

## Zadanie 1 – Zawartość baz danych systemu IOS

1. Przejdź do folderu Accounts  
(~/../private/var/mobile/Library/Accounts). Otwórz bazę danych  
znajdącą się w pliku Accounts3.sqlite:

```
40960 Jan 9 15:08 Applications
8192 Jan 9 15:09 bin
0 Jan 9 14:58 boot
0 Jan 9 14:58 cores
0 Jan 9 14:58 dev
0 Jan 9 14:58 Developer
11 Jan 9 15:09 etc -> private/etc
0 Jan 9 14:58 lib
4096 Jan 9 15:09 Library
0 Jan 9 14:58 mnt
4096 Jan 9 15:01 private
8192 Jan 9 15:09 sbin
0 Jan 9 14:58 System
15 Jan 9 15:09 tmp -> private/var/tmp
4096 Jan 9 14:58 usr
11 Jan 9 15:09 var -> private/var
-1] $ cd private/var/mobile/Library/Accounts/
```

Otwieram bazę danych

```
[arek@fedora Accounts] $ sqlite3 Accounts3.sqlite
SQLite version 3.39.4 2022-09-29 15:55:41
Enter ".help" for usage hints.
sqlite> 
```

A następnie sprawdź dostępne *tables*.

```
sqlite> .tables
ZACCESSOPTIONSKEY      Z_2ENABLEDDATACLASSES
ZACCOUNT                Z_2PROVISIONEDDATACLASSES
ZACCOUNTPROPERTY       Z_4SUPPORTEDDATACLASSES
ZACCOUNTTYPE           Z_4SYNCABLEDATACLASSES
ZAUTHORIZATION         Z_METADATA
ZCREDENTIALITEM        Z_MODELCACHE
ZDATACLASS             Z_PRIMARYKEY
Z_10WNINGACCOUNTTYPES
```

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

```
sqlite> SELECT ZUSERNAME FROM ZACCOUNT;

thisisdfr@gmail.com
thisisdfr@gmail.com
thisisdfr@gmail.com
thisisdfr@gmail.com
thisisdfr@gmail.com
thisisdfr@gmail.com

thisisdfr@gmail.com
thisisdfr@gmail.com

thisisdfr@gmail.com

thisisdfr@gmail.com
```

1 unikalny

b. Podaj odszukane adres/y.

thisisdfr@gmail.com

c. Czy któryś z adresów został podpięty do iCloud? Jeśli tak, to który?

```
sqlite> SELECT ZUSERNAME,ZACCOUNTDESCRIPTION FROM ZACCOUNT;  
|Local  
thisisdfir@gmail.com|  
thisisdfir@gmail.com|  
thisisdfir@gmail.com|iCloud  
thisisdfir@gmail.com|  
thisisdfir@gmail.com|  
thisisdfir@gmail.com|  
|  
|  
|  
thisisdfir@gmail.com|  
thisisdfir@gmail.com|  
|Holiday Calendar  
thisisdfir@gmail.com|thisisdfir@gmail.com  
|  
|  
|  
thisisdfir@gmail.com|Gmail
```

Tak, thisisdfir@gmail.com

d. Czy użytkownik tego systemu posiadał podpięte konto Gmail?

tak, również ten sam email

e. Podaj wartość z tabeli ZDATE. Jaką informację skrywa ta wartość?

```
sqlite> SELECT ZUSERNAME,ZACCOUNTDESCRIPTION,ZDATE FROM ZACCOUNT;  
|Local|606519591.912371  
thisisdfr@gmail.com||606520062.043928  
thisisdfr@gmail.com||606520062.507476  
thisisdfr@gmail.com|iCloud|606520077.068197  
thisisdfr@gmail.com||606520075.27839  
thisisdfr@gmail.com||606520075.243605  
thisisdfr@gmail.com||606520062.363132  
||606520075.446426  
||606520075.3066  
||606520075.373321  
thisisdfr@gmail.com||606520077.847509  
thisisdfr@gmail.com||606520078.027195  
|Holiday Calendar|606520156.473805  
thisisdfr@gmail.com|thisisdfr@gmail.com|606520787.089834  
||606532289.45302  
||606532289.541797  
||606532289.508673  
thisisdfr@gmail.com|Gmail|606532289.572603
```

Z tego, co udało mi się wyczytać, jest to data utworzenia konta od 1 stycznia 2001 roku (w sekundach)

2. Przejdź do pliku lightspeed-100046799400843.db, otwórz go za pomocą programu DB Browser for SQLite i odpowiedz na pytania:

(/private/var/mobile/Containers/Shared/AppGroup/1F111E46-8DC5-4457-8C8A-

31470BAB279E/lightspeed-100046799400843.db - wskazany plik zawiera informacje z portalu Facebook).

```
[arek@fedora mobile] $ cd Containers/Shared/AppGroup/1F111E46-8DC5-4457-8C8A-31470BAB279E/  
[arek@fedora 1F111E46-8DC5-4457-8C8A-31470BAB279E] $ sqlite3 lightspeed-100046799400843.db  
SQLite version 3.39.4 2022-09-29 15:55:41  
Enter ".help" for usage hints.  
sqlite> .tables  
_android_mlite_message_fields  
_android_mlite_thread_key  
_bcf_ranked_contacts  
_cached_participant_thread_info  
_cached_secure_thread_read_status  
_cached_thread_read_status  
_combined_story_buckets  
_friend_story_buckets  
inbox_unit_active_contacts_with_story
```

Przechodzę do folderu i sprawdzam dostępne sekcje

a. Odszukaj ID (thread\_key) właściciela urządzenia.

```
(sqlite> SELECT participant_thread_key FROM android_mlite_thread_participant;  
ONE_TO_ONE:100030845613112  
ONE_TO_ONE:100030845613112
```

