Jailbroken Lab – CyberDefenders

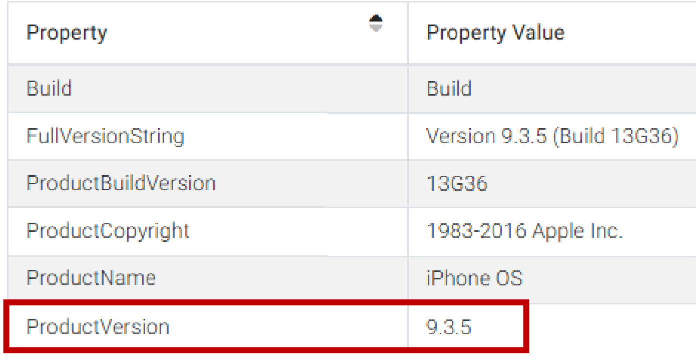
Analyze a jailbroken iOS device.

iLEAPP ver. 2.3.0	Software used for system log analysis and event timeline.
DBrowser ver. 3.13	Software used for database analysis.
Oxygen Forensics ver. 18.1	Software used for analyzing operating system artifacts and visualizing conversations.
Timestamp Decoder	Software used for timestamp conversion.

Figura 1 - Software utilizzati

What is the IOS version of this device?

By analyzing the `LastBuildInfo.plist` file (`.\data\private\var\installd\Library\MobileInstallation\`), it is possible to view a series of information relating to the device's operating system.



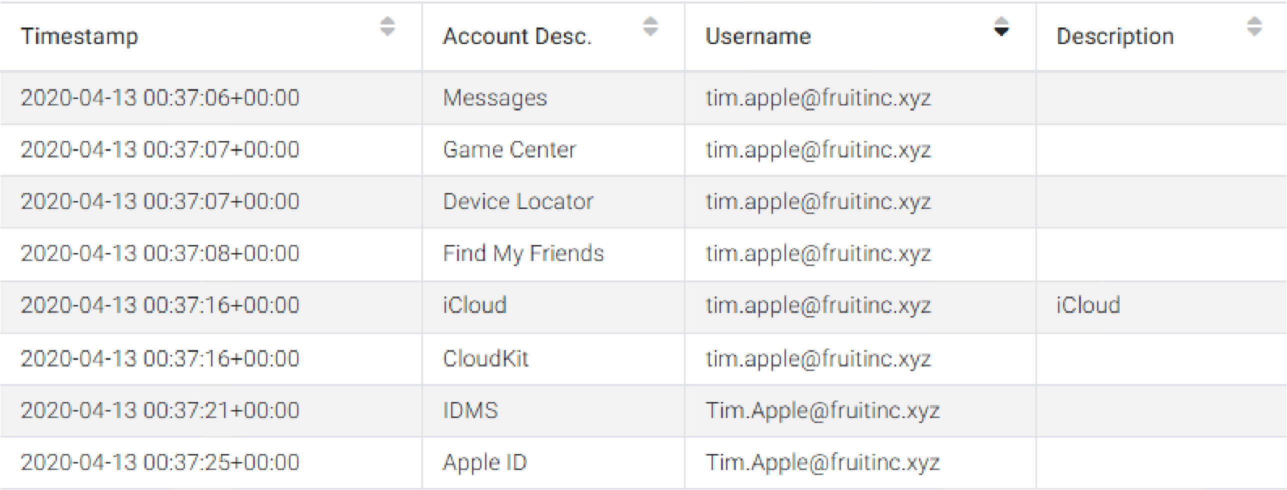
Property	Property Value
Build	Build
FullVersionString	Version 9.3.5 (Build 13G36)
ProductBuildVersion	13G36
ProductCopyright	1983-2016 Apple Inc.
ProductName	iPhone OS
ProductVersion	9.3.5

Figura 2 – iOS version

Who is using the iPad?

Include their first and last name.

From the analysis of the `account data` it is possible to immediately see that the owner's name is `Tim Apple`.

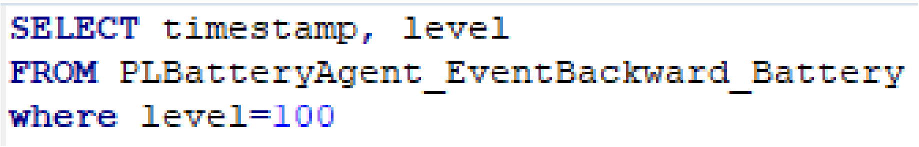


Timestamp	Account Desc.	Username	Description
2020-04-13 00:37:06+00:00	Messages	tim.apple@fruitinc.xyz	
2020-04-13 00:37:07+00:00	Game Center	tim.apple@fruitinc.xyz	
2020-04-13 00:37:07+00:00	Device Locator	tim.apple@fruitinc.xyz	
2020-04-13 00:37:08+00:00	Find My Friends	tim.apple@fruitinc.xyz	
2020-04-13 00:37:16+00:00	iCloud	tim.apple@fruitinc.xyz	iCloud
2020-04-13 00:37:16+00:00	CloudKit	tim.apple@fruitinc.xyz	
2020-04-13 00:37:21+00:00	IDMS	Tim.Apple@fruitinc.xyz	
2020-04-13 00:37:25+00:00	Apple ID	Tim.Apple@fruitinc.xyz	

Figura 3 - Owner's name

When was the last time this device was 100% charged?

