

Szymon Koziol

# ZADANIE 1:

```
(szmpns@kali)-[~/InformatykaSledcza/InfSI_LAB07]
$ sqlite3 Accounts3.sqlite
SQLite version 3.44.2 2023-11-24 11:41:44
Enter ".help" for usage hints.
sqlite> select * from ZACCOUNT;
1|2|8|0|1|1|1|25||606519591.912371||Local||i|iTunesLocal-421A04EA-479A-4E46-B49D-556F7144518D|locationd||
2|2|57|1|1|1|1|25||606520062.043928|||6835410D-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.identityservicesd|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|0|1|24|4|606520075.27839|||798A0EA2-0B24-4857-B19C-3C048732B77D|com.apple.accounts.accountsd|thisisdfr@gmail.com|
6|2|44|1|1|0|1|19|4|606520075.243605|||94F572A1-6ECA-4ECC-B7B3-FF927D48C7E4|com.apple.accounts.accountsd|thisisdfr@gmail.com|
7|2|19|1|1|1|1|1|46|4|606520062.363132|||38835298-47A1-458F-ADAB-0DEF58898C2F|com.apple.accounts.accountsd|thisisdfr@gmail.com|
8|2|1|1|1|1|1|23|4|606520075.446426|||parent||8618B8CD-F392-48D3-8D75-4346ADE75FC8|com.apple.accounts.accountsd||
9|2|4|1|1|1|1|33|4|606520075.3066|||parent||E9B5703B-F844-4845-AD3D-08DE58806F82|com.apple.accounts.accountsd||
10|2|3|1|1|1|1|1|43|4|606520075.373321|||parent||EE84958A-E52C-425E-9171-70DEB1C85DEB|com.apple.accounts.accountsd||
11|2|30|1|1|0|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|0|0|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|18|606532289.45302|||parent||03CF4555-027D-4CBB-87FD-462FC610F64D|com.apple.accounts.accountsd||
16|2|1|1|1|1|1|23|18|606532289.541797|||parent||CEA1DA02-7BCC-4C0B-8CB0-2677865D0E03|com.apple.accounts.accountsd||
17|2|3|1|1|1|1|1|43|18|606532289.508673|||parent||98491756-59C0-4798-9EB6-1714C936158F|com.apple.accounts.accountsd||
18|2|37|1|1|1|1|1|42||606532289.572603||Gmail||4FD35256-CE13-47FE-9840-EBEB5B9FD9C1|com.apple.Preferences|thisisdfr@gmail.com|
sqlite>
```

Dane dotyczące maili znajdowały się w tabeli ZACCOUNT.

a)

Adresy email pojawiają się w różnych kolumnach, zatem prościej będzie całość przeszukać ręcznie.

W bazie danych znajduje się 1 adres email.

b)

[thisisdfr@gmail.com](mailto:thisisdfr@gmail.com)

c)

Tak, ten adres został podpięty do iCloud.

d)

Tak, posiadał.

e)

```
(szmpns@kali)-[~/InformatykaSledcza/InfSl_LAB07]
$ sqlite3 Accounts3.sqlite
SQLite version 3.44.2 2023-11-24 11:41:44
Enter ".help" for usage hints.
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>
```

Dane dotyczące maili znajdujące się w bazie danych:

a)

Adresy email pojawiają się w bazie danych, ale nie są one przeszukane ręcznie.

W bazie danych znajduje się adres email:

b)

[thisisdfir@gmail.com](mailto:thisisdfir@gmail.com)

c)

Tak, ten adres został podany w bazie danych.

d)

