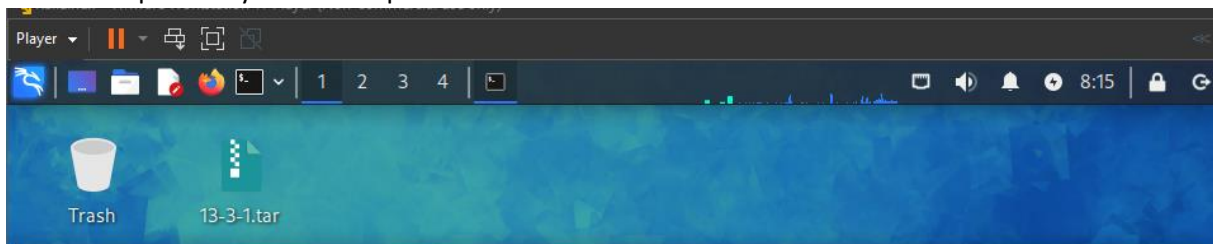


Analiza obrazu systemu IOS – Szymon Szkarłat

Celem zadania 2 projektu jest analiza obrazu systemu IOS, w tym celu posłużyłem się obrazem systemu, który analizowałem podczas wykonywania laboratorium.

Pobranie z platformy MS Teams pliku 13-3-1.tar



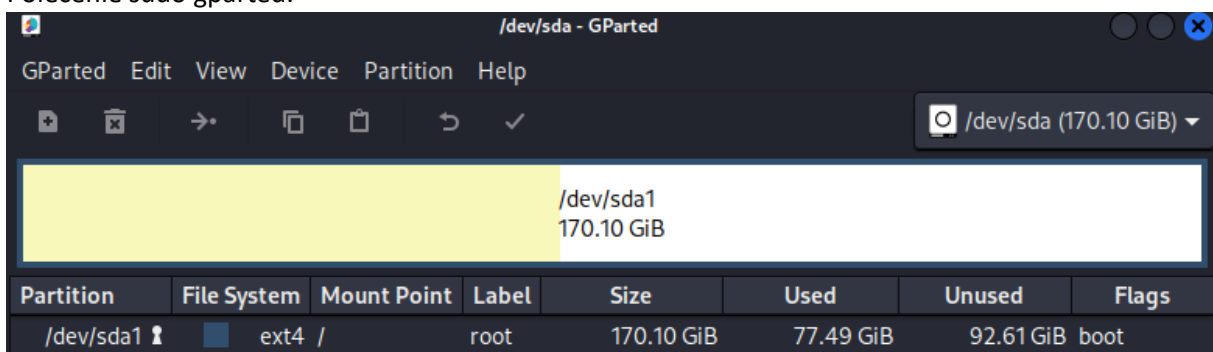
Instalacja na maszynie wirtualnej programu SQLite, przy pomocy komendy: `sudo apt-get install sqlite3`.

```
(kali@kali)-[~/Desktop]
$ sudo apt-get install sqlite3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libsqlite3-0
Suggested packages:
  sqlite3-doc
```

Rozpakowanie pliku 13-3-1.tar w systemie Linux

W związku z problemami związanymi z brakiem miejsca na dysku wirtualnej maszyny z kali Linuxem musiałem rozszerzyć pamięć dysku w ustawieniach maszyny wirtualnej. Prócz tego w systemie Linux za pomocą komendy `sudo gparted` rozszerzyłem partycję systemową, łącząc ją z niezalokowaną pamięcią. Rozszerzenie partycji systemowej przy pomocy komendy `sudo gparted`, pomogło, aby rozpakować plik z rozszerzeniem tar.

Polecenie `sudo gparted`.



Rozpakowanie pliku tar, przy pomocy komendy `tar -xvf 13-3-1.tar`

```
(kali@kali)-[~/Desktop]
$ tar -xvf 13-3-1.tar
```

```
Volumes/JOSH/NoTar-13-3-1/Applications/ActivityMessagesApp.app/_CodeSignature
Volumes/JOSH/NoTar-13-3-1/Applications/AccountAuthenticationDialog.app/_CodeS
Volumes/JOSH/NoTar-13-3-1/Applications/AccountAuthenticationDialog.app/Account
ialog
Volumes/JOSH/NoTar-13-3-1/Applications/AccountAuthenticationDialog.app/Default
Volumes/JOSH/NoTar-13-3-1/Applications/AccountAuthenticationDialog.app/Info.p
Volumes/JOSH/NoTar-13-3-1/Applications/AccountAuthenticationDialog.app/PkgInf
Volumes/JOSH/NoTar-13-3-1/Applications/AccountAuthenticationDialog.app/_CodeS
ources
```

Pobranie programu iLEAPP.

```
(kali㉿kali)-[~/Desktop]
$ git clone https://github.com/abrignoni/iLEAPP.git iLEAPP
```

```
(kali㉿kali)-[~/Desktop]
$ cd iLEAPP

(kali㉿kali)-[~/Desktop/iLEAPP]
$ ls
astc_decomp_faster-1.1.0-cp312-cp312-win_amd64.whl  ileapp.spec          requirements.txt
hook-plugin_loader.py                             LICENSE              scripts
ileappGUI.py                                       plugin_loader.py     zCaseDataExample.lcasedata
ileappGUI.spec                                    __pycache__          zProfileExample.ilprofile
ileapp.py                                          README.md
```

Doinstalowanie odpowiednich bibliotek, znajdujących się w pliku tekstowym requirements.txt.

```
(kali㉿kali)-[~/Desktop/iLEAPP]
$ pip3 install -r requirements.txt
```

Zainstalowanie programu DB Browser for SQLite.

```
(kali㉿kali)-[~/Desktop/iLEAPP]
$ sudo apt install sqlitebrowser
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
sqlitebrowser is already the newest version (3.12.2-3).
0 upgraded, 0 newly installed, 0 to remove and 1209 not upgraded.
```

Zainstalowanie programu Plistutil.

```
(kali㉿kali)-[~/Desktop]
$ sudo apt-get install libplist-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Dostanie się do odpowiedniego katalogu.

