

# Informatyka śledcza Laboratorium nr 6

## Raport – Nikodem Jakubowski

### Przygotowanie środowiska.

Pobrałem wymagany plik.

```
(user@kali)~[/Desktop]
$ ll
total 15892872
-rw-r--r-- 1 user user 16267641856 Dec 21 20:23 13-3-1.tar
```

Pobrałem sqlite3.

```
(user@kali)~[/Desktop]
$ sqlite3 --help
Usage: sqlite3 [OPTIONS] [FILENAME [SQL]]
FILENAME is the name of an SQLite database. A new database is created
if the file does not previously exist. Defaults to :memory:.
OPTIONS include:
--          treat no subsequent arguments as options
-A ARGS...  run ".archive ARGS" and exit
```

Pobrałem iLEAPP na podstawie instrukcji z githuba.

```
(user@kali)~[/Desktop/iLEAPP]
$ python3 ileapp.py
usage: ileapp.py [-h] [-t {fs,tar,zip,gz,itunes}] [-o OUTPUT_PATH] [-i INPUT_PATH] [-tz TIMEZONE] [-w] [-m LOAD_PROFILE] [-d LOAD_CASE_DATA] [-c CREATE_PROFILE_CASEDATA] [-p]

iLEAPP: iOS Logs, Events, And Plists Parser.

options:
-h, --help            show this help message and exit
-t {fs,tar,zip,gz,itunes}
                        Specify the input type. 'fs' for a folder containing extracted files with normal paths and names, 'tar', 'zip', or 'gz' for compressed packages containing files
                        with normal names, or 'itunes' for a folder containing a raw iTunes backup with hashed paths and names.
-o OUTPUT_PATH, --output_path OUTPUT_PATH
                        Path to base output folder (this must exist)
-i INPUT_PATH, --input_path INPUT_PATH
                        Path to input file/folder
-tz TIMEZONE, --timezone TIMEZONE
                        Timezone name (e.g., 'America/NewYork')
-w, --wrap_text        Do not wrap text for output of data files
-m LOAD_PROFILE, --load_profile LOAD_PROFILE
                        Path to iLEAPP Profile file (.ilprofile).
-d LOAD_CASE_DATA, --load_case_data LOAD_CASE_DATA
                        Path to LEAPP Case Data file (.lcsedata).
-c CREATE_PROFILE_CASEDATA, --create_profile_casedata CREATE_PROFILE_CASEDATA
                        Generate an iLEAPP Profile file (.ilprofile) or LEAPP Case Data file (.lcsedata) into the specified path. This argument is meant to be used alone, without any
                        other arguments.
-p, --artifact_paths    Generate a text file list of artifact paths. This argument is meant to be used alone, without any other arguments.
```

Mam też sqldbviewer.

```
(user@kali)~[/Desktop]
$ sudo apt install sqldbviewer
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
sqldbviewer is already the newest version (3.12.2-3).
sqldbviewer set to manually installed.
The following packages were automatically installed and are no longer required:
gcc-12-base libarmadillo11 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8 libcodec2-1.1 libdav1d6 libgcc-12-dev libgdal33 libgeos3.12.0 libgumbo1 libgupnp-igd-1.0-4 libjim0.81
libnfs13 libobjc-12-dev libplacebo292 libstdc++-12-dev libtcluajit2 libutf8proc2 libvp7 libwireshark16 libwiretap3 libwsutil14 lua-lpeg python3-aioredis python3-apscheduler
python3-jdcal python3-pyminifier python3-quamash python3-tzlocal
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 78 not upgraded.
```

Pobrałem również Plistutil.

```
(user@kali)~[/Desktop]
$ plistutil -h
Usage: plistutil [OPTIONS] [-i FILE] [-o FILE]

Convert a plist FILE from binary to XML format or vice-versa.

OPTIONS:
-i, --infile FILE      Optional FILE to convert from or stdin if - or not used
-o, --outfile FILE     Optional FILE to convert to or stdout if - or not used
-f, --format [bin|xml] Force output format, regardless of input type
-d, --debug            Enable extended debug output
-v, --version          Print version information

Homepage: <https://libimobiledevice.org>
Bug Reports: <https://github.com/libimobiledevice/libplist/issues>
```

## Zadanie 1 – Zawartość baz danych systemu IOS.

Musiałem zwiększyć przestrzeń dyskową przy pomocy „gParted”. Następnie odpakować plik tar. Finalnie dostałem się do folderu z instrukcji.

Przechodzę do folderu: Accounts (~/.private/var/mobile/Library/Accounts).

```
(user@kali)-[~/../var/mobile/Library/Accounts]
$ pwd
/home/user/Desktop/Volumes/JOSEH/NoTar-13-3-1/var/mobile/Library/Accounts
```

Wyszukuje dostępne tabele.

```
sqlite> SELECT name FROM sqlite_master WHERE type='table';
ZACCESSOPTIONSKEY
Z_10WNINGACCOUNTTYPES
ZACCOUNT
Z_2ENABLEDDATACLASSES
Z_2PROVISIONEDDATACLASSES
ZACCOUNTPROPERTY
ZACCOUNTTYPE
Z_4SUPPORTEDDATACLASSES
Z_4SYNCABLEDDATACLASSES
ZAUTHORIZATION
ZCREDENTIALITEM
ZDATACLASS
Z_PRIMARYKEY
Z_METADATA
Z_MODELCACHE
```

Tutaj ilość różnych maili.

```
sqlite> SELECT COUNT(DISTINCT ZUSERNAME) AS total_emails FROM ZACCOUNT;
1
```

