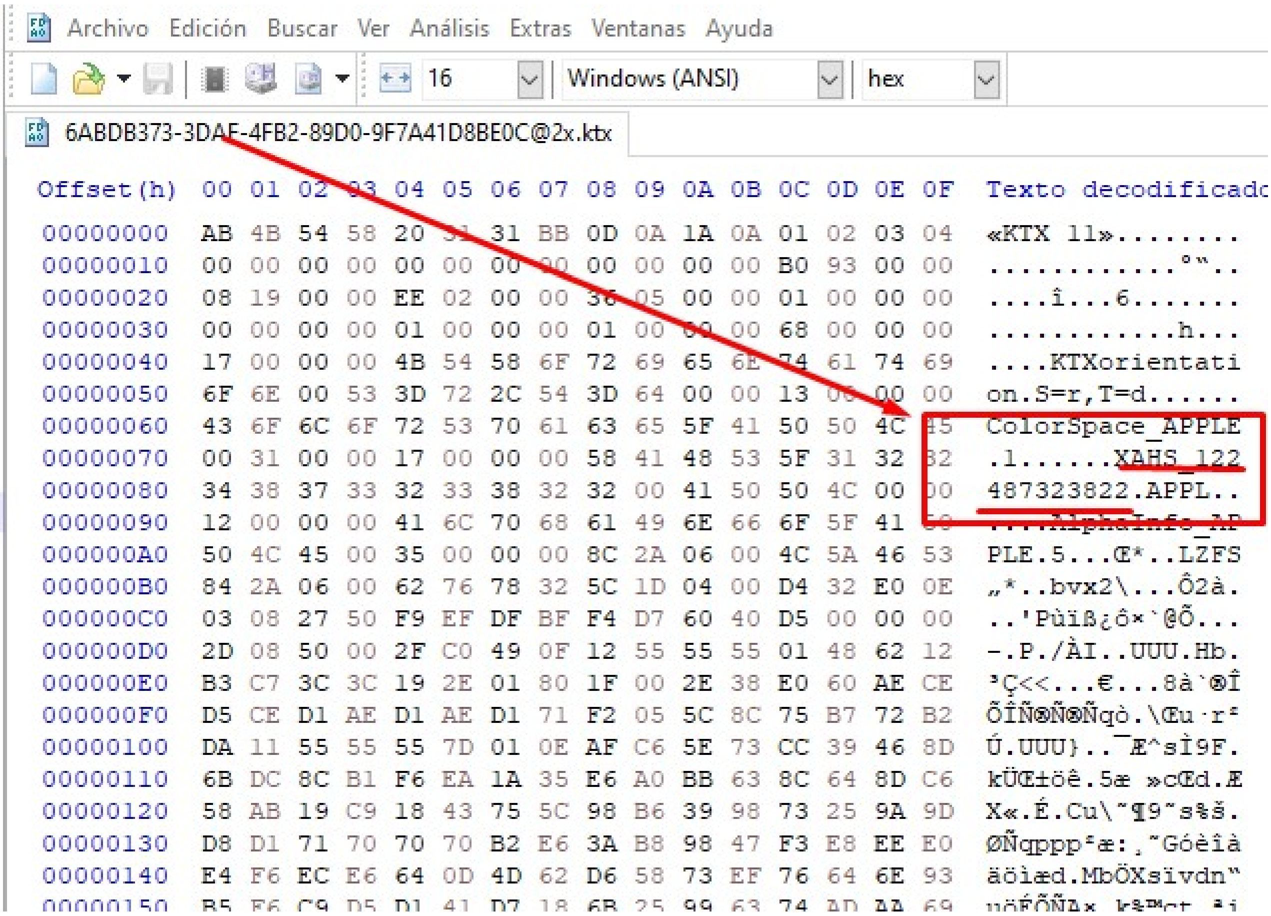
/mnt/c/THREATIA/C2-M2/Medium/Evidence/EXTRACT/private/var/mobile/Containers/Data/Application/074D9D88-04F3-4504-A04D-EE7FF204619C/Library/Caches/Snapshots/ch.protonmail.protonmail/91A31899-4255-4689-9320-1817CA72A0AB@2x.ktx	2021-06-02 22:53:21	
/mnt/c/THREATIA/C2-M2/Medium/Evidence/EXTRACT/private/var/mobile/Containers/Data/Application/074D9D88-04F3-4504-A04D-EE7FF204619C/Library/Caches/Snapshots/ch.protonmail.protonmail/CD01162E-18A3-479E-9F4C-FC9331628ACB@2x.ktx	2021-06-02 23:21:09	