```
(kali㉿kali)-[~/Desktop]
$ cd Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/Accounts

(kali㉿kali)-[~/../var/mobile/Library/Accounts]
$
```

Otworzenie bazy danych, która znajduje się w pliku Accounts3.sqlite3.

```
(kali㉿kali)-[~/.../var/mobile/Library/Accounts]
$ sqlite3 Accounts3.sqlite
SQLite version 3.44.0 2023-11-01 11:23:50
Enter ".help" for usage hints.
sqlite>
```

Dostępne tabele w bazie danych, jest ich całkiem sporo.

```
(kali㉿kali)-[~/.../var/mobile/Library/Accounts]
$ sqlite3 Accounts3.sqlite
SQLite version 3.44.0 2023-11-01 11:23:50
Enter ".help" for usage hints.
sqlite> .table
ZACCESSOPTIONSKEY          Z_2ENABLEDDATACLASSES
ZACCOUNT                    Z_2PROVISIONEDDATACLASSES
ZACCOUNTPROPERTY           Z_4SUPPORTEDDATACLASSES
ZACCOUNTTYPE                Z_4SYNCABLEDATACLASSES
ZAUTHORIZATION              Z_METADATA
ZCREDENTIALITEM             Z_MODELCACHE
ZDATACLASS                  Z_PRIMARYKEY
Z_10OWNINGACCOUNTTYPES
sqlite>
```

Przy pomocy zapytania SELECT * FROM ZACCOUNT; udało mi się wyświetlić wiersze tabeli, które zawierały adresy email użytkowników w bazie danych.

Odpowiedzi na poszczególne pytania:

a) Ile adresów email znajduje się w analizowanej bazie danych?

```
sqlite> SELECT * FROM ZACCOUNT;
1|2|8|0|1|1|1|25||606519591.912371||Local||iTunesLocal-421A04EA-479A-4E46-B49D-556F7144518D|locationd||
2|2|57|1|1|1|1|25||606520062.043928||6B35410D-85C2-4DCD-823A-CE1D598597E5|com.apple.purplebuddy|thisisdfr@gmail.com|
3|2|73|1|1|1|1|40||606520062.507476||381B0D37-7962-43E6-BF7D-139B59033D1C|com.apple.identityservices|thisisdfr@gmail.com|
4|2|38|1|1|1|1|10||606520077.068197||iCloud||1589F4EC-8F6C-4F37-929F-C6F121B36A59|com.apple.purplebuddy|thisisdfr@gmail.com|bplist00+
5|2|13|1|1|1|1|10||606520075.27839||798A0EA2-0B24-4857-B19C-3C048732B77D|com.apple.accounts.accounts|thisisdfr@gmail.com|
6|2|44|1|1|1|1|19||606520075.243605||94F572A1-6ECA-4ECC-B7B3-FF927D48C7E4|com.apple.accounts.accounts|thisisdfr@gmail.com|
7|2|19|1|1|1|1|46||606520062.363132||38B35298-47A1-458F-ADAB-0DEF5B898C2F|com.apple.accounts.accounts|thisisdfr@gmail.com|
8|2|1|1|1|1|1|23||606520075.446426||parent||8618B8CD-F392-48D3-8D75-4346ADE75FC8|com.apple.accounts.accounts|
9|2|4|1|1|1|1|33||606520075.3066||parent||E9B5703B-F844-4845-AD3D-08DE58806F82|com.apple.accounts.accounts|
10|2|3|1|1|1|1|43||606520075.373321||parent||EE84958A-E52C-425E-9171-70DEB1CB5DEB|com.apple.accounts.accounts|
11|2|30|1|1|1|1|44||606520077.847509||8F4A8F1B-DAD9-40F6-A06E-18B6A73D044F|com.apple.AuthKit|thisisdfr@gmail.com|
12|2|26|1|1|1|1|15||606520078.027195||5B9A4BE7-A9AC-4798-A8EE-67EB19537748|com.apple.AuthKit|thisisdfr@gmail.com|
13|2|2|1|1|1|1|0|49||606520156.473805||Holiday Calendar|none||A57F9D65-8AB3-4D80-897A-70F512299C37|dataaccessd|
14|2|2|1|1|1|1|151||606520787.089834||thisisdfr@gmail.com||9B8C69AE-9F27-497B-8B94-D8AD8156181E|com.apple.AuthKit|thisisdfr@gmail.com|
15|2|4|1|1|1|1|33||606532289.45302||parent||03CF4555-027D-4CBB-87FD-462FC610F64D|com.apple.accounts.accounts|
16|2|1|1|1|1|1|23||606532289.541797||parent||CEA1DA02-7BCC-4C0B-8CB0-2677865D0E03|com.apple.accounts.accounts|
17|2|3|1|1|1|1|43||606532289.508673||parent||98491756-59C0-4798-9EB6-1714C936158F|com.apple.accounts.accounts|
18|2|37|1|1|1|1|42||606532289.572603||Gmail||4FD35256-CE13-47FE-9840-EBE85B9FD9C1|com.apple.Preferences|thisisdfr@gmail.com|
sqlite>
```

W analizowanej bazie danych znajduje się 1 unikatowy adres email.

b) Odszukany adres email to: thisisdfr@gmail.com

c) Do iCloud został podpięty adres thisisdfr@gmail.com