Rzeczywiście to się zgadza, są różne wpisy, ale ten sam mail.

```
sqlite> SELECT DISTINCT ZUSERNAME FROM ZACCOUNT;
thisisdffir@gmail.com

sqlite> SELECT ZUSERNAME FROM ZACCOUNT;
thisisdffir@gmail.com
thisisdffir@gmail.com
thisisdffir@gmail.com
thisisdffir@gmail.com
thisisdffir@gmail.com
thisisdffir@gmail.com

thisisdffir@gmail.com
thisisdffir@gmail.com

thisisdffir@gmail.com

thisisdffir@gmail.com
```

Adresy podpięte do iCloud.

```
sqlite> SELECT ZUSERNAME FROM ZACCOUNT WHERE ZACCOUNTDESCRIPTION LIKE '%iCloud%';
thisisdffir@gmail.com
```

Tutaj podpięte do gmail, cały czas ten sam.

```
sqlite> SELECT ZUSERNAME FROM ZACCOUNT WHERE ZACCOUNTDESCRIPTION LIKE '%Gmail%';
thisisdffir@gmail.com
thisisdffir@gmail.com
```

Pogrzebałem w ZACCOUNT.

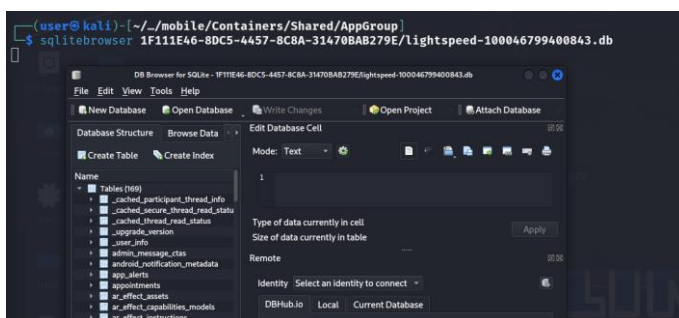
Zawartość ZDATE, wygląda trochę jak timestampy.

```
sqlite> PRAGMA table_info(ZACCOUNT);
0|Z_PK|INTEGER|0||1
1|Z_ENT|INTEGER|0||0
2|Z_OPT|INTEGER|0||0
3|ZACTIVE|INTEGER|0||0
4|ZAUTHENTICATED|INTEGER|0||0
5|ZSUPPORTSAUTHENTICATION|INTEGER|0||0
6|ZVISIBLE|INTEGER|0||0
7|ZACCOUNTTYPE|INTEGER|0||0
8|ZPARENTACCOUNT|INTEGER|0||0
9|ZDATE|TIMESTAMP|0||0
10|ZLASTCREDENTIALRENEWALREJECTIONDATE|TIMESTAMP|0||0
11|ZACCOUNTDESCRIPTION|VARCHAR|0||0
12|ZAUTHENTICATIONTYPE|VARCHAR|0||0
13|ZCREDENTIALTYPE|VARCHAR|0||0
14|ZIDENTIFIER|VARCHAR|0||0
15|ZOWNINGBUNDLEID|VARCHAR|0||0
16|ZUSERNAME|VARCHAR|0||0
17|ZDATACLASSPROPERTIES|BLOB|0||0
sqlite> SELECT ZDATE FROM ZACCOUNT;
606519591.912371
606520062.043928
606520062.507476
606520077.068197
606520075.27839
606520075.243605
606520062.363132
606520075.446426
606520075.3066
606520075.373321
606520077.847509
606520078.027195
```

Jest również możliwość przetworzenia tych timestamps. Dość ciekawy rok...

```
sqlite> SELECT datetime(ZDATE, 'unixepoch') AS formatted_date FROM ZACCOUNT;
1989-03-21 21:39:51
1989-03-21 21:47:42
1989-03-21 21:47:42
1989-03-21 21:47:57
1989-03-21 21:47:55
1989-03-21 21:47:55
1989-03-21 21:47:42
1989-03-21 21:47:55
1989-03-21 21:47:55
1989-03-21 21:47:55
1989-03-21 21:47:57
1989-03-21 21:47:58
1989-03-21 21:49:16
1989-03-21 21:59:47
1989-03-22 01:11:29
1989-03-22 01:11:29
1989-03-22 01:11:29
1989-03-22 01:11:29
```

Otwieram plik lightspeed przy pomocy DB Browser for SQLite.



ID (thread\_key) właściciela urządzenia, czyli Josha.

Name	Type	Schema
Tables (169)		
_cached_participant_thread_info		CREATE TABLE _cached_participant_thread_info( thread_key LONG_INT NOT NULL PRIMARY KEY, th
thread_key	LONG_INT	"thread_key" LONG_INT NOT NULL
thread_name	TEXT	"thread_name" TEXT
other_participant_profile_picture_...	TEXT	"other_participant_profile_picture_url" TEXT
other_participant_profile_picture_...	TEXT	"other_participant_profile_picture_fallback_url" TEXT
other_participant_url_expiration_t...	LONG_INT	"other_participant_url_expiration_timestamp_ms" LONG_INT

DB Browser for SQLite - 1F11E46-8DC5-4457-8C8A-31470B8279E/lightspeed-100

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project

Database Structure Browse Data Edit Pragma Execute SQL

Table: thread\_participant\_detail

contact_id	thread_key	name	nickname	profile_picture_url	profil
100030845613112	100030845613112	Josh Hickman	NULL	https://scontent-iad3-1.xx.fbcdn.net/v/...	/messaging/lis

Emoji jest bardzo sporo, bo aż 1579.

