

Informatyka Śledcza - Laboratorium 7

Magdalena Ślusarczyk

1 SQLite

1. W bazie danych znajduje się jeden adres email: thisisdfir@gmail.com:

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

2. Konto jest podpięte pod iCloud:

```
4|2|38|1|1|1|1|10||606520077.068197||iCloud||1589F4EC-8F6C-4F37-929F-C6F121836A59|com.apple.purplebuddy|thisisdfir@gmail.com|bplist00
```

3. Konto jest podpięte pod Gmail:

```
18|2|37|1|1|1|1|42||606532289.572603||Gmail||4FD35256-CE13-47FE-9840-EBEB5B9FD9C1|com.apple.Preferences|thisisdfir@gmail.com|
```

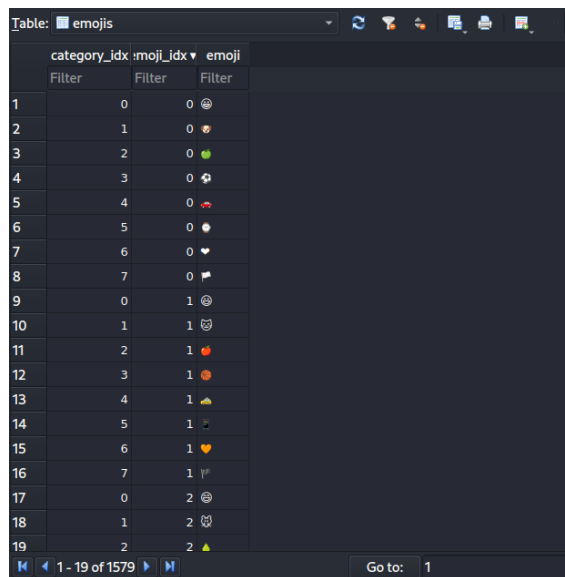
4. Wartości w ZDATE wskazują czas od 1.01.2001r. wyrażony w sekundach np 606532289.572603.

2 DB Browser for SQLite

1. Thread key właściciela urządzenia: 100030845613112.
2. Właścicielem thread key o wartości 100030845613112 jest Josh Hickman:

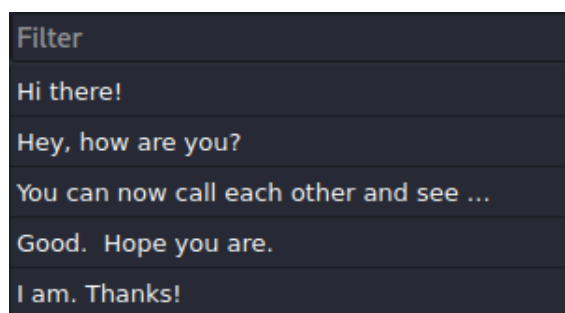
Table: thread_participant_detail					
	contact_id	thread_key	name	nickname	
	Filter	Filter	Filter	Filter	Filter
1	100030845613112	100030845613112	Josh Hickman	NULL	https://sc
2	100046799400843	100030845613112	Thisis Dfir	NULL	https://sc

3. W tabeli emojis znajduje się 1579 emoji:



	category_idx	moji_idx	emoji
1	0	0	😊
2	1	0	👉
3	2	0	🍏
4	3	0	🎱
5	4	0	🚗
6	5	0	👤
7	6	0	♥️
8	7	0	📢
9	0	1	😬
10	1	1	😏
11	2	1	🍎
12	3	1	🍌
13	4	1	🌂
14	5	1	👤
15	6	1	♥️
16	7	1	📢
17	0	2	👉
18	1	2	😏
19	2	2	🍏

4. W tabeli messages znajdują się wiadomości tekstowe np:



Filter

Hi there!

Hey, how are you?