```
4|2|38|1|1|1|1|10||606520077.068197||iCloud||1589F4EC-8F6C-4F37-929F-C6F121B36A59|com.apple.purplebuddy|thisisdfr@gmail.com|bplist00+
```

d) Użytkownik tego systemu posiada podpięte konto Gmail, konkretnie na adres:

thisisdfr@gmail.com

```
18|2|37|1|1|1|1|42||606532289.572603||Gmail||4FD35256-CE13-47FE-9840-EBE85B9FD9C1|com.apple.Preferences|thisisdfr@gmail.com|
```

e) Wartość z tabeli ZDATE to timestampy, które reprezentują daty i godziny zdarzeń w bazie danych.

"606520075.27839" oznacza datę i godzinę zdarzenia w formie liczby zmiennoprzecinkowej, którą można przekształcić na czytelną datę i godzinę za pomocą funkcji datetime.

Dane przed przekształceniem:

```
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  
606520156.473805  
606520787.089834  
606532289.45302  
606532289.541797  
606532289.508673  
606532289.572603  
sqlite>
```

Wykonanie polecenia `SELECT datetime(ZDATE, 'unixepoch', 'localtime') FROM ZACCOUNT;`

Dane po wykonaniu polecenia:

```
sqlite> SELECT datetime(ZDATE, 'unixepoch', 'localtime') FROM ZACCOUNT;  
1989-03-21 16:39:51  
1989-03-21 16:47:42  
1989-03-21 16:47:42  
1989-03-21 16:47:57  
1989-03-21 16:47:55  
1989-03-21 16:47:55  
1989-03-21 16:47:42  
1989-03-21 16:47:55  
1989-03-21 16:47:55  
1989-03-21 16:47:55  
1989-03-21 16:47:57  
1989-03-21 16:47:58  
1989-03-21 16:49:16  
1989-03-21 16:59:47  
1989-03-21 20:11:29  
1989-03-21 20:11:29  
1989-03-21 20:11:29  
1989-03-21 20:11:29  
sqlite>
```

2. Przejście do odpowiedniego katalogu

```
(kali㉿kali)-[~/.../Containers/Shared/AppGroup/1F111E46-8DC5-4457-8C8A-31470BAB279E]  
└─$ ls  
100046799400843          lightspeed-100046799400843.db  lightspeed-uploadCache  
BreakpadExtensionCrashes lightspeed-imageCache  
Library                  lightspeed-mediaSendCache  
  
(kali㉿kali)-[~/.../Containers/Shared/AppGroup/1F111E46-8DC5-4457-8C8A-31470BAB279E]  
└─$
```

Wykonanie polecenia: sqlitebrowser na odpowiedniej bazie danych.

```
(kali@kali)-[~/.../Containers/Shared/AppGroup/1F11E46-8DC5-4457-8C8A-31470BAB279E]
$ sqlitebrowser lightspeed-100046799400843.db
```

a) ID właściciela urządzenia to: 100030845613112.

Table: _cached_participant_thread_info				
thread_key	thread_name	other_participant_profile_picture_url	other_participant_profile_picture_fallback_url	her_participant_url_expiration_timestamp
Filter	Filter	Filter	Filter	Filter
1 100030845613112	Josh Hickman	https://scontent-iad3-1.xx.fbcdn.net/v/t1.30497-1/...	/messaging/lightspeed/media_fallback/7...	1587366381

b) Podane ID należy do Josh'a Hickman'a.

c) Informacje o emoji. Jest ich 1579.

Table: emojis			
	category_idx	emoji_idx	emoji
	Filter	Filter	Filter
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	😊