Table: emojis

category_idx	emoji_idx	emoji
1	0	0
2	0	1
3	0	2
4	0	3
5	0	4
6	0	5
7	0	6
8	0	7
9	0	8
10	0	9
11	0	10
12	0	11
13	0	12
14	0	13
15	0	14
16	0	15
17	0	16
18	0	17

1 - 19 of 1579

Na podstawie messages. Doskonale widać wszystko.

Table: messages

thread_key	timestamp_ms	message_id	e_thread_id	text	sender_id	status
100030845613112	1584888980560	mid....	66475...	NULL	100030845613112	N
100030845613112	1584888655426	mid....	66475...	NULL	100046799400843	N
100030845613112	1584888421780	mid....	66475...	Good question.	100046799400843	N
100030845613112	1584888282625	mid....	66475...	That's about right. Wonder if it will actually...	100030845613112	N
100030845613112	1584888176761	mid....	66475...		100046799400843	N
100030845613112	1584888130585	mid....	66475...	Lol!!	100046799400843	N
100030845613112	1584887353191	mid....	66474...	Yep!	100046799400843	N
100030845613112	1584887319288	mid....	66474...	I see. I also see some of our previous ...	100030845613112	N
100030845613112	1584887217210	mid....	66474...	Switched over to FB Messenger.	100046799400843	N
100030845613112	1581271803495	mid....	66323...		100046799400843	N
100030845613112	1580583848183	mid....	66294...	NULL	100030845613112	N
100030845613112	1580583713711	mid....	66294...	NULL	100046799400843	N
100030845613112	1580583583877	mid....	66294...		100046799400843	N
100030845613112	1580583466974	mid....	66294...		100030845613112	N
100030845613112	1580583125918	mid....	66294...	I am. Thanks!	100030845613112	N
100030845613112	1580583078205	mid....	66294...	Good. Hope you are.	100046799400843	N
100030845613112	1580583024499	mid....	66294...	You can now call each other and see ...	100030845613112	N

Wykonuje dodatkowe operacje SQL na danych, żeby znaleźć liczbę osób biorących udział w rozmowie.

DB Browser for SQLite - 1F11E46-8DC5-4457-8C8A-31470B8279E/lightspeed-100046799400843.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database

Database Structure Browse Data Edit Pragma Execute SQL

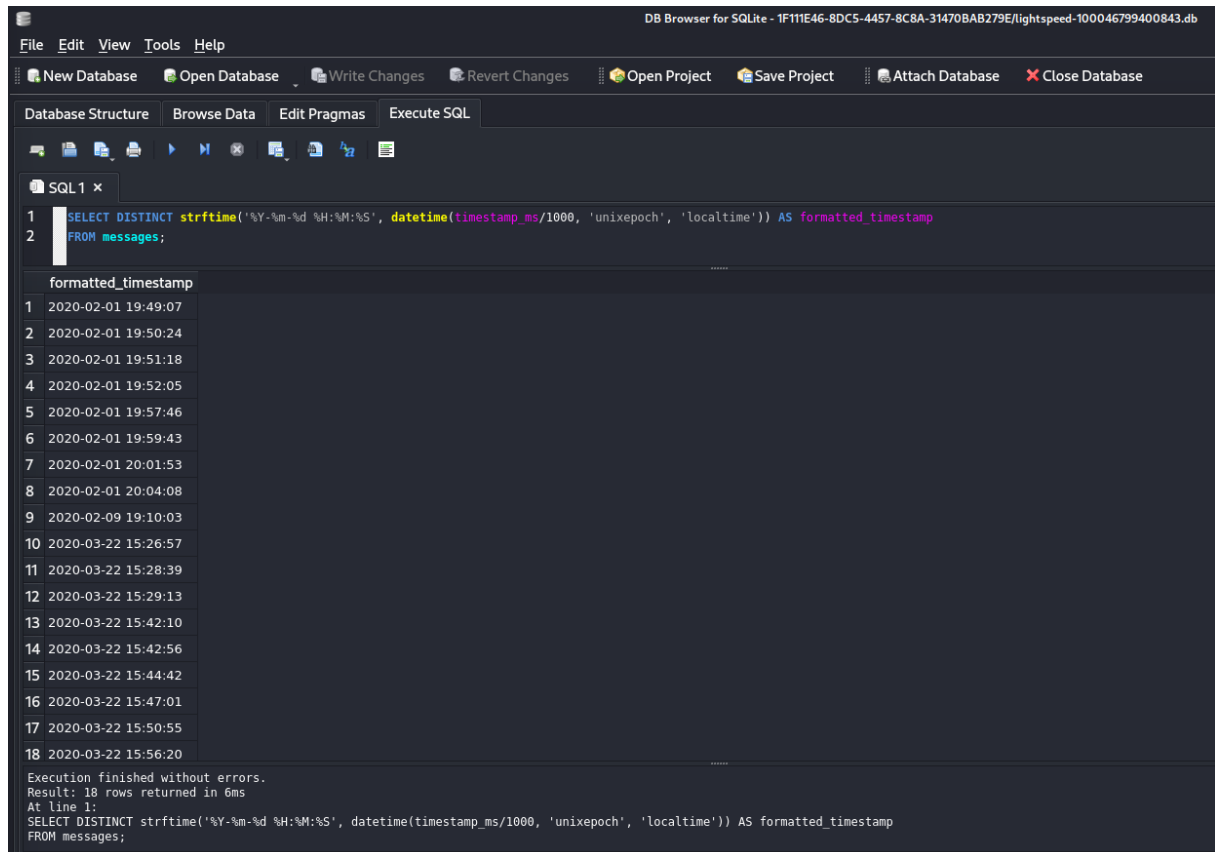
SQL 1 x

```
1 SELECT DISTINCT sender_id FROM messages;
```