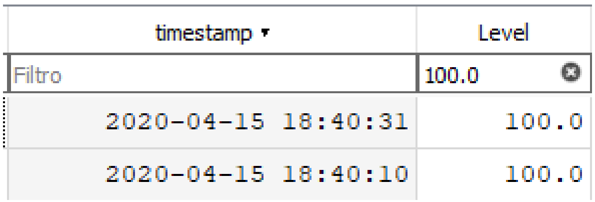
To solve this challenge, a query was performed on the `PLBatteryAgent_EventBackward_Battery` database looking for all the dates when the battery level was brought to 100%.



```
SELECT timestamp, level
FROM PLBatteryAgent_EventBackward_Battery
where level=100
```

Figura 4 - Query

To display the date correctly, you need to perform the following conversion: `datetime("timestamp", 'unixepoch')`.

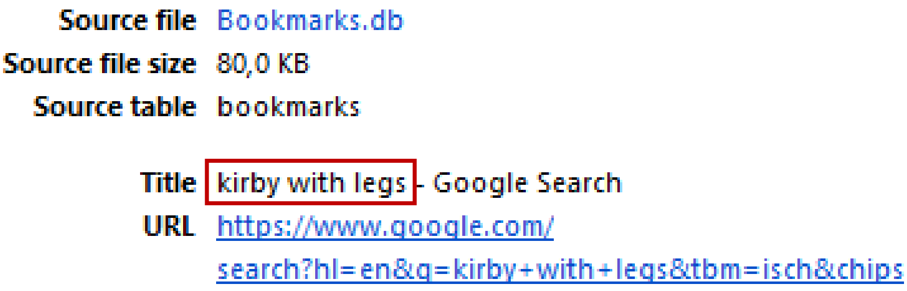


timestamp ▾	Level
Filtro	100.0
2020-04-15 18:40:31	100.0
2020-04-15 18:40:10	100.0

Figura 5 - Correct date

What is the title of the webpage that was viewed the most?

Analyzing the web history with oxygen, it was noticed that in `Bookmarks\com.apple.FrequentlyVisitedSites` section there is only one entry:



Source file	Bookmarks.db
Source file size	80,0 KB
Source table	bookmarks
Title	kirby with legs - Google Search
URL	https://www.google.com/search?hl=en&q=kirby+with+legs&tbm=isch&chips

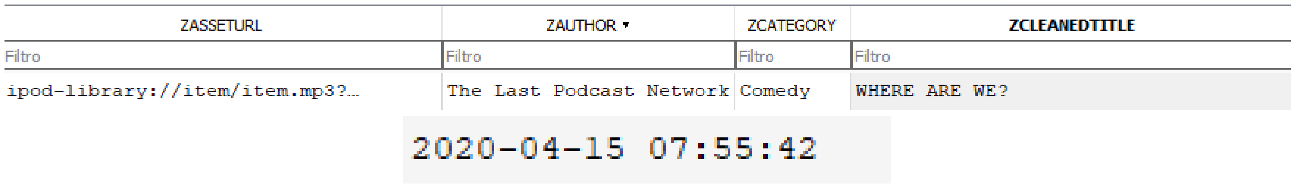
Figura 6 - Frequently Visited Website

The answer is therefore "`kirby with legs`".

What is the title of the first podcast that was downloaded?

The folder containing the podcasts in the phone's Podcast application has been analyzed: `.\private\var\mobile\Containers\Shared\AppGroup\80179E24-1812-4B5F-8063-AECFC3773A7A\Documents`. The database called MTLibrary.sqlite was analyzed to find the last downloaded episode.

The table `ZMTEPISODE` containing all downloaded episodes has been analyzed and the fist downloaded episode is "`WHERE ARE WE?`" by *The Last Podcast Network*.