100030845613112

b. Do kogo należy thread\_key o nr 100030845613112?

```
(sqlite> SELECT participant_thread_key,display_name FROM android_mlite_thread_participant;  
ONE_TO_ONE:100030845613112|Josh
```

Do Josh'a

c. Odszukaj z bazy informacje o emoji, ile ich tam się znajduje?

```
sqlite> SELECT COUNT(*) FROM emojis;  
1579
```

1579

d. Wyświetl informacje z „messages”, czy w pliku znajdują się wiadomości tekstowe?

```
sqlite> SELECT text FROM messages;  
  
Good question.  
That's about right. Wonder if it will actually happen this year.  
  
Lol!!  
Yep!  
I see. I also see some of our previous Android 10 convo's are here.  
Switched over to FB Messenger.  
  
  
  
  
  
  
  
  
  
I am. Thanks!  
Good. Hope you are.  
You can now call each other and see information like Active Status and when you've read messages.  
Hey, how are you?  
Hi there!
```

Jak najbardziej

e. Dodatkowo określ liczbę osób biorących udział w rozmowie i podaj ich ID.

```
sqlite> SELECT sender_id,text FROM messages;
100030845613112|
100046799400843|
100046799400843|Good question.
100030845613112|That's about right. Wonder if it will actually happen this year.
100046799400843|
100046799400843|Lol!!
100046799400843|Yep!
100030845613112|I see. I also see some of our previous Android 10 convo's are here.
100046799400843|Switched over to FB Messenger.
100046799400843|
100030845613112|
100046799400843|
100046799400843|
100030845613112|
100030845613112|I am. Thanks!
100046799400843|Good. Hope you are.
100030845613112|You can now call each other and see information like Active Status and when yo
u've read messages.
100030845613112|Hey, how are you?
100046799400843|Hi there!
```

100046799400843 - pierwsza osoba

100030845613112 - druga osoba

f. Rubryka `timestamp_ms` zawiera informacje o „czasie”. Podaj w jakie dni była prowadzona rozmowa pomiędzy użytkownikami, w tym celu napisz prosty program, który przekonwertuje wybrane wiersze i wskaże ich poprawny czas wykorzystując do tego np. konsolową wersję Pythona (może być PHP, JS, itp.)

```
skrypt.py > [e] date
1  from datetime import datetime
2
3  output = "1580582947430 1580583024443 1580583024499
4
5  for date in output.split(" "):
6      print("\n" + date)
7      print(datetime.fromtimestamp(int(date)/1000))
8
```

PROBLEMS	OUTPUT	DEBUG CONSOLE	JUPYTER
OUTPUT		Code	
1580582947430 2020-03-22 15:28:39.288000			
1580583024443 2020-03-22 15:29:13.191000			
1580583024499 2020-03-22 15:42:10.585000			
1584888176761 2020-03-22 15:42:56.761000			
1584888282625 2020-03-22 15:44:42.625000			
1584888421780 2020-03-22 15:47:01.780000			
1584888655426 2020-03-22 15:50:55.426000			
1584888980560 2020-03-22 15:56:20.560000			

Była prowadzona w 1 i 9 lutego oraz 22 marca 2020



## Zadanie 2 – Pliki plist

### 1. Opisz do czego służą w systemie IOS pliki o rozszerzeniu .plist?

Plist - Property List file. Są w niej zawarte informacje działania systemu, w tym np. konfiguracja systemów firmy Apple.

### 2. Do jakiej postaci można konwertować ww. pliki?

Przykładowo ASCII, XML, pliku binarnego

Warto zaznaczyć że struktura tych plików bardzo przypomina strukturę XML'ów lub jsonów właśnie

### 3. Przy pomocy programu Plistutil wyświetl informacje zawarte w pliku i odpowiedz na pytanie, jakie informacje znajdują się wewnątrz badanego pliku (podaj kilka przykładów).

```
[arek@fedora SystemConfiguration] $ plistutil -i com.apple.accounts.exists.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>com.apple.account.Google.count</key>
  <integer>1</integer>
  <key>com.apple.account.DeviceLocator.exists</key>
  <integer>1</integer>
  <key>com.apple.account.iTunesStore.count</key>
  <integer>2</integer>
  <key>com.apple.account.AppleAccount.exists</key>
  <integer>1</integer>
  <key>com.apple.account.FindMyFriends.count</key>
  <integer>1</integer>
  <key>com.apple.account.IMAPNotes.exists</key>
  <integer>1</integer>
  <key>com.apple.account.AppleAccount.count</key>
  <integer>1</integer>
  <key>com.apple.account.IdentityServices.exists</key>
  <integer>1</integer>
  <key>com.apple.account.HolidayCalendar.exists</key>
  <integer>1</integer>
  <key>com.apple.account.GameCenter.count</key>
  <integer>1</integer>
  <key>com.apple.account.DeviceLocator.count</key>
  <integer>1</integer>
  <key>com.apple.account.AppleIDAuthentication.exists</key>
  <integer>1</integer>
  <key>com.apple.account.IMAPNotes.count</key>
  <integer>2</integer>
  <key>com.apple.account.CloudKit.count</key>
  <integer>1</integer>
  <key>com.apple.account.iTunesStore.exists</key>
```

Przykładowo aplikacje i usługi będące preinstalowane na urządzeniach

Informację o protokole eapol dla karty sim

```
[arek@fedora SystemConfiguration] $ plistutil -i com.apple.eapol.sim.generation.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>SIMGenerationID</key>
  <integer>1</integer>
</dict>
</plist>
```

## Tryb samolotowy

```
[arek@fedora SystemConfiguration] $ plistutil -i com.apple.radios.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>AirplaneMode</key>
    <true/>
</dict>
</plist>
```

Zawiera listę zapisanych sieci wifi, datę połączenia, id urządzenia, BSS, adres MAC, również informację o zmianie hasła wifi albo próby połączenia do hot-spotu, aktualizację OTA