Execution finished without errors.  
Result: 2 rows returned in 8ms  
At line 1:  
SELECT DISTINCT sender\_id FROM messages;

sender_id
1 100030845613112
2 100046799400843

Analiza rubryki timestamps. Tych różnych dat (razem z godzinami) wyszło w sumie 18. Ostatnia wiadomość



The screenshot shows the DB Browser for SQLite interface. The top menu bar includes File, Edit, View, Tools, and Help. Below the menu is a toolbar with icons for New Database, Open Database, Write Changes, Revert Changes, Open Project, Save Project, Attach Database, and Close Database. The main window has tabs for Database Structure, Browse Data, Edit Pragma, and Execute SQL. The Execute SQL tab is active, showing a query in the SQL editor:

```
1 SELECT DISTINCT strftime('%Y-%m-%d %H:%M:%S', datetime(timestamp_ms/1000, 'unixepoch', 'localtime')) AS formatted_timestamp
2 FROM messages;
```

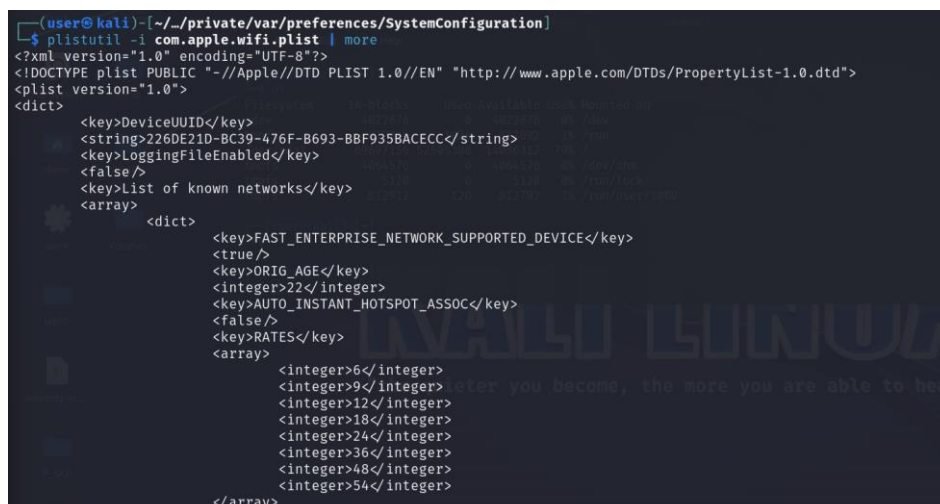
The results are displayed in a table with the column header 'formatted\_timestamp' and 18 rows of data, each representing a unique timestamp. The timestamps range from 2020-02-01 19:49:07 to 2020-03-22 15:56:20. Below the table, a status bar indicates 'Execution finished without errors. Result: 18 rows returned in 6ms. At line 1: SELECT DISTINCT strftime('%Y-%m-%d %H:%M:%S', datetime(timestamp\_ms/1000, 'unixepoch', 'localtime')) AS formatted\_timestamp FROM messages;'

## Zadanie 2 – Pliki plist.

Pliki o rozszerzeniu .plist w systemie iOS to pliki właściwości, używane do przechowywania konfiguracji, danych aplikacji i innych informacji w formie klucz-wartość.

Mogą być one konwertowane do dwóch głównych postaci: XML, które jest czytelne dla człowieka i łatwe do edycji, oraz binarnej, która jest bardziej efektywna pod względem przechowywania danych i szybsza do przetwarzania przez aplikację.

Wyświetlam informacje zawarte w pliku com.apple.wifi.plist.



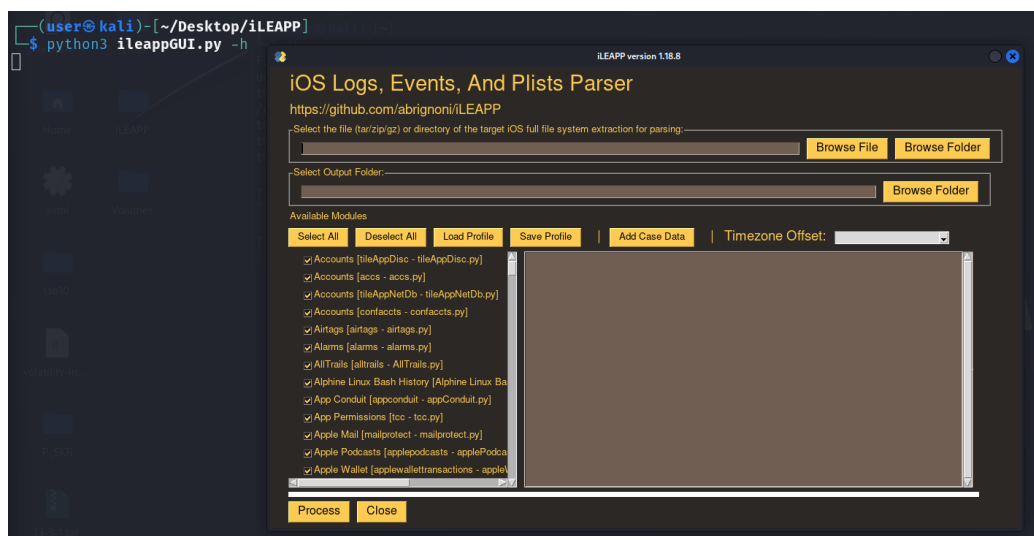
The screenshot shows a terminal window with the command prompt '(user@kali) [~/private/var/preferences/SystemConfiguration]'. The user has entered the command '\$ plutil -i com.apple.wifi.plist | more'. The output is an XML representation of the plist file, showing the root element <dict> with various keys and values. The output is truncated by the 'more' command, showing only the first part of the dictionary. The visible keys include DeviceUUID, string, LoggingFileEnabled, false, List of known networks, array, FAST\_ENTERPRISE\_NETWORK\_SUPPORTED\_DEVICE, true, ORIG\_AGE, integer, AUTO\_INSTANT\_HOTSPOT\_ASSOC, false, RATES, array, and integer values.