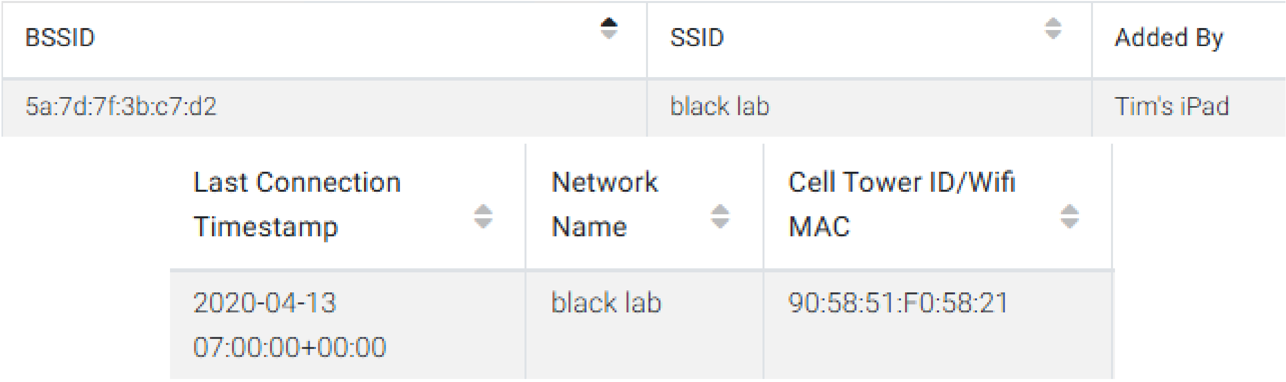
ZASSETURL	ZAUTHOR ▾	ZCATEGORY	ZCLEANEDTITLE
Filtro	Filtro	Filtro	Filtro
ipod-library://item/item.mp3?...	The Last Podcast Network	Comedy	WHERE ARE WE?

2020-04-15 07:55:42

Figura 7 - First podcast

What is the name of the WiFi network this device connected to?

Simple information to find in the `com.apple.wifid.plist` file and `netusage.sqlite`:



BSSID	SSID	Added By
5a:7d:7f:3b:c7:d2	black lab	Tim's iPad

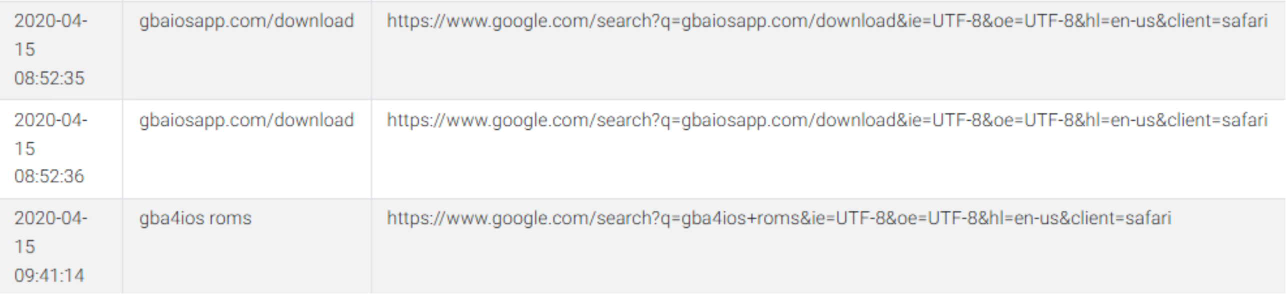
Last Connection Timestamp	Network Name	Cell Tower ID/Wifi MAC
2020-04-13 07:00:00+00:00	black lab	90:58:51:F0:58:21

Figura 8 - WiFi network

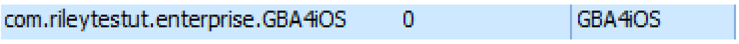
The correct answer is therefore `black lab`.

What is the name of the skin/color scheme used for the game emulator?

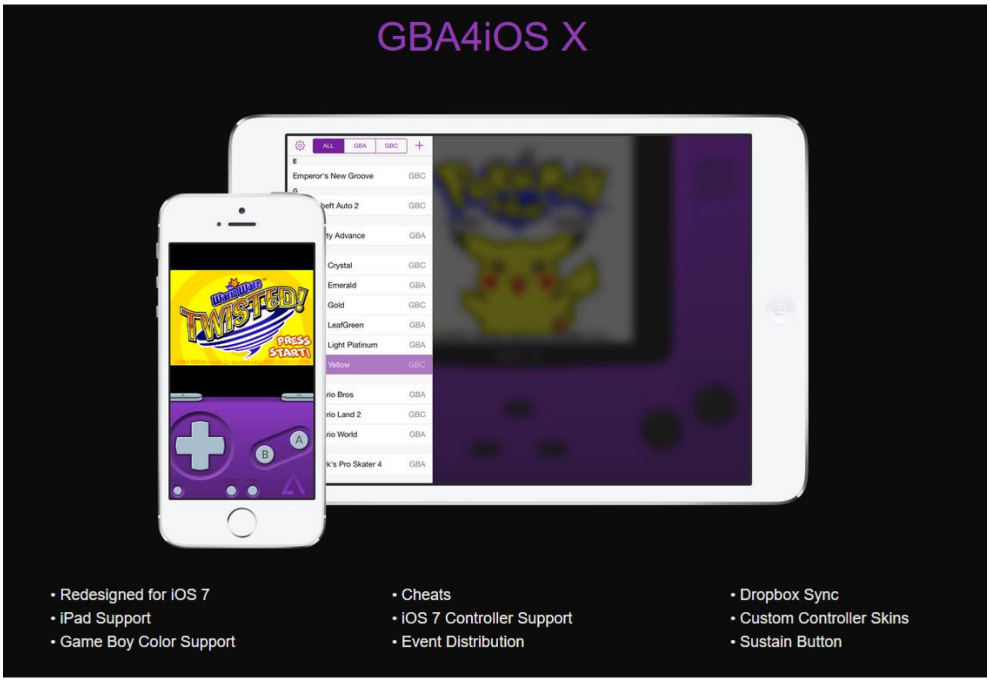
Among Google searches, there are some related to the following game emulator.