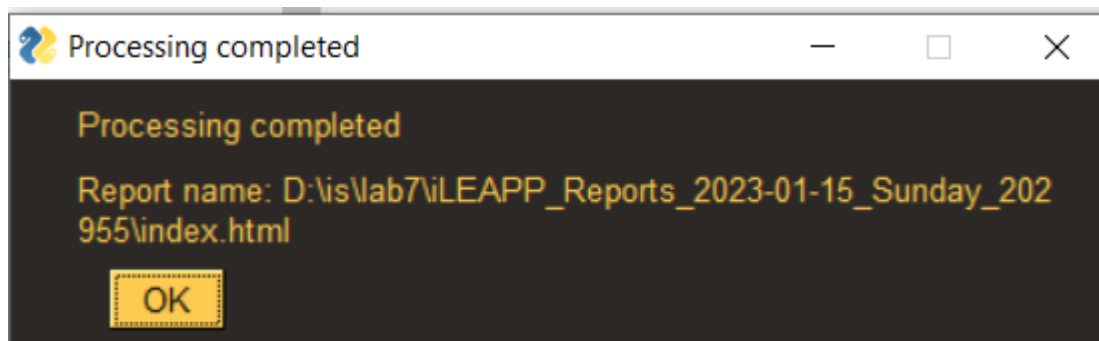
```
[arek@fedora SystemConfiguration] $ plistutil -i com.apple.wifi.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>DeviceUUID</key>
    <string>226DE21D-BC39-476F-B693-BBF935BACECC</string>
    <key>LoggingFileEnabled</key>
    <false/>
    <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>
            <key>IE</key>
            <data>
BwpVUyBkDB6VBR4AMBQBAAAPrAQBAAAPrAQBAAAPrAIMAC0a7wIb
//8AAAAAAAAAAAAAAAAAAAAAAAAA9FqEFBAAAAAAAAAAAAAAAA
AAAAAAAAAB/CAQAAAAAAAAABVwyY0YAZ+v8AAPr/AADABQG6bAPz/
</data>
            <key>CaptiveNetwork</key>
            <false/>
            <key>SNR</key>
            <integer>34</integer>
            <key>SSID_STR</key>
            <string>CcookiesDcastleR5 Guest</string>
            <key>CAPABILITIES</key>
            <integer>17</integer>
        </dict>
    </array>
</dict>
</plist>
```

```
<dict>
  <key>CHANNEL</key>
  <integer>1</integer>
  <key>lastRoamed</key>
  <date>2020-04-10T20:04:15Z</date>
  <key>beaconLossCount</key>
  <integer>0</integer>
  <key>trigDisconnectCount</key>
  <integer>0</integer>
  <key>BSSID</key>
  <string>f8:bb:bf:8d:b9:c9</string>
  <key>CHANNEL_FLAGS</key>
  <integer>10</integer>
```

### Zadanie 3 – Automatyzacja analizy plików systemu IOS

Uruchamiam program

Procesowanie przeszło pomyślnie!



# 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

Jak widać na powyższym screenshocie, dalszej analizie zostanie poddane urządzenie z systemem iOS 13.3.1

A sam użytkownik nazywa się **Josh Hickman**

## Lista odnalezionych informacji

Warto na wstępie zaznaczyć iż program wydobył naprawdę sporo informacji - ta liczba jest aż zatrważająca!

Do dyspozycji są m.in. następujące kategorie:

- książka adresowa
- historia połączeń
- alarmy
- zainstalowane aplikacje
- uprawnienia aplikacji
- apple: podcasts/wallet/carplay
- bluetooth
- kalendarz
- aplikacje: Discord/Facebook/Instagram/Kik/TikTok/Venmo/Whatsapp
- geolokalizacja
- zdrowie
- iOS build
- iTunes backup
- załączniki
- klawiatura
- powiadomienia
- zdjęcia
- zakładki i wyszukiwania w przeglądarce Safari
- emaile
- dokładną listę zainstalowanych aplikacji na każdym z pulpitów

# Książka adresowa, Call History

Show15entries

Search:

Contact ID	Contact Number	First Name	Middle Name	Last Name	Email Address	Creation Date	Modification Date	Storage Place
1	+19195790479	Josh		Hickman	joshua.hickman1@me.com	2020-03-22 01:11:33	2020-03-27 18:44:01	Address Book
2		This is		DFIR		2020-03-27 18:43:13	2020-03-27 18:43:26	Card
Contact ID	Contact Number	First Name	Middle Name	Last Name	Email Address	Creation Date	Modification Date	Storage Place

Niestety nasz użytkownik nie ma zbyt wiele kontaktów - jedynie do samego siebie - numer telefonu i adres e mail, chociaż w logach połączeń istnieje znacznie więcej wpisów

Timestamp	Phone Number	Name	Answered	Call Type	Call Direction	Call Duration	ISO Country Code	Location
2020-03-23 20:02:52	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA
2020-03-24 17:37:18	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA
2020-03-26 17:51:45	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA
2020-03-27 16:25:36	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA
2020-03-27 19:55:03	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA
2020-04-01 20:06:38	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA
2020-04-03 16:10:54	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA
2020-04-05 20:42:18	9197627808		No	Phone	Outgoing	00:00:23	US	Fuquay-Varina, NC
2020-04-06 20:34:33	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA
2020-04-06 21:48:08	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA
2020-04-06 22:43:00	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA
2020-04-07 18:10:42	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA
2020-04-07	+14082560700		No	Phone	Incoming	00:00:00	US	San Jose, CA

Timestamp	Phone Number	Name	Answered	Call Type	Call Direction	Call Duration	ISO Country Code	Location	Service Provider
2020-04-12 14:04:06	9192853680		No	Phone	Outgoing	00:01:04	US	Fuquay-Varina, NC	com.apple.Telephony
2020-04-12 15:26:43	joshua.hickman1@me.com		No	FaceTime Video	Outgoing	00:01:38		<<RecentsNumberLocationNotFound>>	com.apple.FaceTime