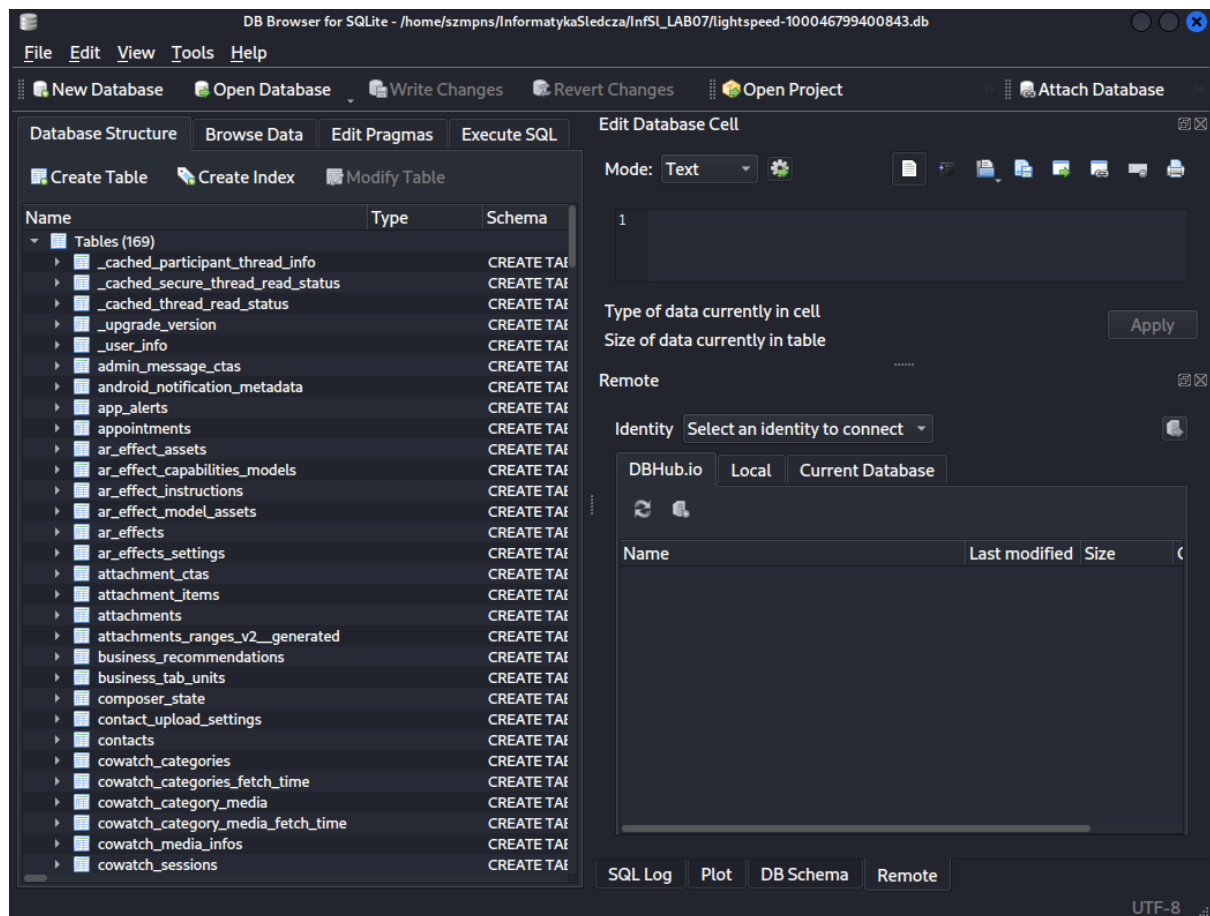
Są to prawdopodobnie sekundy, które minęły od daty 01.01.2001

```
error here —^
sqlite> SELECT strftime('%Y-%m-%d %H:%M:%f', ZDATE + 978307200, 'unixepoch') FROM ZACCOUNT;
2020-03-21 21:39:51.912
2020-03-21 21:47:42.044
2020-03-21 21:47:42.507
2020-03-21 21:47:57.068
2020-03-21 21:47:55.278
2020-03-21 21:47:55.244
2020-03-21 21:47:42.363
2020-03-21 21:47:55.446
2020-03-21 21:47:55.307
2020-03-21 21:47:55.373
2020-03-21 21:47:57.848
2020-03-21 21:47:58.027
2020-03-21 21:49:16.474
2020-03-21 21:59:47.090
2020-03-22 01:11:29.453
2020-03-22 01:11:29.542
2020-03-22 01:11:29.509
2020-03-22 01:11:29.573
sqlite>
```

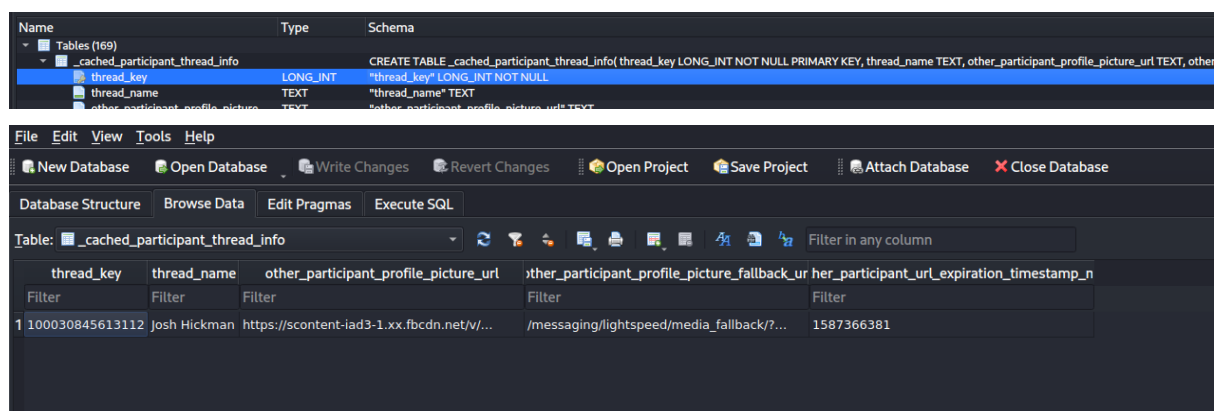
Są to prawdopodobnie sekundy, które minęły od daty 01.01.2001