2020-04-15 08:52:35	gbaiosapp.com/download	https://www.google.com/search?q=gbaiosapp.com/download&ie=UTF-8&oe=UTF-8&hl=en-us&client=safari
2020-04-15 08:52:36	gbaiosapp.com/download	https://www.google.com/search?q=gbaiosapp.com/download&ie=UTF-8&oe=UTF-8&hl=en-us&client=safari
2020-04-15 09:41:14	gba4ios roms	https://www.google.com/search?q=gba4ios+roms&ie=UTF-8&oe=UTF-8&hl=en-us&client=safari



com.rileytestut.enterprise.GBA4iOS	0	GBA4iOS



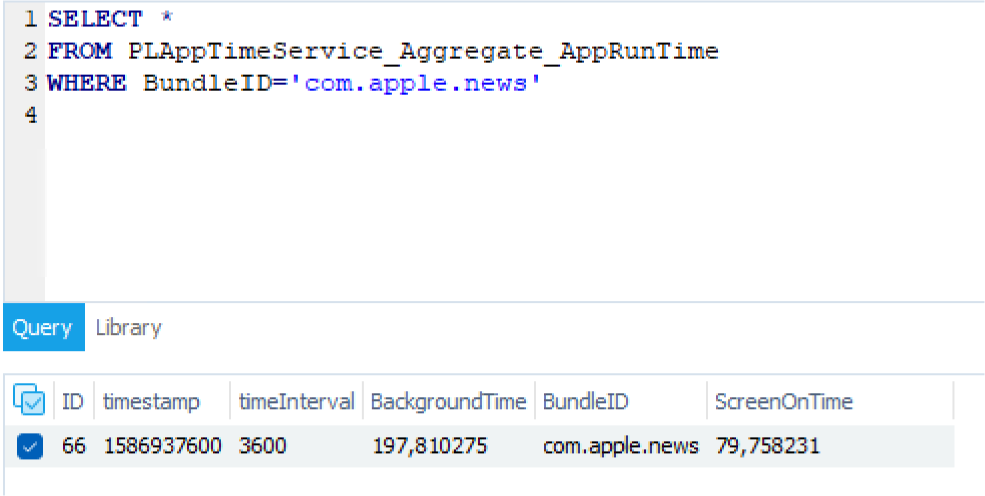
- Redesigned for iOS 7
- iPad Support
- Game Boy Color Support
- Cheats
- iOS 7 Controller Support
- Event Distribution
- Dropbox Sync
- Custom Controller Skins
- Sustain Button

Figura 9 - Game emulator

The scheme name used by the game emulator is `Default.gbaskin`. The evidence was obtained from the GBA4iOS.app directory.

How long did the News app run in the background?

From the analysis of the `PLAppTimeService_Aggregate_AppRunTime` database, data relating to the `com.apple.news` application were analyzed using the following query:



```sql
SELECT *
FROM PLAppTimeService_Aggregate_AppRunTime
WHERE BundleID='com.apple.news'