Co ciekawe, jest dostępna dokładna długość połączeń

## Płatności

Cards located at: D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_Sunday\_202955\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

Show15entries

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

Obawiający jest fakt, że można wydobyć tak poufne informacje jak numer karty kredytowej osoby wraz z datą upływu! Przez skompromitowaniem owej karty brakuje jedynie 3

cyfrowego kodu cvv - a to dosyć mała liczba kombinacja co pozwala na próbę ręcznego wpisania kodu z nie tak małą szansą na powodzenie.  
Zastanawiające jest, czemu system przetrzymuje takie informacje, a tym bardziej dlaczego nie w sposób zaszyfrowany

Venmo - Transactions report

Total number of entries: 30

Venmo - Transactions located at: D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_Sunday\_202955\temp\Volumes\JOSH\NoTar-13-3-1\private\var\mobile\Containers\Data\Application\C2E351B4-35D5-461E-AC96-3D20CB4ED5CB\Documents\PublicFeed\...\D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_Sunday\_202955\temp\Volumes\JOSH\NoTar-13-3-1\private\var\mobile\Containers\Data\Application\C2E351B4-35D5-461E-AC96-3D20CB4ED5CB\Documents\FriendsFeed

Show 15 entries

Search:

Date Created	Date Completed	Action	Payer	Payer ID	Receiver	Receiver ID	Note	Amount	Status	Audience	Type	Context
2019-11-01 01:56:26	2019-11-01 01:56:26	pay	Joshua Hickman	Josh-Hickman-19	Joshua Hickman	Thisis-DFIR	For the testing stuff. My first payment.	5	settled	private	payment	Joshua Hickman paid Joshua Hickman 5
2019-11-02 17:23:55	2019-11-02 17:23:55	pay	Joshua Hickman	Thisis-DFIR	Joshua Hickman	Josh-Hickman-19	Test stuff.	7.5	settled	friends	payment	Joshua Hickman paid Joshua Hickman 7.5
2019-11-03 17:06:39	2019-11-03 17:06:39	pay	Joshua Hickman	Josh-Hickman-19	Joshua Hickman	Thisis-DFIR	Chipotle guacamole!	2.5	settled	private	payment	Joshua Hickman paid Joshua Hickman 2.5

Również jest dostępna dokładna historia transakcji aplikacji Venmo  
Można zobaczyć ile, na co i kiedy użytkownik wydał pieniądze

## Bluetooth

Address
Public D8:E0:E1:3D:C3:99
Random FC:A9:DC:81:CC:6E
Random CA:3A:88:36:38:4A
Random E7:FC:DD:92:F4:B5
Random EA:1E:66:65:28:41
Random C0:B9:B5:A5:AA:7D
Public 28:39:5E:7F:8B:C1
Random E3:21:BC:AE:58:CF
Random D5:68:1A:28:D6:D8
Public 38:EC:0D:E0:61:D0
Public 28:F0:76:3E:79:09
Public F8:04:2E:88:1F:C5
Public 70:48:0F:E5:8F:3F
Public 78:D2:94:99:7C:55
Public 68:64:4B:3E:C9:43

Można również znaleźć informację o adresach sprzętowych urządzeń podłączonych za pomocą protokołu bluetooth

UUID	Name	Name Origin	Address	Resolved Address	Last Connection Time
169D0C0E-D1D9-C5D7-27DB-374F753EEA47	Charge 3	2	Public C4:B4:5E:16:B5:E9	Public C4:B4:5E:16:B5:E9	270
73B2841A-1840-E495-76C5-5D18504668F3	Hue Lamp	2	Random EA:35:1F:3B:98:CC	Random EA:35:1F:3B:98:CC	1226
7ECE723E-8F05-B882-A2BE-0AD5D11A117D	Hue Lamp	2	Random EE:86:C3:D5:EF:C3	Random EE:86:C3:D5:EF:C3	1227
7F2A3B52-02BB-560A-D57B-3345F0BE875B	Office	2	Public D4:A3:3D:64:E4:43	Public D4:A3:3D:64:E4:43	711
9978D8CC-BD39-0371-FE07-9BE1C48AB0DE	This Is's Apple Watch	2	Random 63:B0:ED:30:A1:CF	Public F8:6F:C1:4E:FF:6A	274

MAC Address	Name Key	Name
B4:EC:02:73:FF:93		
F8:6F:C1:4E:FF:6A		Apple Watch
7C:04:D0:89:89:A0		Josh's AirPods
38:EC:0D:E2:49:CF	This Is's AirPods Pro	AirPods Pro

A urządzenia, które zostały podłączone to:

- Charge 3 - prawdopodobnie głośnik firmy JBL

- Hue Lamp
- Office - możliwe, że urządzenie z biura z pracy
- This Is's Apple Watch
- Josh's AirpoDs
- This Is's AirPods Pro

## Connected Devices

Z tej zakładki, można się dowiedzieć, że użytkownik posiada też urządzenie Mac mini

### Connected Devices report

Total number of entries: 1

Connected Devices located at: D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_Sunday\_202955\temp\Volumes\JOSH\NoTar-13-3-1\private\var\mobile\Media\iTunes\_Control\iTunes\iTunesPrefs

Show  entries

User & Computer Names
Joshua Hickman - Joshua's Mac mini Joshua Hickman - Joshua's Mac mini Joshua Hickman - Joshua's Mac mini

## Wiadomości

Jedną z zakładek, z której można się dowiedzieć najwięcej o użytkowniku, są właśnie wiadomości różnych programów - SMS'ów, Discorda, Facebooka, Whatsapp, Tiktoka. Jest to o tyle niepokojące, iż wiadomości nie były w żaden sposób szyfrowane, i są dostępne plaintextem.