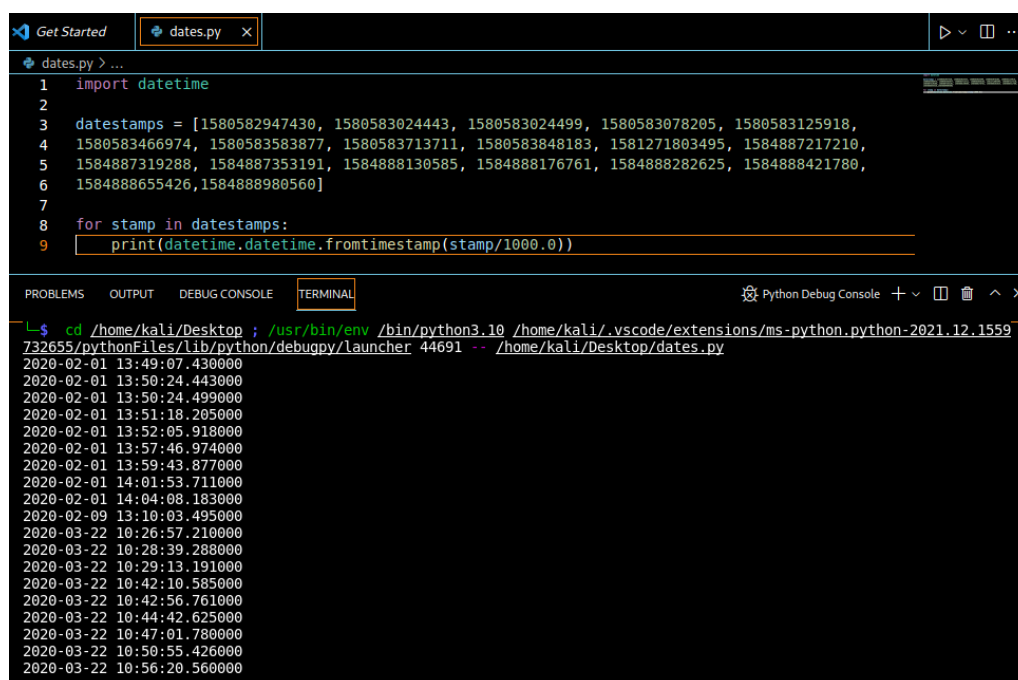
You can now call each other and see ...

Good. Hope you are.

I am. Thanks!

5. W rozmowie brały udział dwie osoby: 100030845613112 oraz 100046799400843

6. Ramy czasowe konwersacji:



```
1 import datetime
2
3 timestamps = [1580582947430, 1580583024443, 1580583024499, 1580583078205, 1580583125918,
4 1580583466974, 1580583583877, 1580583713711, 1580583848183, 1581271803495, 1584887217210,
5 1584887319288, 1584887353191, 1584888130585, 1584888176761, 1584888282625, 1584888421780,
6 1584888655426, 1584888980560]
7
8 for stamp in timestamps:
9     print(datetime.datetime.fromtimestamp(stamp/1000.0))
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL Python Debug Console