```

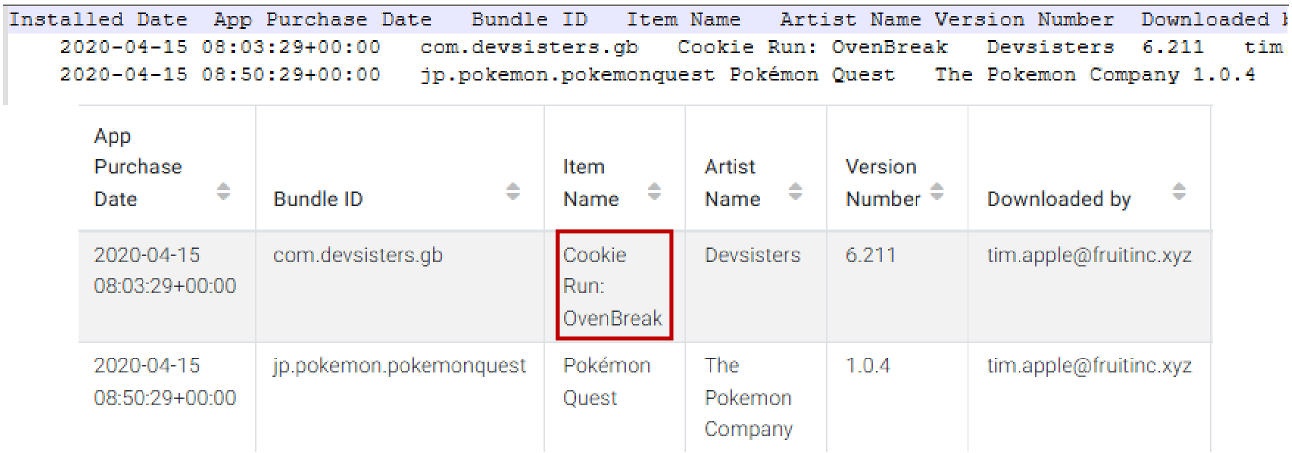
ID	timestamp	timeInterval	BackgroundTime	BundleID	ScreenOnTime
66	1586937600	3600	197,810275	com.apple.news	79,758231

Figura 10- Query and answer

The correct answer is `197.810275`.

What was the first app download from AppStore?

iOS logs AppStore installations are in `private/var/installd/Library/Logs/MobileInstallation/` log files. An easier way to find the result is to look at the `Apps - Itunes Metadata.tsv` file with `iLEAPP`, in which it is clear that the answer is **`Cookie Run`.**



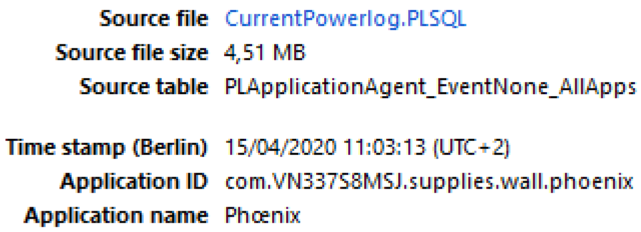
```
Installed Date  App Purchase Date   Bundle ID   Item Name   Artist Name Version Number  Downloaded
    2020-04-15 08:03:29+00:00   com.devsisters.gb   Cookie Run: OvenBreak   Devsisters  6.211   tim
    2020-04-15 08:50:29+00:00   jp.pokemon.pokemonquest Pokémon Quest   The Pokemon Company 1.0.4
```

App Purchase Date	Bundle ID	Item Name	Artist Name	Version Number	Downloaded by
2020-04-15 08:03:29+00:00	com.devsisters.gb	Cookie Run: OvenBreak	Devsisters	6.211	tim.apple@fruitinc.xyz
2020-04-15 08:50:29+00:00	jp.pokemon.pokemonquest	Pokémon Quest	The Pokemon Company	1.0.4	tim.apple@fruitinc.xyz

Figura 11 - First download app

What app was used to jailbreak this device?

Phoenix, https://phoenixpwn.com/, it appears to be the app used to jailbreak the device.



Source file	CurrentPowerlog.PLSQL
Source file size	4,51 MB
Source table	PLApplicationAgent_EventNone_AllApps
Time stamp (Berlin)	15/04/2020 11:03:13 (UTC+2)
Application ID	com.VN337S8MSJ.supplies.wall.phoenix
Application name	Phœnix

PHŒNIX
Semi-untethered jailbreak for 9.3.5-9.3.6.
All 32-bit devices supported.

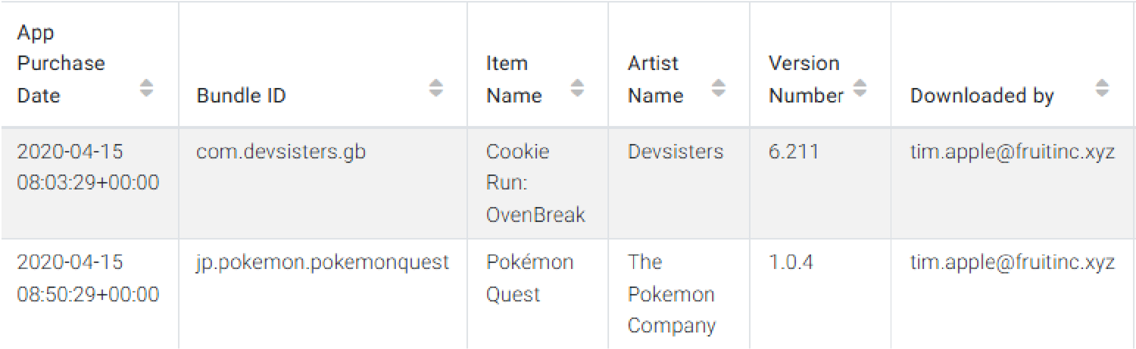
com.VN337S8MSJ.supplies.wall.phoenix

/private/var/containers/Bundle/Application/E9DB300B-6B96-422E-9122-327F475623F0/**Phoenix.app**

Figura 12 - Jailbreak app

How many applications were installed from the app store?