Przykładowe informacje zawarte w badanym pliku .plist:

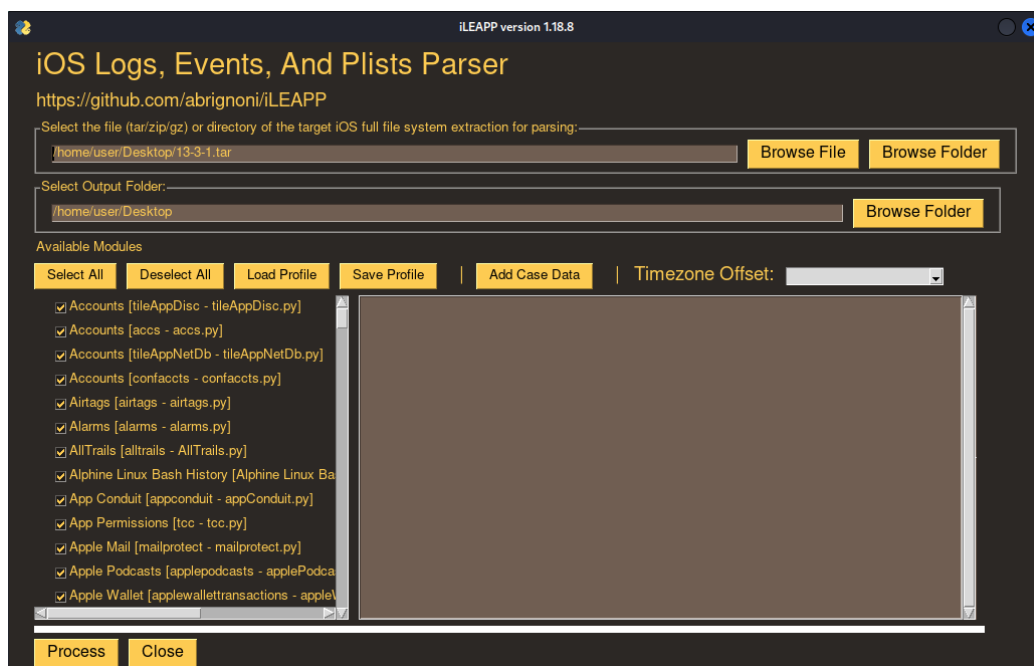
1. DeviceUUID: Unikalny identyfikator urządzenia - "226DE21D-BC39-476F-B693-BBF935BACECC".
2. LoggingFileEnabled: Informacja o tym, czy funkcja zapisu dziennika jest włączona (false).
3. List of known networks: Lista znanych sieci Wi-Fi, z danymi o poszczególnych sieciach, w tym ich SSID, siłę sygnału (Strength), datę ostatniego połączenia (lastJoined), itp.
4. Fallback Preference: Preferencje dotyczące wyboru awaryjnego (2).
5. DisassociationInterval: Interwał rozłączania (1800 sekund).
6. JoinRecommendationMode: Tryb rekomendacji dołączania (Quality).
7. DiagnosticsEnabled: Informacja o włączonych diagnostykach (false).

## Zadanie 3 – Automatyzacja analizy plików systemu IOS.

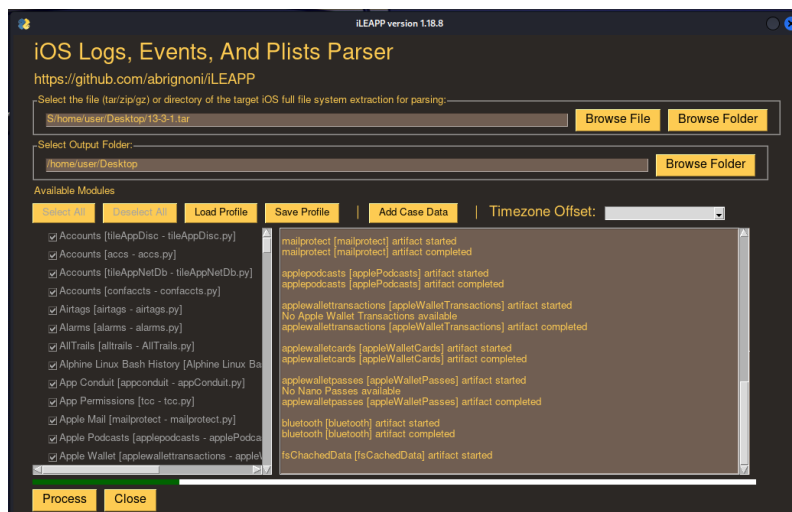
Uruchamiam program.