```
cd /home/kali/Desktop ; /usr/bin/env /bin/python3.10 /home/kali/.vscode/extensions/ms-python.python-2021.12.1559
732655/pythonFiles/lib/python/debugpy/launcher 44691 -- /home/kali/Desktop/dates.py
2020-02-01 13:49:07.430000
2020-02-01 13:50:24.443000
2020-02-01 13:50:24.499000
2020-02-01 13:51:18.205000
2020-02-01 13:52:05.918000
2020-02-01 13:57:46.974000
2020-02-01 13:59:43.877000
2020-02-01 14:01:53.711000
2020-02-01 14:04:08.183000
2020-02-09 13:10:03.495000
2020-03-22 10:26:57.210000
2020-03-22 10:28:39.288000
2020-03-22 10:29:13.191000
2020-03-22 10:42:10.585000
2020-03-22 10:42:56.761000
2020-03-22 10:44:42.625000
2020-03-22 10:47:01.780000
2020-03-22 10:50:55.426000
2020-03-22 10:56:20.560000
```

3 Pliki plist

1. Pliki plist i iOS służą do zapisywania konfiguracji i ustawień aplikacji.
2. Można je przekonwertować do XML lub postaci binarnej.
3. Przykładowe informacje zawarte w com.apple.wifi.plist:
 - Device UUID: 226DE21D-BC39-476F-B693-BBF935BACECC
 - Lista znanych sieci
 - Device Updated Date: 2020-03-21T21:38:56Z
 - Device Software version: 17D50

4 Automatyczna analiza systemu iOS

4.1 Podstawowe informacje o urządzeniu

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

Do urządzenia podłączone są konta np.: Google, iCloud, GameCenter, iTunesStore, wszystkie na email thisisdfr@gmail.com.

4.2 Kontakty

W kontaktach możemy znaleźć numer oraz email osoby nazywającej się Josh Hickman:

Contact ID	Contact Number	First Name	Middle Name	Last Name	Email Address
1	+19195790479	Josh		Hickman	joshua.hickman1@me.com

4.3 Karta kredytowa

Do urządzenia podpięta została karta Visa o numerze 4852464484724033

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

4.4 Podłączone urządzenia

Możemy zobaczyć z jakimi urządzeniami Bluetooth łączył się telefon:

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-8FC5-B882-A2BE-CAD5D11A117D	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
9978DBCC-BD39-0371-FE07-9BE1C48ABCDE	This Is's Apple Watch	2	Random 63:B0:ED:30:A1:CF	Public F8:6F:C1:4E:FF:6A	274

4.5 Historia połączeń

Z historii połączeń możemy dowiedzieć się np.: o FaceTime Video z Joshem Hickmanem:

2020-04-12 15:26:43	joshua.hickman1@me.com		No	FaceTime Video	Outgoing	00:01:38
------------------------	------------------------	--	----	-------------------	----------	----------

4.6 DHCP

Adres IP urządzenia to 192.168.11.20 a adres jego bramy domyślnej (routera) to 192.168.11.1

Key	Value
IPAddress	192.168.11.20
LeaseLength	28800
LeaseStartDate	2020-04-12 19:04:02
RouterHardwareAddress	b'\xf8\xbb\xbf\x1e\xfa\xfo'
RouterIPAddress	192.168.11.1
SSID	CcookiesDcastleR5 Guest

4.7 Discord

Właściciel urządzenia ma konto na Discordzie o nazwie ThisIsDFIR. Poprzez komunikator została przeprowadzona jedna rozmowa z użytkownikiem josh_hickman1, w której Josh dziękuje właścicielowi urządzenia za coś i druga na temat alergii.

4.8 Facebook

Między właścicielem urządzenia a Joshem Hickmanem zostały przeprowadzone 2 rozmowy audio i 2 rozmowy wideo przez Facebooka. Rozmawiali ze sobą również na chacie, gdzie właściciel udostępnił Joshowi swoją lokalizację. Prowadzili też ze sobą sekretną konwersację, odbywającą się szyfrowanym kanałem.

4.9 IMO HD Chat

W tej aplikacji istnieją dwa numery kontaktowe do Josha Hickmana, jeden pod pseudonimem John Hicks, drugi Lil Enusynt. Właściciel telefonu prowadził z nim konwersacje na temat jakichś problemów technicznych.

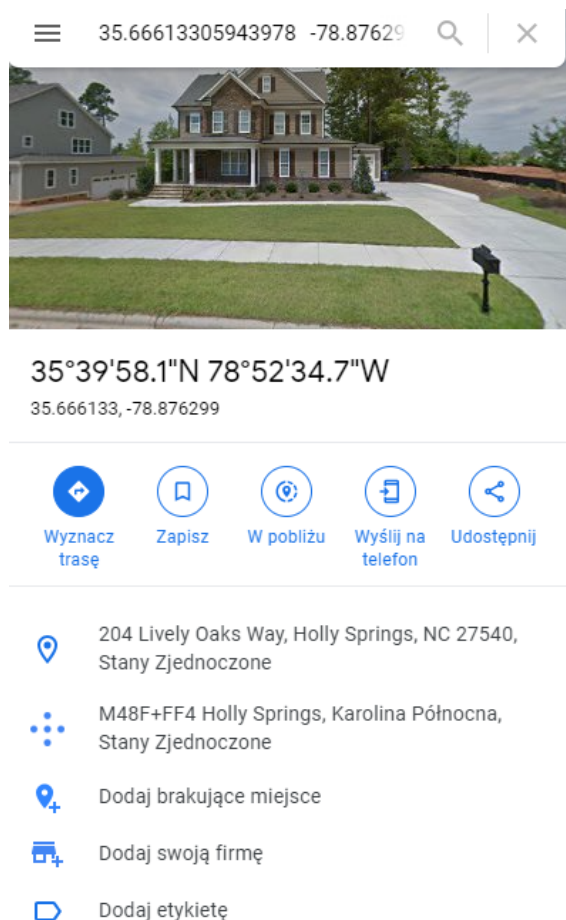
Timestamp	Sender Name	Sender Alias	Sender Phone	Message
2020-03-22 17:23:26	Josh Hickman	Josh Hickman	9195790479	Took a break. I'm back now.
2020-03-22 17:24:57				Ok good. I was having some service issues but I think it's ok now.
2020-03-22 18:02:52	Josh Hickman	Josh Hickman	9195790479	uploaded photo: https://cdn.imoim.us/s/object/.42VJlUYeJXeKmGOCzinzrnXDjE/
2020-03-22 18:20:27				
2020-03-30 11:26:18	Josh Hickman	Josh Hickman	9193912507	is now on imo!

4.10 Instagram

Na instagramie również właściciel telefonu prowadził rozmowę z Joshem, tym razem na temat samej aplikacji Instagrama. Prowadzili też video chat.

4.11 Miejsca

Z aplikacji Apple Maps możemy odczytać lokalizację, wskazującą na jakiś dom, prawdopodobnie właściciela urządzenia:



W wyszukiwaniach pojawia się miejsce Manhattan Pizza w tej samej miejscowości.

4.12 Przeglądarka

Właściciel telefonu wyszukiwał hasła związane z hokejem i bejsbolem:

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?

4.13 Płatności

Właściciel telefonu otrzymał od Josha płatności o tytułach 'Android 10 image' czy też 'for the testing stuff'.

4.14 Podsumowanie

Właściciel telefonu często rozmawia z osobą nazywającą się Josh Hickerman. Historia płatności i rozmów może wskazywać na to, że właściciel telefonu coś dla Josha testował. Z wyszukiwań w przeglądarce możemy dowiedzieć się o jego zainteresowaniach, a z lokalizacji o miejscu zamieszkania.