# Discord Messages report

Total number of entries: 10

Discord Messages located at: D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_S1\private\var\mobile\Containers\Data\Application\237E0C71-5961-459

Show 15 entries

Timestamp	Edited Timestamp	Username	Bot?	Content
2020-02-01T01:39:39.931000+00:00		ThisIsDFIR		Well hello there.
2020-02-01T02:09:38.714000+00:00		ThisIsDFIR		Thanks!
2020-02-01T01:41:07.748000+00:00		josh_hickman1		Hey there! Thanks for helping out.
2020-03-22T13:12:22.413000+00:00		ThisIsDFIR		Got it. Thank you!
2020-03-22T13:07:53.078000+00:00		ThisIsDFIR		Good morning. How are you? The pollen is in full force so my

Z wiadomości z Discorda, można się dowiedzieć, że Josh ma uczulenie na pyłki kwiatowe

Good morning.  
How are you? The pollen is in full force so my allergies are kicking!

Były wykonywane również połączenia głosowe na Messengerze

Timestamp	Sender Name	Sender ID	Call Type	Call Duration/Subtitle
2020-02-01 19:01:53	ThisIs Dfir	100030845613112	Audio Call	1 min
2020-02-01 19:04:08	Josh Hickman	100030845613112	Video Chat	1 min
2020-03-22 14:50:55	ThisIs Dfir	100030845613112	Audio Call	1 min
2020-03-22 14:56:20	Josh Hickman	100030845613112	Video Chat	1 min

# Facebook Messenger - Chats report

Total number of entries: 15

Facebook Messenger - Chats located at: D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_Sunday\_202955\temp\Volume1\private\var\mobile\Containers\Shared\AppGroup\1F111E46-8DC5-4457-8C8A-31470BAB279E\lightspeed

Show 15 entries

Timestamp	Sender Name	Sender ID	Message
2020-02-01 18:50:24	Josh Hickman	100030845613112	You can now call each other and see information like Active Status and when you've read messages.
2020-03-22 14:29:13	ThisIs Dfir	100030845613112	Yep!
2020-03-22 14:44:42	Josh Hickman	100030845613112	That's about right. Wonder if it will actually happen this year.
2020-03-22 14:26:57	ThisIs Dfir	100030845613112	Switched over to FB Messenger.
2020-03-22 14:42:10	ThisIs Dfir	100030845613112	Lol!!
2020-03-22 14:28:39	Josh Hickman	100030845613112	I see. I also see some of our previous Android 10 convo's are here.
2020-02-01 18:52:05	Josh Hickman	100030845613112	I am. Thanks!
2020-02-01 18:49:07	ThisIs Dfir	100030845613112	Hi there!
2020-02-01 18:50:24	Josh Hickman	100030845613112	Hey, how are you?
2020-02-01 18:51:18	ThisIs Dfir	100030845613112	Good. Hope you are.

W przypadku messenger'a są tu dostępne zwykłe/codzienne wiadomości

Co ciekawsze, jest również zakładka, gdzie znalazły się zaszyfrowane wiadomości Facebooka -

## Facebook Messenger - Secret Conversation report

Total number of entries: 5

Facebook Messenger - Secret Conversation located at: D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_Sunday\_202955\temp\Volumes\JOSH\NoTar-13-3-1\private\var\mobile\Containers\Shared\AppGroup\1F111E46-8DC5-4457-8C8A-31470BAB279E\lightspeed-100046799400843.db

Show 15 entries

Search:

Timestamp	Thread Key	Sender Name	Message (Encrypted)
2020-04-12 02:23:14	100030845613112	ThisIs Dfir	AKNjqvWw3Si8+i11WqpBHffKhfDpBTvmCrxuWQOhY5UDS7+K86Pd6x5486/b3YpMH5ukYRSRxp000rhwbTwkIjgPHAesZ2FjHTQG48g5YcdZNELxjX3srqmQEXyig==
2020-04-12 02:24:37	100030845613112	Josh Hickman	AOyKswF+3M4D3yyTh4uUTRvIEKaUV4659FZwDqcBi5CMJUSOCmFfAdR+gHh/267oJdINzpGFKshx+f8dbSnoXy838ucgQB3dWQuMHgDDF8lN/69EMv3oAtIQ1OYf/+tPu+NreEU/Lk1
2020-04-12 02:25:38	100030845613112	ThisIs Dfir	AHB5zky0NyxW/twXnDFWcljN7f7tRtYNUQl6Mguz8OfzT//91NO68XPW8ACiix0NEpLDxcMthqu+UIFsQBn72s=

Timestamp	Sender ID	Username	Video Chat Title	Video Chat ID
2020-03-25 01:57:22.525579	9368974384	ThisIsDFIR	You started a video chat	18135998026062170
2020-03-25 01:57:39.820195	9368974384	ThisIsDFIR	Video chat ended	18135998026062170
2020-03-25 01:59:30.471154	22824420	josh_hickman	josh_hickman started a video chat	18135998146062170
2020-03-25 02:00:51.747248	22824420	josh_hickman	Video chat ended	18135998146062170

## Połączenia wideo na instagramie wraz z ich ID

Timestamp	Sender ID	Username	Message
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 01:46:24.285569	9368974384	ThisIsDFIR	Right. But not necessarily the other way around. The person has to be in the close

## Oraz Whatsapp

Timestamp	Sender Name	From ID	Receiver	To ID	Message
2020-03-26 18:42:57	Local User		Josh Hickman	19195790479@s.whatsapp.net	What's up?!
2020-03-26 18:47:12	Local User		Josh Hickman	19195790479@s.whatsapp.net	Not yet but the effects of this will be felt later I'm sure.
2020-03-26 18:43:48	Josh Hickman	19195790479@s.whatsapp.net	Local User		Not much. Just waiting to hop on a conference call. You?
2020-03-27 00:37:02	Local User		Josh Hickman	19195790479@s.whatsapp.net	My turn.
2020-03-27 00:36:36	Josh Hickman	19195790479@s.whatsapp.net	Local User		Lol!!
2020-03-26 18:46:05	Josh Hickman	19195790479@s.whatsapp.net	Local User		Awesome. I bet you guys are busy with everyone working from home.
2020-03-26 18:44:44	Local User		Josh Hickman	19195790479@s.whatsapp.net	A little busy. Finished one report this morning and going to start a second one in a few minutes.