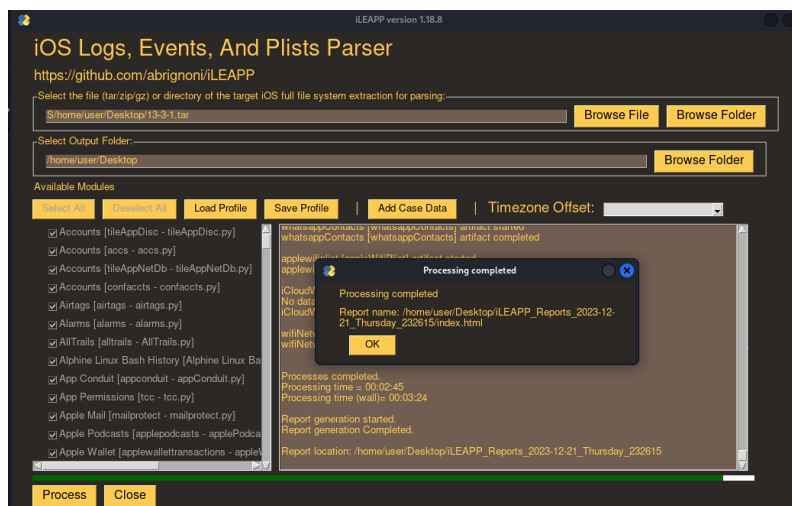
Ustawiam zalecenia zgodnie z poleceniem.



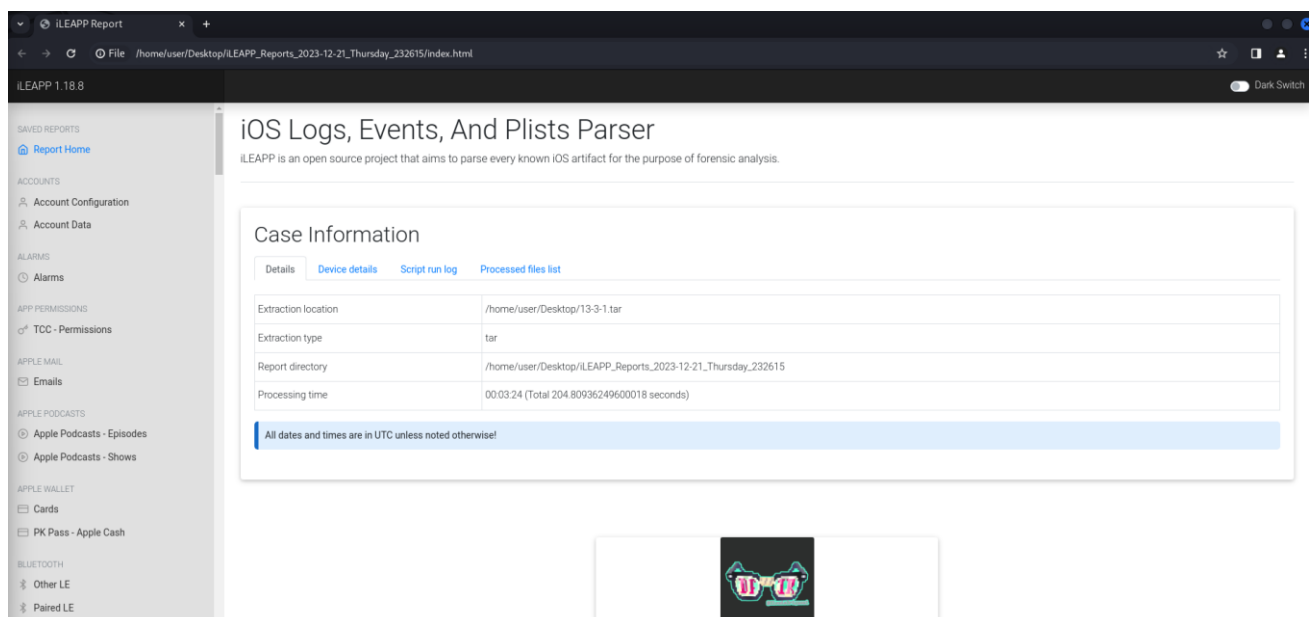
Proces trwa...



Proces zakończony.



Zawartość raportu.





Mamy masę informacji o urządzeniu, z którego pozyskaliśmy dane.

Case Information

- Details
- Device details
- Script run log
- Processed files list

iOS version: 13.3.1  
ProductBuildVersion: 17D50  
Product: iPhone OS  
Reported Phone Number: 19195794674  
IMEI: 355800076093966  
MEID: 35580007609396  
Last Known ICCID: 8901260971148676693  
Keep Message for Days: 0  
Advertiser Identifier: 0D99ABE9-B1D0-41C1-8C45-2681A498AD97  
Obliterated Timestamp: 2020-03-21 21:38:44  
Last iTunes Backup TZ: EDT  
Last Cloud iTunes Backup TZ: EDT  
Last iTunes Backup Date: 2020-04-12 16:55:58  
Cloud Backup Enabled: True  
Last Cloud iTunes Backup Date: 2020-04-11 20:08:23  
Reported Phone Number: 19195794674  
IMEIs: [{‘second’: ‘355800076093966’, ‘first’: ‘1:kOne’}]  
Serial Number: DX3T126VH2XV  
UDID: 00008006-0014141C0AE2002E  
Vehicle - Last Connected: 2020-04-12 13:54:06.534258 - Last Disconnected: 2020-04-12 14:27:42.607752 - Type: CarKit NissanConnect  
Timezone Set: True  
Last Bootstrap Timezone: America/New\_York  
Last Bootstrap Date: 2020-04-10 01:15:02.495596  
Last Good IMSI: 310260974867669  
Self Registration Update IMSI: 310260974867669  
Self Registration Update IMEI: 355800076093966  
Phone Number: 19195794674

Cenne informacje o koncie.