These are the two apps above.

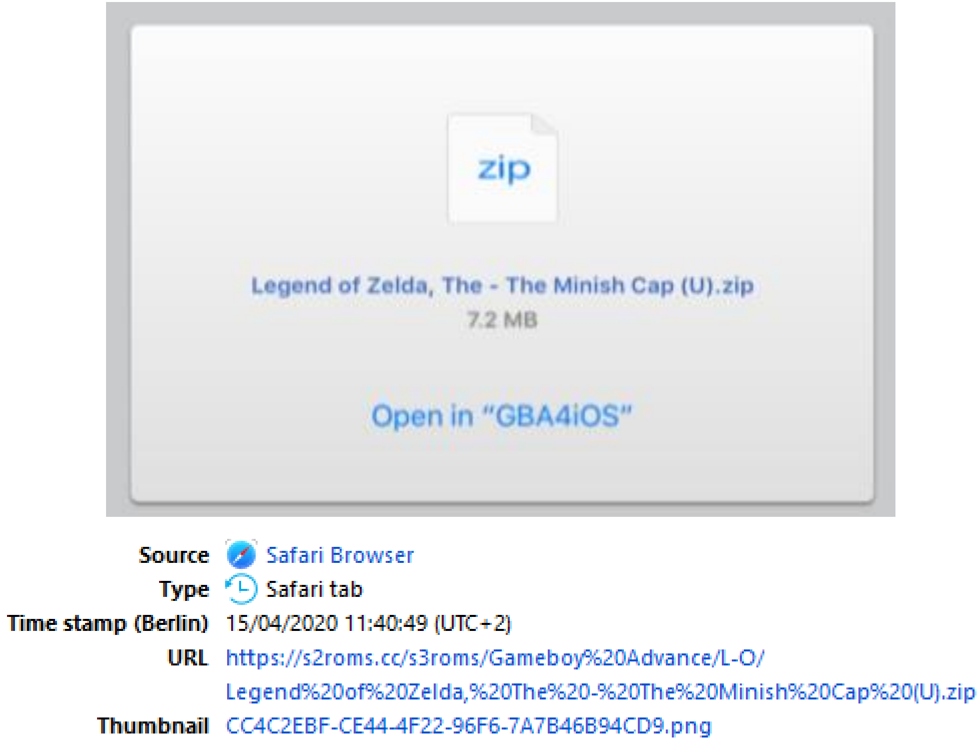


App Purchase Date	Bundle ID	Item Name	Artist Name	Version Number	Downloaded by
2020-04-15 08:03:29+00:00	com.devsisters.gb	Cookie Run: OvenBreak	Devsisters	6.211	tim.apple@fruitinc.xyz
2020-04-15 08:50:29+00:00	jp.pokemon.pokemonquest	Pokémon Quest	The Pokemon Company	1.0.4	tim.apple@fruitinc.xyz

Figura 13 - Apps

How many save states were made for the emulator game that was most recently obtained?

`Safari Broswer – History` has to be analyzed, sorting by descending `Visit Timestamp`, so that can be found that the game is `Legend Of Zelda`.

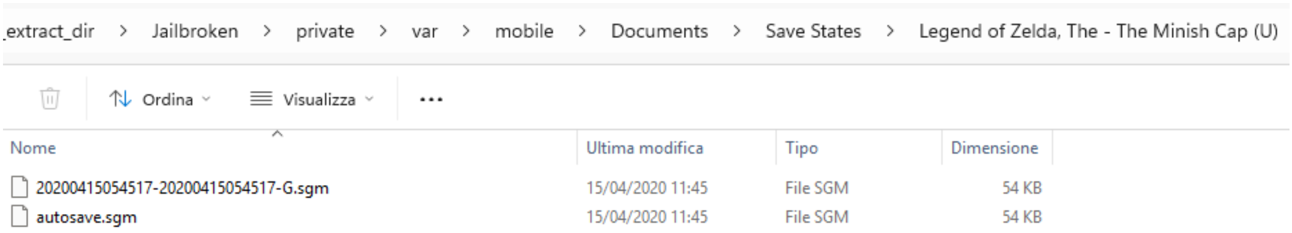


Legend of Zelda, The - The Minish Cap (U).zip
7.2 MB

Source	Safari Browser
Type	Safari tab
Time stamp (Berlin)	15/04/2020 11:40:49 (UTC+2)
URL	https://s2roms.cc/s3roms/Gameboy%20Advance/L-O/Legend%20of%20Zelda,%20The%20-%20The%20Minish%20Cap%20(U).zip
Thumbnail	CC4C2EBF-CE44-4F22-96F6-7A7B46B94CD9.png