## Files App - Filenames

### Files App - Filenames report

Files App - Files stored in the "On my iPad" area.

Total number of entries: 1

Files App - Filenames located at: D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_Sunday\_202955\temp\Volumes\JOSH\NoTar-13-3-1\private\var\mobile\Containers\Shared\AppGroup\44B9D016-1D98-43A5-A968-F0F8F9AAECCD\smartfolders.db

Show 15 entries

Search:

Last Hit Date	Folder ID	Filename	Frequency at Last Hit Date	Creation Date	Modification Date	User Info	Child Item Count	Flags
2020-04-12 15:22:19.983254	i6305c	iOS_Bug_Reporting_for_Forensic_Purposes_1,2	1.0	2020-03-28 01:45:15	2020-03-28 01:49:10	{'csbm': 0, 'zid': 1, 's': 0, 'pzid': 1, 'cs': 0, 'cstrm': 0}	2	{'_userExecutable': False, '_userWritable': True, '_hidden': False, '_pathExtensionHidden': True, '_userReadable': True}

Josh próbował również swoich sił w zgłaszaniu bugów programu

## Geolokalizacja

Cała historia lokalizacji użytkownika ma miejsce w Stanach Zjednoczonych -> Holly Springs

2020-04-12 13:55:55	hndl-7e4b57fc9784ad7da1d7509c59bffd6b	muid- 7247590733274866017	2020-04-13 01:55:55	com.apple.Maps" <a href="#">Manhattan Pizzab!</a> http://www.manhattanpizza.comR Holly Springs: 9G_W A@A>9 pizza America/New_York: \tn=address\ 305 \tn=normal\ Matthews Drive* 1586073988222' \$fa50d7bb-0bff-47a1-92a6-0b8af3c27bb2 305 Matthews DrZ \tn=normal\b- en-us 305 Matthews Dr fooddrinks \tn=normal\ Matthews DriveZ8 en" Holly Springs, NC 27540Z A@1aL Pizza* North Carolina* poiJ Matthews DriveZ Pizza* fromLegacy" Holly Springs0 \$6F5522DB-E2CC-42A4-A4AF-4F4CB8328983
------------------------	---------------------------------------	------------------------------	------------------------	--

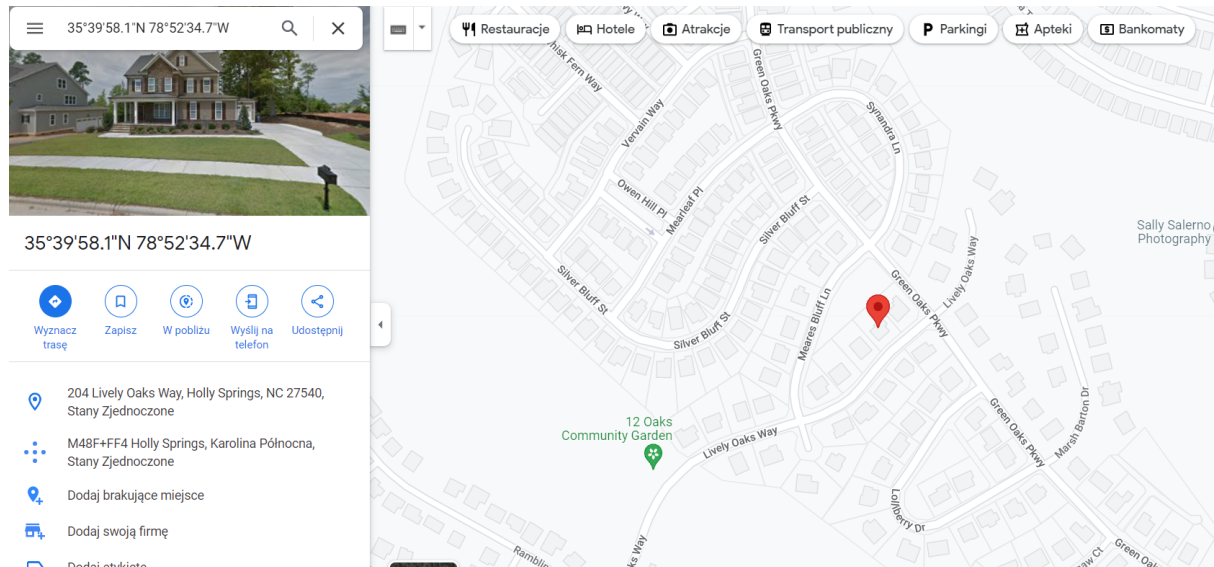
2020-04-12 13:59:06		12 Oaks Country Club	
2020-04-12 13:59:06			
2020-04-12 13:59:06			
2020-04-12 13:59:10		Woods Creek Rd	

		WOODS CREEK RD
2020-04-12 13:59:10		Woods Creek Rd
2020-04-12 13:57:53		Woodfield Dead End Rd, Woods Creek Rd
2020-04-12 13:58:11		Woodfield Dead End Rd, Woods Creek Rd
		Willow Springs Elem SCH Park
2020-04-05 20:33:35		Western Union
		Walmart Neighborhood Market, Whole Foods Market
		Wake County Convenience Center
		Vista Point On Jordan Lake
2020-04-12 14:03:32		Utley Creek, White Oak Creek
		Tricity Family Medicine & Urgent Care Clinic
2020-04-01 17:52:44		Traci Huffman Photography
2020-04-01 17:49:16		Home Grown Pizza, Pierce Group Benefits
2020-04-01 17:47:49		Home Grown Pizza
2020-04-01 17:45:43		Holly Springs Taxi, Veterans Park
2020-04-01 17:46:47		Holly Springs Taxi
2020-04-05 20:43:19		Holly Springs High School, Sheetz
2020-04-05 20:36:54		Holly Springs Food Cupboard
2020-04-05 20:37:34		Holly Springs Food Cupboard