Figure 14

This said, player should pay attention to this fact: one image damaged the rest of the images working? So, it´s mandatory to analyse the picture located at:

- \private\var\mobile\Library\UserNotifications\ch.protonmail.protonmail\6ABDB373-3DAF-4FB2-89D0-9F7A41D8BE0C@2x.ktx

Using an Hex Editor , like HxD player will able to identify the required 12 numbers among the XAHS string, which is SHAX string, but in reverse order: XAHS_**122487323822**



6ABDB373-3DAF-4FB2-89D0-9F7A41D8BE0C@2x.ktx

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Texto decodificado
00000000  AB 4B 54 58 20 31 31 BB 0D 0A 1A 0A 01 02 03 04  «KTX 11»........
00000010  00 00 00 00 00 00 00 00 00 00 00 00 B0 93 00 00  ............°“..
00000020  08 19 00 00 EE 02 00 00 36 05 00 00 01 00 00 00  ....î...6.......
00000030  00 00 00 00 01 00 00 00 01 00 00 00 68 00 00 00  ............h...
00000040  17 00 00 00 4B 54 58 6F 72 69 65 6E 74 61 74 69  ....KTXorientati
00000050  6F 6E 00 53 3D 72 2C 54 3D 64 00 00 13 06 00 00  on.S=r,T=d......
00000060  43 6F 6C 6F 72 53 70 61 63 65 5F 41 50 50 4C 45  ColorSpace_APPLE
00000070  00 31 00 00 17 00 00 00 58 41 48 53 5F 31 32 32  .1......XAHS_122
00000080  34 38 37 33 32 33 38 32 32 00 41 50 50 4C 00 00  487323822.APPL..
00000090  12 00 00 00 41 6C 70 68 61 49 6E 66 6F 5F 41 50  ....AlphaInfo_AP
000000A0  50 4C 45 00 35 00 00 00 8C 2A 06 00 4C 5A 46 53  PLE.5...Œ*..LZFS
000000B0  84 2A 06 00 62 76 78 32 5C 1D 04 00 D4 32 E0 0E  „*..bvx2\...Ô2à.
000000C0  03 08 27 50 F9 EF DF BF F4 D7 60 40 D5 00 00 00  ..'Pùïß¿ô×`@Õ...
000000D0  2D 08 50 00 2F C0 49 0F 12 55 55 55 01 48 62 12  -.P./ÀI..UUU.Hb.
000000E0  B3 C7 3C 3C 19 2E 01 80 1F 00 2E 38 E0 60 AE CE  ³Ç<<...€...8à`®Î
000000F0  D5 CE D1 AE D1 AE D1 71 F2 05 5C 8C 75 B7 72 B2  ÕÎÑ®Ñ®Ñqò.\Œu·r²
00000100  DA 11 55 55 55 7D 01 0E AF C6 5E 73 CC 39 46 8D  Ú.UUU}..¯Æ^sÌ9F.
00000110  6B DC 8C B1 F6 EA 1A 35 E6 A0 BB 63 8C 64 8D C6  kÜŒ±öê.5æ »cŒd.Æ
00000120  58 AB 19 C9 18 43 75 5C 98 B6 39 98 73 25 9A 9D  X«.É.Cu\˜¶9˜s%š.
00000130  D8 D1 71 70 70 70 B2 E6 3A B8 98 47 F3 E8 EE E0  ØÑqppp²æ:¸˜Góèîà
00000140  E4 F6 EC E6 64 0D 4D 62 D6 58 73 EF 76 64 6E 93  äöìæd.MbÖXsïvdn“
00000150  B5 F6 C9 D5 D1 41 D7 18 6B 25 99 63 74 AD AA 69  µöÉÕÑA×.k%™ct.ªi
```

Figure 15

Flag Information

flag{122487323822}