```
SQL 1 x
1 SELECT count(*) as ilosc_emoji FROM emojis;
```

ilosc_emoji	
1	1579

d) W pliku znajdują się wiadomości tekstowe, w tabeli „messages”

Table: messages								
thread_key	timestamp_ms	message_id	offline_threading_id	text	sender_id	sticker_id	is_admin_message	
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	
1	100030845613112	1584888980560	mid.\$cAAAAB8r0m7N3NAPsUFxAr6kRQ1Gs	6647506190672810412	NULL	100030845613112	NULL	0
2	100030845613112	1584888655426	mid.\$cAAAAB8r0m7N3M_72QlxArmuOeCtm	6647504826973825894	NULL	100046799400843	NULL	0
3	100030845613112	1584888421780	mid.\$cAAAAB8r0m7N3M_tlfXArYdRkCW	6647503846699443618	Good question.	100046799400843	NULL	0
4	100030845613112	1584888282625	mid.\$cAAAAB8r0m7N3M_lGAVxArP9y_i5l	6647503263144748213	That's about right. Wonder if it will actual...	100030845613112	NULL	0
5	100030845613112	1584888176761	mid.\$cAAAAB8r0m7N3M_eoeVxArJOUCNEY	6647502799849443608		100046799400843	NULL	0
6	100030845613112	1584888130585	mid.\$cAAAAB8r0m7N3M_b0GVxArGrLiyWJ	6647502624680256905	Lol!!	100046799400843	NULL	0
7	100030845613112	1584887353191	mid.\$cAAAAB8r0m7N3M-sXZ1xAqXO2Uj-p	6647499364444028841	Yep!	100046799400843	NULL	0
8	100030845613112	1584887319288	mid.\$cAAAAB8r0m7N3M-q5-FxAqVjtIDCy	6647499221488906418	I see. I also see some of our previous ...	100030845613112	NULL	0
9	100030845613112	1584887217210	mid.\$cAAAAB8r0m7N3M-kEOlxArQ7EbLSe	6647498793449993374	Switched over to FB Messenger.	100046799400843	NULL	0
10	100030845613112	1581271803495	mid.\$cAAAAB8r0m7N2XGouZ1wKyTiujkpp	6632334646540388969		100046799400843	NULL	0
11	100030845613112	1580583848183	mid.\$cAAAAB8r0m7N2M2jQ91wAIOI7I2-h	6629449156733136801	NULL	100030845613112	NULL	0
12	100030845613112	1580583713711	mid.\$cAAAAB8r0m7N2M2bDr1wAIf7pnELI	6629448592717005512	NULL	100046799400843	NULL	0
13	100030845613112	1580583583877	mid.\$cAAAAB8r0m7N2M2TihVwAh9-JBTMM	6629448045635646220		100046799400843	NULL	0
14	100030845613112	1580583466974	mid.\$cAAAAB8r0m7N2M2L_3lwAh21J1jmK	6629447554949331338		100030845613112	NULL	0
15	100030845613112	1580583125918	mid.\$cAAAAB8r0m7N2M13LnlwAhH_U8KsB	6629446122764020481	I am. Thanks!	100030845613112	NULL	0
16	100030845613112	1580583078205	mid.\$cAAAAB8r0m7N2M10RPVwAhfl_ptAM	6629445930207072268	Good. Hope you are.	100046799400843	NULL	0
17	100030845613112	1580583024499	mid.\$cAAAAB8r0m7N2M1w_c1wAhb3bQ5nl	6629445701963323848	You can now call each other and see ...	100030845613112	NULL	1
18	100030845613112	1580583024443	mid.\$cAAAAB8r0m7N2M1w_O1wAhbyvO_GK	6629445696939618698	Hey, how are you?	100030845613112	NULL	0
19	100030845613112	1580582947430	mid.\$cAAAAB8r0m7N2M1sSZlwAhXL6muVm	6629445380366591334	Hi there!	100046799400843	NULL	0

e) Liczba osób biorących udział w rozmowie to 2 osoby.

ID pierwszego to: 100030845613112 oraz ID drugiego: 100046799400843.

f) Przekonwertowałem za pomocą polecenia SQL. Poniżej przedstawiono daty konwersacji.

SQL 1 ×		
1	SELECT timestamp_ms, datetime(timestamp_ms / 1000, 'unixepoch', 'localtime') as czas FROM messages;	
	timestamp_ms	czas
1	1580582947430	2020-02-01 13:49:07
2	1580583024443	2020-02-01 13:50:24
3	1580583024499	2020-02-01 13:50:24
4	1580583078205	2020-02-01 13:51:18
5	1580583125918	2020-02-01 13:52:05
6	1580583466974	2020-02-01 13:57:46
7	1580583583877	2020-02-01 13:59:43
8	1580583713711	2020-02-01 14:01:53
9	1580583848183	2020-02-01 14:04:08
10	1581271803495	2020-02-09 13:10:03
11	1584887217210	2020-03-22 10:26:57
12	1584887319288	2020-03-22 10:28:39
13	1584887353191	2020-03-22 10:29:13
14	1584888130585	2020-03-22 10:42:10
15	1584888176761	2020-03-22 10:42:56
16	1584888282625	2020-03-22 10:44:42
17	1584888421780	2020-03-22 10:47:01
18	1584888655426	2020-03-22 10:50:55
19	1584888980560	2020-03-22 10:56:20

Pliki o rozszerzeniu .plist w systemie IOS służą do przechowywania struktury danych w formie pliku XML lub binarnego pliku wiadomości. Plist to skrót od „property list”. Pliki te często są wykorzystywane do przechowywania konfiguracji, ustawień aplikacji. Pliki .plist są często używane przez aplikacje IOS do zapisywania i odczytywania danych konfiguracyjnych oraz innych danych, które są wymagane przez aplikację do poprawnego działania.

Pliki .plist w systemie IOS mogą występować w dwóch głównych formatach: XML oraz binarnym. XML – jest to czytelny dla człowieka format. Jest to forma, którą może być edytowany ręcznie za pomocą edytora tekstu, co jest przydatne podczas testowania.

Binary Property List – jest to zoptymalizowana wersja pliku .plist. Ta forma jest bardziej efektywna pod względem rozmiaru i szybkości odczytu, ale nie jest czytelna dla człowieka. Zazwyczaj jest generowana i używana w czasie wykonania przez aplikacje IOS.

Wyświetlenie informacji, które są zawarte w pliku. Podanie kilku przykładów.

```
(kali@kali)-[~/Desktop]
$ cd Volumes/JOSH/NoTar-13-3-1/private/var/preferences/SystemConfiguration

(kali@kali)-[~/../private/var/preferences/SystemConfiguration]
$ plistutil -i com.apple.wifi.plist
```

Plik „com.apple.wifi.plist” to plik konfiguracyjny na systemie IOS, który przechowuje informacje związane z ustawieniami i historią sieci Wi-Fi na urządzeniu. Zawiera dane o znanych sieciach, takie jak ich nazwy (SSID), adresy MAC punktów dostępu (BSSID), siła sygnału, historia połączeń, a także różne ustawienia dotyczące bezpieczeństwa i preferencje sieciowe. Plik ten jest istotny dla funkcji zarządzania połączeniami Wi-Fi na urządzeniu IOS, umożliwiając śledzenie historii połączeń i dostosowywanie ustawień sieciowych.

O to kilka przykładów tego co udało się znaleźć w pliku

a) DeviceUUID – unikalny identyfikator urządzenia Wi-Fi.

```
<key>DeviceUUID</key>
<string>226DE21D-BC39-476F-B693-BBF935BACECC</string>
```

b) List of known networks – lista znanych sieci Wi-Fi, z każdą siecią reprezentowaną jako słownik zawierający różne informacje o sieci.