Account Data report

Configured user accounts

Total number of entries: 18  
Account Data located at: /home/user/Desktop/ILEAPP\_Reports\_2023-12-21\_Thursday\_232615/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/Accounts/Accounts3.sqlite

Show 15 entries

Search:

Timestamp	Account Desc.	Username	Description	Identifier	Bundle ID
2020-03-21 21:39:51+00:00	iTunes Store		Local	iTunesLocal-421A04EA-479A-4E46-B49D-556F7144518D	locationd
2020-03-21 21:47:42+00:00	iTunes Store	thisisdfr@gmail.com		6B35410D-85C2-4DCD-823A-CE1D598597E5	com.apple.purplebuddy
2020-03-21 21:47:42+00:00	Messages	thisisdfr@gmail.com		3B180D37-7962-43E6-BF7D-139859033D1C	com.apple.identityservicesd
2020-03-21 21:47:42+00:00	CloudKit	thisisdfr@gmail.com		3B835298-47A1-458F-ADAB-ODEF5898C2F	com.apple.accounts.accountsd
2020-03-21 21:47:55+00:00	Find My Friends	thisisdfr@gmail.com		798ADEA2-0B24-4857-B19C-3CD48732B77D	com.apple.accounts.accountsd
2020-03-21 21:47:55+00:00	Device Locator	thisisdfr@gmail.com		94F572A1-6ECA-4ECC-87B3-FF927D48C7E4	com.apple.accounts.accountsd
2020-03-21 21:47:55+00:00	iMAPNotes			86186BCD-F392-48D3-8D75-4346ADE75FC8	com.apple.accounts.accountsd
2020-03-21 21:47:55+00:00	CalDAV			E9B5703B-F844-4845-AD3D-08DE58806F82	com.apple.accounts.accountsd
2020-03-21 21:47:55+00:00	CardDAV			EE84958A-E52C-425E-9171-70DEB1CB5DEB	com.apple.accounts.accountsd
2020-03-21 21:47:57+00:00	iCloud	thisisdfr@gmail.com	iCloud	1589F4EC-8F6C-4F37-929F-C6F121B36A59	com.apple.purplebuddy
2020-03-21 21:47:57+00:00	IDMS	thisisdfr@gmail.com		8F4A8F1B-DAD9-40F6-A06E-18B6A73D044F	com.apple.AuthKit
2020-03-21 21:47:58+00:00	Apple ID	thisisdfr@gmail.com		5B9A4BE7-A9AC-4798-ABEE-67EB19537748	com.apple.AuthKit

Co ciekawe mamy wgląd do wielu maili.

Apple Mail report

Total number of entries: 176  
Apple Mail located at: /home/user/Desktop/ILEAPP\_Reports\_2023-12-21\_Thursday\_232615/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/Mail

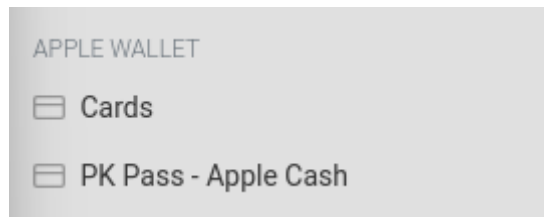
Show 15 entries

Search:

Date Sent	Date Received	Address	Comment	Subject	Summary	Read?	Flagged?	Deleted	Mailbox
2020-01-29 15:41:06+00:00	2020-01-29 15:41:07+00:00	no-reply@accounts.google.com	Google	Security alert	New device signed in to thisisdfr@gmail.comYour Google Account was just signed in to from a new Google Pixel 3 device. You're getting this email to make sure it was you. Check activity You received this email to let you know about important changes to your Google Account and services. © 2020 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.	1	0	0	imap://4FD35256-CE13-47FE-9840-EBEB5B9FD9C1/INBOX
2020-01-29 15:41:06+00:00	2020-01-29 15:41:07+00:00	no-reply@accounts.google.com	Google	Security alert	New device signed in to thisisdfr@gmail.comYour Google Account was just signed in to from a new Google Pixel 3 device. You're getting this email to make sure it was you. Check activity You received this email to let you know about important changes to your Google Account and services. © 2020 Google LLC, 1600	1	0	0	imap://4FD35256-CE13-47FE-9840-EBEB5B9FD9C1/%5BGmail%5D/%SCAilMail



Niesamowicie mamy nawet dużą część danych o nr karty i innych formach płatności.



## Cards report

Total number of entries: 1

Cards located at: /home/user/Desktop/iLEAPP\_Reports\_2023-12-21\_Thursday\_232615/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Containers/Data/Application/E58E5270-EEB1-4969-B2AA-0D1CF11B77D7/Library/Caches/com.apple.Passbook/Cache.db

Show 15 entries

Search:

Timestamp (Card Added)	Card Number	Expiration Date	Type
2020-03-21 21:53:14	4852464484724033	01/27	Visa
Timestamp (Card Added)	Card Number	Expiration Date	Type

Mamy nawet dostęp do kalendarza.