Miejsca, które odwiedza użytkownik

- Pizzeria Manhattan
- Woods Creek Rd
- Holly Springs High School
- Holly Springs Food Cupboard
- Veterans Park
- 

Warto zaznaczyć iż okres szczególnej aktywności przypada na kwiecień 2020



## Zdrowie

W tej zakładce można się dowiedzieć naprawdę sporo a propos sytuacji zdrowotnej Josha

Start Timestamp	End Timestamp	Type	Heart Rate
2020-03-22 00:52:59	2020-03-22 00:52:59	Heart Rate	73.0
2020-03-22 00:57:17	2020-03-22 00:57:17	Heart Rate	71.0
2020-03-22 01:00:10	2020-03-22 01:00:10	Heart Rate	69.0
2020-03-22 01:06:03	2020-03-22 01:06:03	Heart Rate	65.0
2020-03-22 01:10:31	2020-03-22 01:10:31	Heart Rate	57.0
2020-03-22 01:16:36	2020-03-22 01:16:36	Heart Rate	61.0
2020-03-22 01:19:31	2020-03-22 01:19:31	Heart Rate	65.0
2020-03-22 01:23:40	2020-03-22 01:23:40	Heart Rate	60.0
2020-03-22 01:29:52	2020-03-22 01:29:52	Heart Rate	63.0
2020-03-22 01:33:31	2020-03-22 01:33:31	Heart Rate	61.0
2020-03-22 01:40:23	2020-03-22 01:40:23	Heart Rate	65.0
2020-03-22 01:47:27	2020-03-22 01:47:27	Heart Rate	62.0
2020-03-22 01:52:11	2020-03-22 01:52:11	Heart Rate	63.0
2020-03-22 01:56:49	2020-03-22 01:56:49	Heart Rate	67.0
2020-03-22 01:58:33	2020-03-22 01:58:33	Heart Rate	61.0



Start Timestamp ↕	End Timestamp ↕	Workout Type ↕	Workout Duration ↕	Duration (In Mintues) ↕	Distance (In KM) ↕	Distance (In Miles) ↕	Calories Burned ↕	Total Basel Energy Burned ↕	Goal Type ↕
2020-03-27 18:57:39	2020-03-27 19:15:39	RUNNING	00:18:00	18.002008283138274	3.2479800059968365	2.0182005843062605	208.57206077784014	26.335517881735733	OPEN
2020-03-28 14:41:25	2020-03-28 14:58:44	RUNNING	00:17:19	17.321344498793284	3.235360245681312	2.0103590312192425	203.1070299221264	25.337790344788736	OPEN
2020-03-30 12:44:04	2020-03-30 13:10:35	RUNNING	00:26:31	26.51777028242747	4.845504469437863	3.010855957679074	302.5802317267029	38.851842234397	OPEN
2020-03-31 18:58:47	2020-03-31 19:24:59	RUNNING	00:26:12	26.20422958334287	4.864848439344114	3.0228757396036916	302.8614065541439	38.32172323992147	OPEN
2020-04-02 17:36:41	2020-04-02 18:02:31	RUNNING	00:25:50	25.838798115650814	4.853044262344192	3.015540966337073	301.88919753776554	37.96722736353608	OPEN
2020-04-03 19:11:28	2020-04-03 19:37:49	RUNNING	00:26:20	26.3498759329319	4.8627497677395874	3.021571685930115	369.85077135753846	46.00887820267365	OPEN

Start Timestamp ↕	End Timestamp ↕	Decibels ↕	Bundle Name ↕	Device Name ↕	Device Manufacturer ↕	Device Model ↕	Local Identifier ↕	Key ↕
2020-03-27 18:55:14	2020-03-27 19:19:09	70.3830005252994	com.apple.Music	AirPods	Apple Inc.	0x2002	7C:04:D0:89:89:A0-tacl	_HKPrivateMediaSourceBundleIdentifier
2020-03-28 14:39:34	2020-03-28 14:58:52	67.95333190421479	com.apple.NanoMusic	AirPods	Apple Inc.	0x2002	7C:04:D0:89:89:A0-tacl	_HKPrivateMediaSourceBundleIdentifier
2020-03-30 12:41:28	2020-03-30 13:10:51	69.82387004481137	com.apple.NanoMusic	AirPods	Apple Inc.	0x2002	7C:04:D0:89:89:A0-tacl	_HKPrivateMediaSourceBundleIdentifier
2020-03-31 18:58:07	2020-03-31 19:25:18	74.53960427840138	com.apple.NanoMusic	AirPods Pro	Apple Inc.	0x200e	38:EC:0D:E2:49:CF-tacl	_HKPrivateMediaSourceBundleIdentifier
2020-04-02 17:33:00	2020-04-02 18:02:55	76.20252727791753	com.apple.NanoMusic	AirPods Pro	Apple Inc.	0x200e	38:EC:0D:E2:49:CF-tacl	_HKPrivateMediaSourceBundleIdentifier
2020-04-02 18:02:55	2020-04-02 18:09:02	69.52907160424718	com.apple.NanoMusic	AirPods Pro	Apple Inc.	0x200e	38:EC:0D:E2:49:CF-tacl	_HKPrivateMediaSourceBundleIdentifier
2020-04-03 19:08:02	2020-04-03 19:37:58	74.95567138825342	com.apple.NanoMusic	AirPods Pro	Apple Inc.	0x200e	38:EC:0D:E2:49:CF-tacl	_HKPrivateMediaSourceBundleIdentifier
2020-04-03 19:37:58	2020-04-03 19:47:12	72.03553798789825	com.apple.NanoMusic	AirPods Pro	Apple Inc.	0x200e	38:EC:0D:E2:49:CF-tacl	_HKPrivateMediaSourceBundleIdentifier