```
<key>List of known networks</key>
<array>
  <dict>
    <key>FAST_ENTERPRISE_NETWORK_SUPPORTED_DEVICE</key>
    <true/>
    <key>ORIG_AGE</key>
    <integer>22</integer>
    <key>AUTO_INSTANT_HOTSPOT_ASSOC</key>
    <false/>
    <key>RATES</key>
    <array>
      <integer>6</integer>
      <integer>9</integer>
      <integer>12</integer>
      <integer>18</integer>
      <integer>24</integer>
      <integer>36</integer>
      <integer>48</integer>
      <integer>54</integer>
    </array>
  </dict>
</array>
```

c) SSID_STR – nazwa (SSID) konkretnej sieci Wi-Fi.

```
<integer>34</integer>
<key>SSID_STR</key>
<string>CcookiesDcastleR5 Guest</string>
<key>CAPABILITIES</key>
```

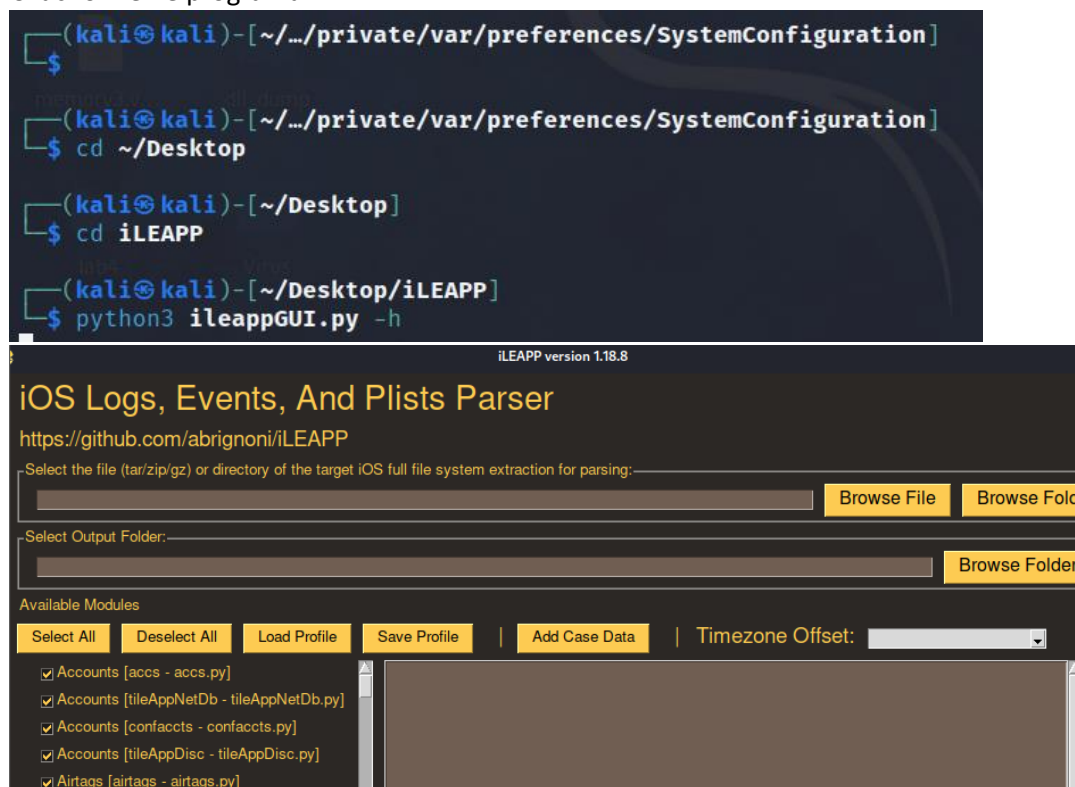
d) BSSID – adres MAC punktu dostępu dla danej sieci Wi-Fi

```
<key>BSSID</key>
<string>f8:bb:bf:90:a8:f9</string>
<key>BSSID</key>
<string>f8:bb:bf:1e:fa:f1</string>
```

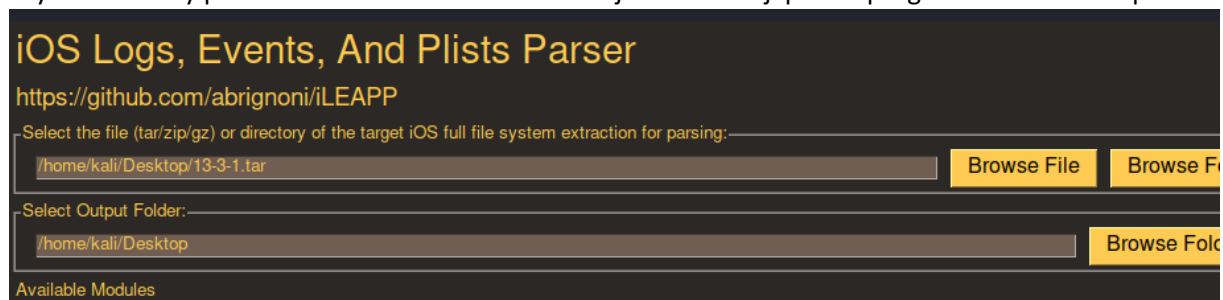
e) lastUpdate - data ostatniej aktualizacji informacji o danej sieci Wi-Fi.