Figura 14 - Game

In `private/var/mobile/Documents` there's the folder `Save States`: in the Zelda game folder there is only 1 save state.



extract_dir > Jailbroken > private > var > mobile > Documents > Save States > Legend of Zelda, The - The Minish Cap (U)

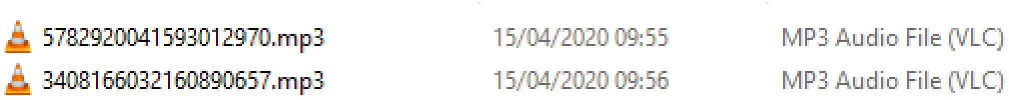
Nome	Ultima modifica	Tipo	Dimensione
20200415054517-20200415054517-G.sgm	15/04/2020 11:45	File SGM	54 KB
autosave.sgm	15/04/2020 11:45	File SGM	54 KB

Figura 15 - the only save state

What language is the user trying to learn?

According to the podcast he is listening to, the language is `Spanish`.

You can listen to them in `private/var/mobile/Media/Podcasts` folder.



5782920041593012970.mp3	15/04/2020 09:55	MP3 Audio File (VLC)
3408166032160890657.mp3	15/04/2020 09:56	MP3 Audio File (VLC)

Figura 16 - Podcast

The user was reading a book in real life but used their IPad to record the page that they had left off on. What number was it?

In the DCIM folder there is a video in which a book is opened and stopped at `page 85` (`IMG_0008.MOV`).

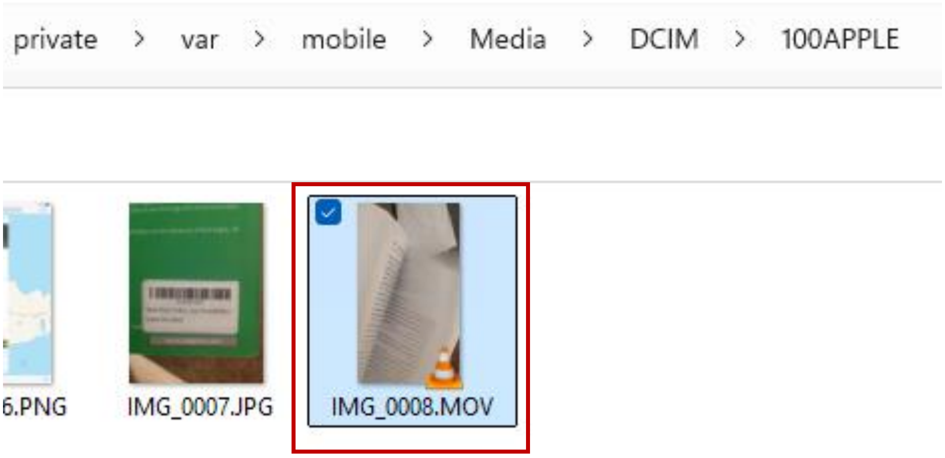
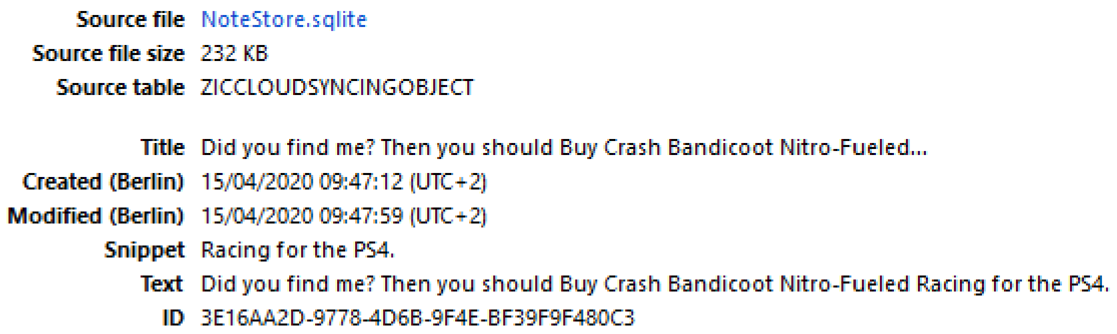


Figura 17 - File di interesse

If you found me, what should I buy?