Created Timestamp ↕	Earned Date ↕	Achievement ↕	Value ↕	Unit ↕	Creat
2020-03-23 21:53:00	2020-03-23	NewMoveGoalAchieved	480.0	kcal	1
2020-03-27 19:15:40	2020-03-27	FirstWorkout-HKWorkoutActivityTypeRunning			1
2020-03-29 21:19:09	2020-03-29	PerfectWeekStand	8.0	count	1
2020-03-31 02:38:35	2020-03-30	NewExerciseRecord	77.0	min	1
2020-03-31 02:50:55	2020-03-30	NewMoveRecord	881.5340000000002	kcal	1
2020-04-02 17:56:07	2020-04-02	LongestMoveStreak	8.0	count	1
2020-04-03 19:23:54	2020-04-03	LongestMoveStreak	9.0	count	1
2020-04-03 19:37:50	2020-04-03	BestWorkout-HKWorkoutActivityTypeRunning	369.85077135753846	kcal	1

Można zobaczyć:

- w jakiej dokładnie chwili miał dane ciśnienie (odstępów około 5 minutowe)
- sesje treningowe - bieganie, jak długo trwały, przebiegnięty dystans, spalane kalorie
- przekroczenie głośności słuchawek w decybelach - zastanawiający był dla mnie fakt, czemu system operacyjny przetrzymuje takie informacje

Backup

Mobile Backup report

Total number of entries: 2  
Mobile Backup located at: D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_Sunday\_202955\temp\Volumes\JOSH\NoTar-13-3-1\private\var\root\Library\Preferences\com.apple.MobileBackup.plist


Show 15 entries

Key	Value
date	2020-04-11 20:08:06.745905
isCloud	True
Key	Value

11 kwietnia 2020 użytkownik zrobił dokładną kopię systemu w iCoudzie

Zdjęcia

W folderze tym znajduje się naprawdę dużo memów pobranych z różnych mediów społecznościowych np. reddit

	2020-03-22 13:25:02	2020-03-22 13:25:02
---	---------------------	---------------------

Ale również znajdują się zdjęcia, które zrobił Josh

	2020-04-11 17:56:09	2020-04-11 17:56:09	101 Duck Savannah Dr Holly Springs, NC 27540 United States	Wake	Twelve Oaks	33	33
---	---------------------	---------------------	--	------	-------------	----	----

DCIM/100APPLE	public.jpeg	Made/saved with this device	NA
---------------	-------------	-----------------------------------	----

Posiadają one lokalizacje GPS wskazującą na przedmieścia Holly Springs - jakieś osiedle w którym najprawdopodobniej mieszka

Na tych zdjęciach zostało zachowanych naprawdę sporo metadanych

## Przeglądarka

### Safari Browser Bookmarks report

Total number of entries: 12

Safari Browser Bookmarks located at: D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_Sunday\_202955\temp\Volum1\private\var\mobile\Library\Safari\Bookmarks.db

Show  entries

Title	URL
Apple	<a href="https://www.apple.com/">https://www.apple.com/</a>
Ars Technica	<a href="https://arstechnica.com/">https://arstechnica.com/</a>
Bing	<a href="https://www.bing.com/">https://www.bing.com/</a>
BookmarksBar	
com.apple.FrequentlyVisitedSites	
com.apple.ReadingList	
Cult of Mac	<a href="https://www.cultofmac.com/">https://www.cultofmac.com/</a>
Google	<a href="https://www.google.com/?client=safari&amp;channel=iphone_bm">https://www.google.com/?client=safari&amp;channel=iphone_bm</a>
iPhone User Guide	<a href="https://help.apple.com/iphone/guide/">https://help.apple.com/iphone/guide/</a>
Mac Rumors	<a href="https://www.macrumors.com/">https://www.macrumors.com/</a>
Root	
Yahoo	<a href="https://yahoo.com/">https://yahoo.com/</a>

## Safari Recent WebSearches report

Total number of entries: 2

Safari Recent WebSearches located at: D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_Sunday\_202955\temp\Volumes\JOSH\private\var\mobile\Containers\Data\Application\842C9702-4CA9-4A73-A315-62A1F4FD7537\Library\Preferences

Show 15 entries

Date	Search Term
2020-03-28 00:58:35.887930	when does mlb start 2020
2020-03-28 01:02:44.022380	Is the NHL going to resume?

Można tutaj znaleźć między innymi zapisane strony w zakładkach lub czego dokładnie wyszukiwał użytkownik

## Wifi

### Wifi Network Store Model - Networks report

Total number of entries: 2

Wifi Network Store Model - Networks located at: D:\is\lab7\iLEAPP\_Reports\_2023-01-15\_Sunday\_202955\temp\Volumes\JOSH\NoTar-13-3-1\private\var\root\Library\Application Support\WiFiNetworkStoreModel.sqlite

Show 15 entries

Search:

Last Connected Timestamp	PK	SSID	Latitude	Longitude	BSSID	5 GHz Network	2.4 GHz Network
2020-04-12 19:03:49	2	Wemo.Mini.873	35.65922167838447	-78.87317238578156	f8.bb.bf.1e:fa:ef		Yes
2020-04-12 19:03:56	1	CookiesDcoastleR5 Guest	35.65922167838447	-78.87317238578156	f8.bb.bf.1e:fa:f0	Yes	

Można znaleźć tutaj 2 odrębne sieci wifi wraz z ich nazwami, a nawet lokalizacją GPS