```
<key>lastUpdated</key>
<date>2020-03-22T19:00:00Z</date>
```

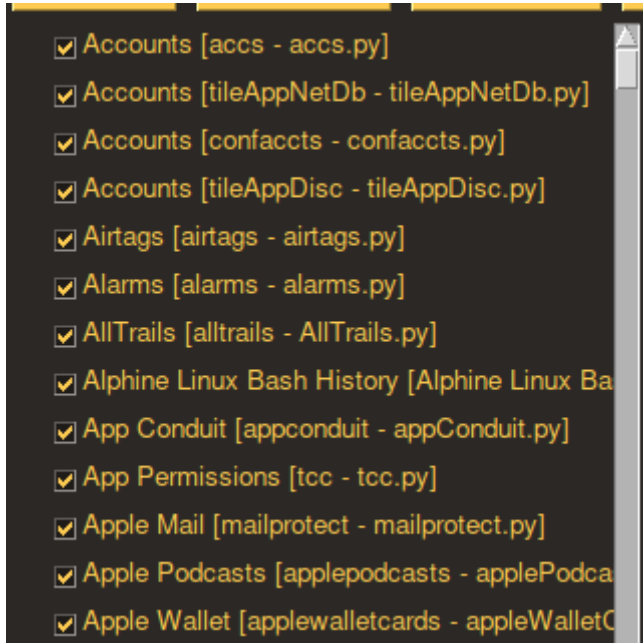
Uruchomienie programu iLEAPP



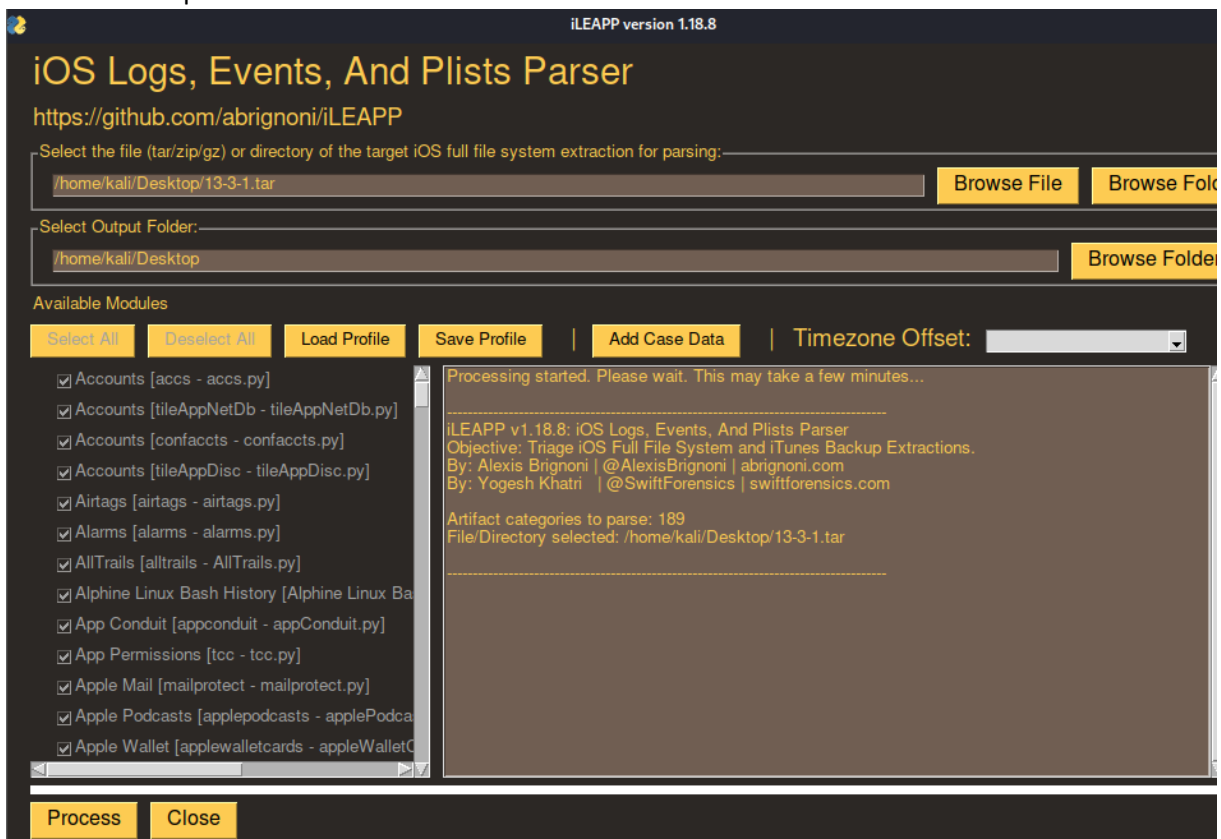
Wybranie z listy pliku 13-3-1.tar oraz ustawieni miejsca ekstrakcji pliku z programem na Desktop.



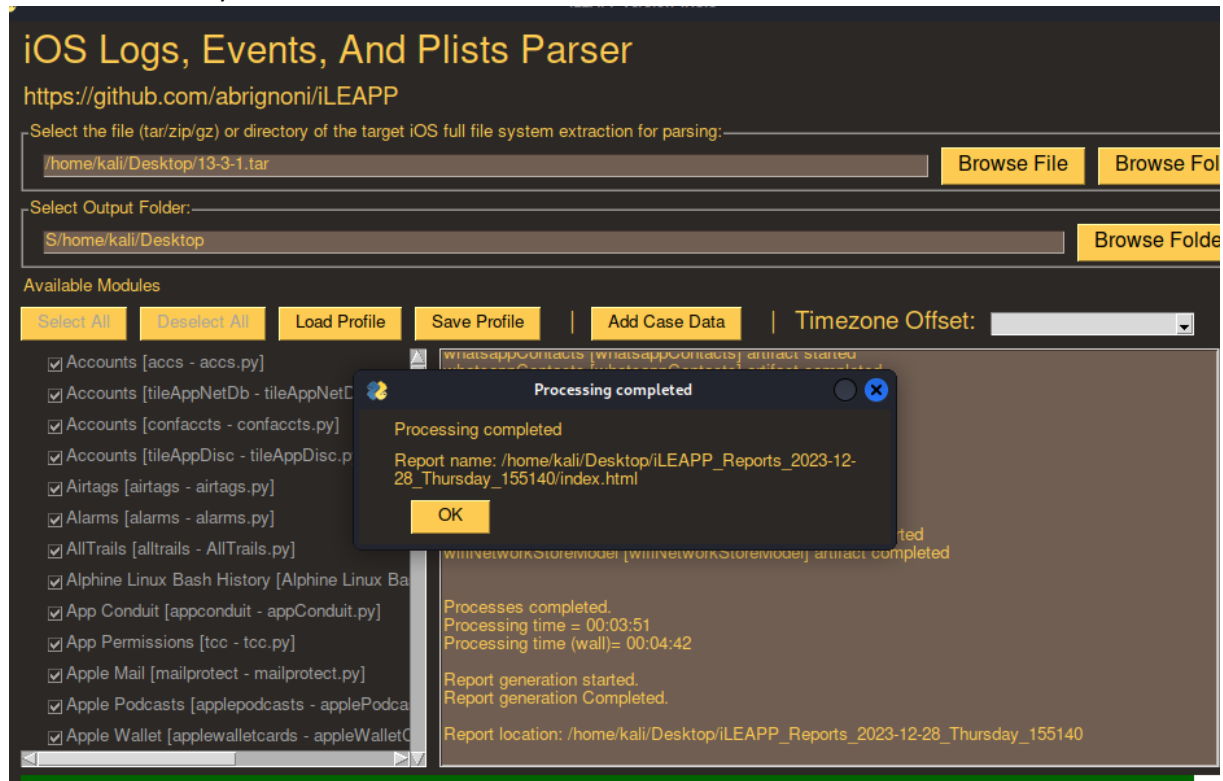
Zaznaczenie wszystkich modułów ekstrakcji danych (default).



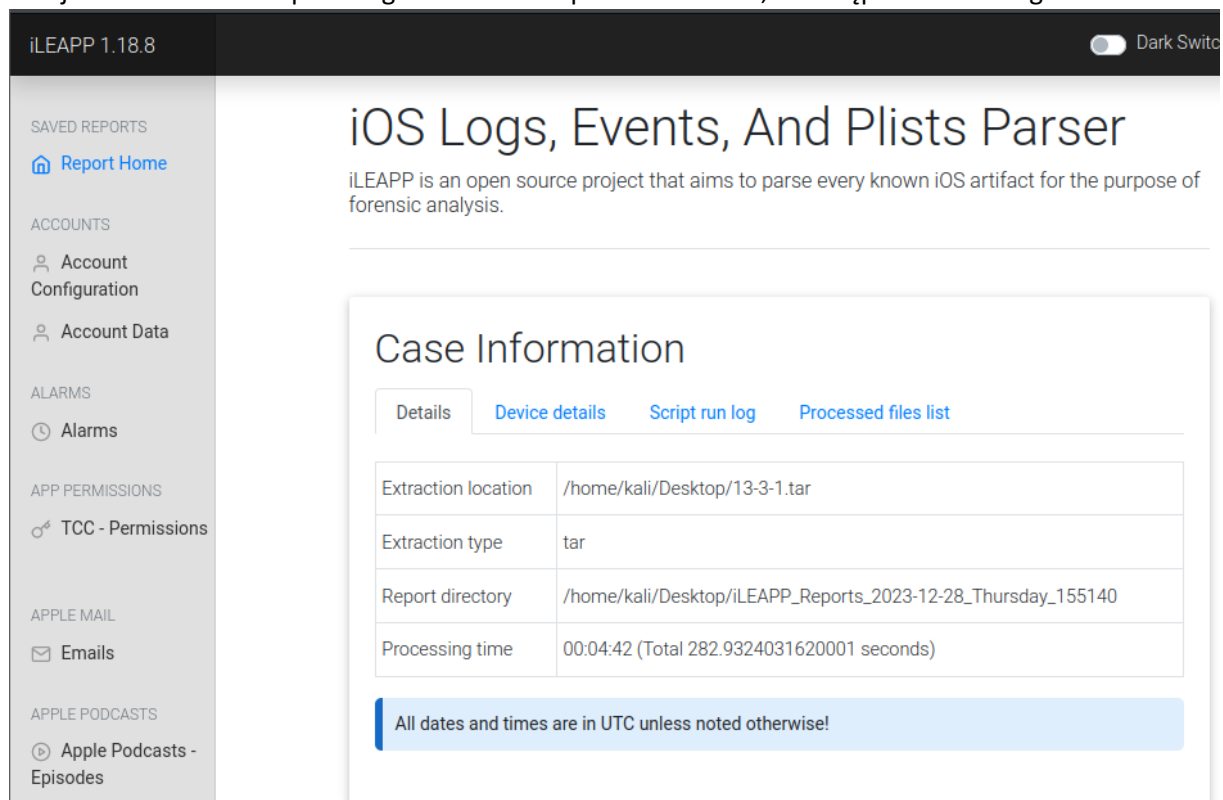
Uruchomienie procesu



Proces zakończony



Przejdźcie do folderu outputowego i odszukanie pliku index.html, a następnie otwarcie go.



Przeprowadzenie analizy raportu w oparciu o uzyskane dane. Analiza powinna składać się ze wszystkich najistotniejszych informacji m.in. o osobie, miejscu, czynności i czasie. Informacje o karcie podpiętej do telefonu.

Cards report

Total number of entries: 1

Cards located at: /home/kali/Desktop/iLEAPP_Reports_2023-12-28_Thursday_155140/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

Showing 1 to 1 of 1 entries

Previous1Next

Kalendarz

Calendar Events report

Total number of entries: 119

Calendar Events located at: /home/kali/Desktop/iLEAPP_Reports_2023-12-28_Thursday_155140/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	Creation 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									

Informacje o osobie, właścicielu urządzenia

Kik Local Account report


Kik Local Account.

Total number of entries: 1

Kik Local Account located at: /home/kali/Desktop/iLEAPP_Reports_2023-12-28_Thursday_155140/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Containers/Shared/AppGroup/52B76AC9-C286-47D5-9C26-02FF13BCD37C/cores/private/0a2545d0626b49f9bf028a413678b3fe/kik.sqlite

Show 15 entries

Search:

User ID	Display Name	Username	Profile Pic URL	Member Group ID	Administratortor Group ID	Group Tag	Group Name	Group ID	Group Pic URL	Blob	Additional Information
2	ThisIs DFIR	ThisIsDFIR									b"\n\x10\n\x0ethisisdfr_r3b\x1a\x0c\n\nThisIsDFIR"\n\n\x0bThisIs DFIR'
User ID	Display Name	Username	Profile Pic URL	Member Group ID	Administratortor Group ID	Group Tag	Group Name	Group ID	Group Pic URL	Blob	Additional Information