## Calendar Events report

Total number of entries: 119

Calendar Events located at: /home/user/Desktop/iLEAPP\_Reports\_2023-12-21\_Thursday\_232615/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/Calendar/Calendar.sqlitedb

Show 15 entries

Search:

Start Time	End Time	Timezone	Calendar Name	Account Name	Event Title	Location Name	Location Address	Location Coordinates	Invitation From	Invitees	Conference URL	Attachments	Notes	Crea Time
2018-01-01 00:00:00+00:00	2018-01-01 23:59:59+00:00		US Holidays	Subscribed Calendars	New Year's Day									
2018-01-15 00:00:00+00:00	2018-01-15 23:59:59+00:00		US Holidays	Subscribed Calendars	Martin Luther King, Jr. Day									
2018-02-02 00:00:00+00:00	2018-02-02 23:59:59+00:00		US Holidays	Subscribed Calendars	Groundhog Day									
2018-02-14 00:00:00+00:00	2018-02-14 23:59:59+00:00		US Holidays	Subscribed Calendars	Valentine's Day									
2018-02-16 00:00:00+00:00	2018-02-16 23:59:59+00:00		US Holidays	Subscribed Calendars	Lunar New Year									

Z kolejnych wrażliwych informacji nawet nr telefonu, na które dana osoba dzwoniła.

## Call History report

Total number of entries: 32

Call History located at: /home/user/Desktop/iLEAPP\_Reports\_2023-12-21\_Thursday\_232615/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/CallHistoryDB/CallHistory.storedata

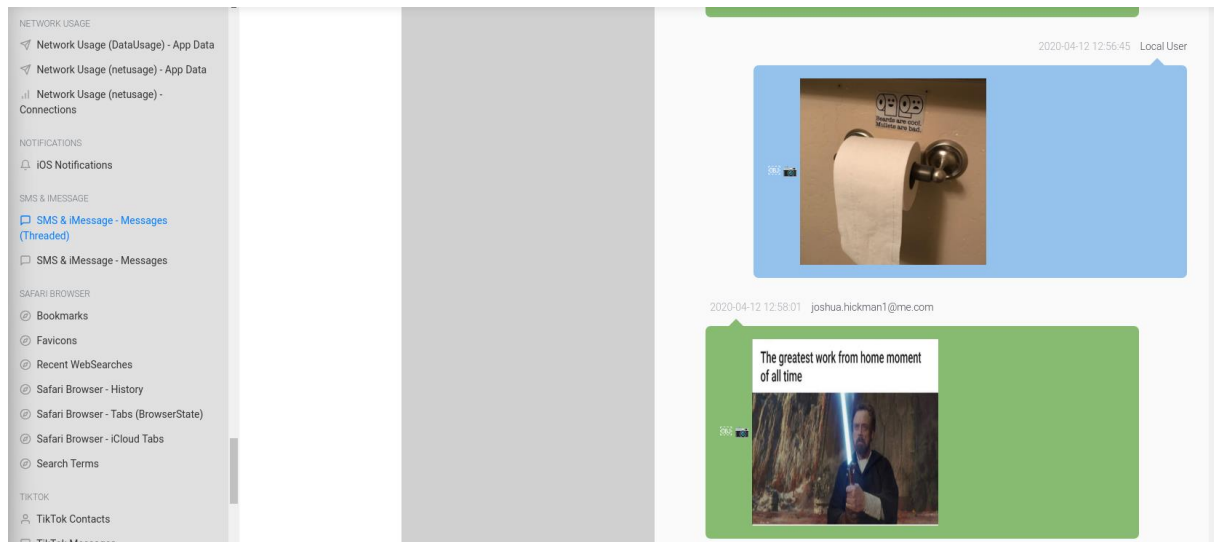
Show 15 entries

Search:

Starting Timestamp	Ending Timestamp	Service Provider	Call Type	Call Direction	Phone Number	Answered	Call Duration	FaceTime Data	Disconnected Cause	ISO Country Code	Location
2020-03-23 20:02:52+00:00	No Call Duration	com.apple.Telephony	Phone Call	Incoming	+14082560700	No	00:00:00		Rejected	US	San Jose, CA
2020-03-24 17:37:18+00:00	No Call Duration	com.apple.Telephony	Phone Call	Incoming	+14082560700	No	00:00:00		Rejected	US	San Jose, CA
2020-03-26 17:51:45+00:00	No Call Duration	com.apple.Telephony	Phone Call	Incoming	+14082560700	No	00:00:00		Rejected	US	San Jose, CA
2020-03-27 16:25:36+00:00	No Call Duration	com.apple.Telephony	Phone Call	Incoming	+14082560700	No	00:00:00		Rejected	US	San Jose, CA
2020-03-27 19:55:03+00:00	No Call Duration	com.apple.Telephony	Phone Call	Incoming	+14082560700	No	00:00:00		Rejected	US	San Jose, CA
2020-04-01 20:06:38+00:00	No Call Duration	com.apple.Telephony	Phone Call	Incoming	+14082560700	No	00:00:00		Rejected	US	San Jose, CA

Poza tym jest cała masa innych elementów. Najciekawsze z nich to:

1. Księga adresowa.
2. Informacje o koncie na Discord.
3. Informacje o rozmowach głosowych i czatach na facebook'u.
4. Dane lokalizacyjne wykorzystywane przez niektóre aplikacje.
5. Wrażliwe informacje zdrowotne z aplikacji zdrowie.
6. Dane z Instagrama i wiadomości z niego pochodzące.
7. Dostęp do wiadomości SMS! Widać nawet przesyłane memy!



8. Dostępna jest również historia przeglądania w safari.
9. Widać aplikacje otwierane na kilku ekranach w formie widżetów i wiele więcej.

Ostatnie narzędzie wykorzystywane na tym laboratorium, czyli „iLEAPP” jest naprawdę potężne. Tak naprawdę w kilka minut dostajemy z 15 GB pliku poukładane informacje, w większości możliwe do szybkiego przeglądania... To naprawdę imponujące.