On the phone there is a note, which is the answer:



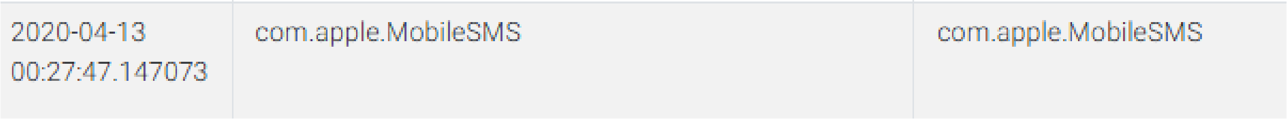
Source file	NoteStore.sqlite
Source file size	232 KB
Source table	ZICCLOUDSYNCINGOBJECT
Title	Did you find me? Then you should Buy Crash Bandicoot Nitro-Fueled...
Created (Berlin)	15/04/2020 09:47:12 (UTC+2)
Modified (Berlin)	15/04/2020 09:47:59 (UTC+2)
Snippet	Racing for the PS4.
Text	Did you find me? Then you should Buy Crash Bandicoot Nitro-Fueled Racing for the PS4.
ID	3E16AA2D-9778-4D6B-9F4E-BF39F9F480C3

Figura 18 - Buy it

The answer is `Crash Bandicoot Nitro-Fueled` Racing for PS4.

There was an SMS app on this device's dock. Provide the name in bundle format.

The native iMessage application package is `com.apple.MobileSMS`.

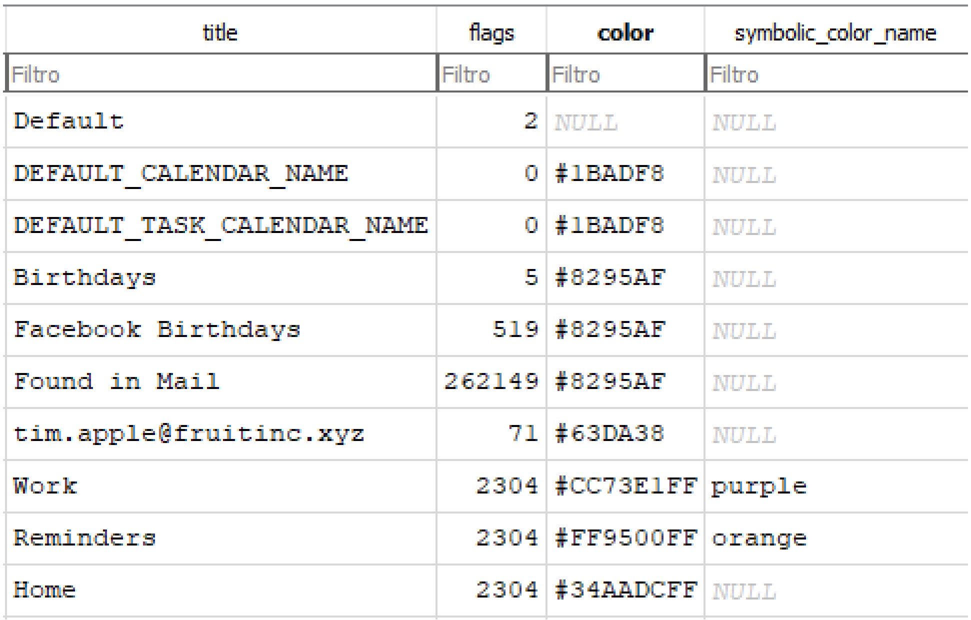


2020-04-13 00:27:47.147073	com.apple.MobileSMS	com.apple.MobileSMS

Figura 19 - SMS app

A reminder was made to get something, what was it?

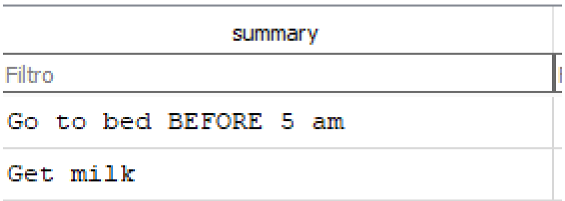
Analyzing the calendars present on the device, there is one called "`Reminder`" (orange).



title	flags	color	symbolic_color_name
Default	2	NULL	NULL
DEFAULT_CALENDAR_NAME	0	#1BADF8	NULL
DEFAULT_TASK_CALENDAR_NAME	0	#1BADF8	NULL
Birthdays	5	#8295AF	NULL
Facebook Birthdays	519	#8295AF	NULL
Found in Mail	262149	#8295AF	NULL
tim.apple@fruitinc.xyz	71	#63DA38	NULL
Work	2304	#CC73E1FF	purple
Reminders	2304	#FF9500FF	orange
Home	2304	#34AADCFF	NULL

Figura 20 – Calendar

The data of interest is found in the `CalendarItem` table: “Get `milk`”.



summary
Go to bed BEFORE 5 am
Get milk

Figura 21 - Get milk