2020-03-27 18:43:13+00:00		This Is	DFIR							Card	2020-03-27 18:43:26+00:00
Creation Date	Thumbnail	First Name	Last Name	Phone Numbers	Email addresses	Storage Place	Modification Date				

Informacje o systemie operacyjnym

iOS Build report

Total number of entries: 9

iOS Build located at: /home/kali/Desktop/iLEAPP_Reports_2023-12-28_Thursday_155140/temp/Volu
/LastBuildInfo.plist

Show 15 entries

Key	Values
Build	Build
BuildID	E1D4AC52-39E3-11EA-97AE-3AC900CBAE32
FullVersionString	Version 13.3.1 (Build 17D50)
ProductBuildVersion	17D50
ProductCopyright	1983-2020 Apple Inc.
ProductName	iPhone OS
ProductVersion	13.3.1
SystemImageID	7E03B897-330C-432E-A4EF-B9CFF230EB14
Version	Version
Key	Values

Showing 1 to 9 of 9 entries

Tutaj mamy na przykład konwersacje pomiędzy właścicielem sprzętu (ThisIsDFIR a josh_hickmanem)

Timestamp	Sender ID	Username	Message	Video Chat Tit
2020-03-25 01:41:17.164116	22824420	josh_hickman	Clicked over to Threads. I still do not understand why this app exists.	
2020-03-25 01:43:07.262706	9368974384	ThisIsDFIR	I don't either. It makes no sense.	
2020-03-25 01:44:11.856069	22824420	josh_hickman	I just noticed Instagram throws a notification when messages are sent though here.	
2020-03-25	9368974384	ThisIsDFIR	Right But	

Poniżej przedstawiony został screen z Apple Map

Show 15 entries

Search:

Timestamp	App	Location	Short Address	Place Name	Latitude	Longitude	Search Not in Protobuf	Search Term	Search Term	Lat1	Lon1	Lat2
2020-04-01 17:45:35.736000		Manhattan Pizza, Holly Springs										
2020-04-01 17:45:35.736000		Manhattan Pizza, Holly Springs										
2020-04-01 17:45:37.503789												

Oraz sprawdzenie pogody

Weather App Locations report

Total number of entries: 3

Weather App Locations located at: /home/kali/Desktop/iLEAPP_Reports_2023-12-28_Thursday_155140/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Containers/Shared/AppGroup/A752F974-50F7-47B6-9277-55D9E37598ED/Library/Preferences/group.com.apple.weather.plist

Show 15 entries

Search:

Update Time	Name	Country	TimeZone	City Timezone Update Key	Latitude	Longitude
2020-04-12 18:34:31.134007	Santa Clara	US		1586702576.0	37.34999084472656	-121.95000457763672
2020-04-12 18:34:31.134007	New York	US		1586702576.0	40.71666717529297	-74.01667022705078
2020-04-12 18:34:31.134007	Cupertino	US		1586702576.0	37.318629	-122.029259
Update Time	Name	Country	TimeZone	City Timezone Update Key	Latitude	Longitude

Znalazłem również informację o wzroście i wadze

Show 15 entries

Search:

Height Value Timestamp	Height (in Meters)	Height (in Centimeters)	Height (Feet and Inches)
2020-04-03 18:23:55	1.7780000000000002	177	5'10"
Height Value Timestamp	Height (in Meters)	Height (in Centimeters)	Height (Feet and Inches)
2020-04-12 04:00:00	81.64	12 Stone 12 Pounds	180.00

Podsumowując, analiza systemu IOS sprawiła mi bardzo dużo radości i satysfakcji. Podczas przeprowadzanej analizy okazało się jak wiele danych jest gromadzonych na urządzeniach mobilnych, tj. smartfonach, takich jak telefony od firmy Apple. Na wcześniej wymienionych przykładach i zaprezentowanych screenach dało się zauważyć, że wszystkie informacje również z innych bezpośrednio połączonych ze smartfonem urządzeń jesteśmy w stanie zdobyć i odczytać. Mowa tu między innymi o odczytach poziomu ciśnienia we krwi czy innych parametrach medycznych, które podczas wykonywania przez posiadacza telefonu aktywności fizycznej zbierał i zapisywał połączony w wygodny sposób zegarek (smartwatch). Dodatkowo jesteśmy w stanie dostrzec podłączoną kartę bankomatową oraz dowiedzieć się o parametrach fizycznych właściciela telefonu, takich jak wzrost czy waga, które zmieniały się w czasie. Jesteśmy w stanie przejrzeć prywatne wiadomości właściciela smartfonu oraz podejrzeć jak często i na jakie kwoty dokonywał płatności kartą przy użyciu telefonu. Słowem wygoda nie zawsze idzie parą z bezpieczeństwem. Podczas analizy obrazu systemu IOS, zrozumiałem ile cennych i wrażliwych informacji jesteśmy w stanie wyciągnąć podczas jej przeprowadzania.