## Część 2:

Otwarcie:



a)



Id użytkownika facebook: 100030845613112

b)

Josh Hickman

c)

▶ emoji_categories		CREATE TABLE emoji_categories( category_idx INTEGER NOT NULL PRIMARY KEY, localized_cate
▼ emojijs		CREATE TABLE emojijs( category_idx INTEGER NOT NULL, emoji_idx INTEGER NOT NULL, emoji T
category_idx	INTEGER	"category_idx" INTEGER NOT NULL
emoji_idx	INTEGER	"emoji_idx" INTEGER NOT NULL
emoji	TEXT	"emoji" TEXT NOT NULL
▶ experiment_emergency_push		CREATE TABLE experiment_emergency_push( config TEXT NOT NULL, version INTEGER NOT NUL
▶ experiment_value		CREATE TABLE experiment_value( config TEXT NOT NULL, param TEXT NOT NULL, value TEXT, ty

1563	7	242	🇬🇧
1564	7	243	🇪🇬
1565	7	244	🇵🇰
1566	7	245	🇳🇮
1567	7	246	🇺🇸
1568	7	247	🇺🇾
1569	7	248	🇻🇮
1570	7	249	🇺🇿
1571	7	250	🇻🇺
1572	7	251	🇻🇦
1573	7	252	🇻🇪
1574	7	253	🇻🇳
1575	7	254	🇼🇫
1576	7	255	🇪🇭
1577	7	256	🇾🇪
1578	7	257	🇿🇲
1579	7	258	🇿🇼

⏮ ⏪ 1552 - 1579 of 1579 ⏩ ⏭

Jest ich dokładnie 1579

d)

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database									
Database Structure Browse Data Edit Pragmas Execute SQL									
Table: messages									
	thread_key	timestamp_ms	message_id	offline_threading_id	text	sender_id	sticker_id	is_admin_message	auth
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	100030845613112	1584888980560	mid.\$cAAAAB8r0m7N3NAPsUFxAr6kRQ1Gs	6647506190672810412	NULL	100030845613112	NULL	0	
2	100030845613112	1584888655426	mid.\$cAAAAB8r0m7N3M_72QJxArmuOeCtm	6647504826973825894	NULL	100046799400843	NULL	0	
3	100030845613112	1584888421780	mid.\$cAAAAB8r0m7N3M_tIlFxArydRkCW	6647503846699443618	Good question.	100046799400843	NULL	0	
4	100030845613112	1584888282625	mid.\$cAAAAB8r0m7N3M_JGAvxArP9y_iS1	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	Lo!!	100046799400843	NULL	0	
7	100030845613112	1584887353191	mid.\$cAAAAB8r0m7N3M-sXZ1xAqXO2Uj-p	6647499364444028841	Yep!	100046799400843	NULL	0	
8	100030845613112	1584887319288	mid.\$cAAAAB8r0m7N3M-qS-FxAqVjtDCy	6647499221488906418	I see. I also see some of our previous ...	100030845613112	NULL	0	
9	100030845613112	1584887217210	mid.\$cAAAAB8r0m7N3M-kEOlxArQ07EBLSe	6647498793449993374	Switched over to FB Messenger.	100046799400843	NULL	0	
10	100030845613112	1581271803495	mid.\$cAAAAB8r0m7N2XGouZ1wKyTujkpp	6632334646540388969		100046799400843	NULL	0	
11	100030845613112	1580583848183	mid.\$cAAAAB8r0m7N2M2jO91wAIO7I2-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_c1wAhh3bQ5nI	6629445701963323848	You can now call each other and see ...	100030845613112	NULL	1	
18	100030845613112	1580583024443	mid.\$cAAAAB8r0m7N2M1w_O1wAhhbyv0_GK	6629445696939618698	Hey, how are you?	100030845613112	NULL	0	
19	100030845613112	1580582947430	mid.\$cAAAAB8r0m7N2M1sSZlWAhXL6muVm	6629445380366591334	Hi there!	100046799400843	NULL	0	

Tak znajdują się.

e)

```
~/InformatykaSledcza/InfSI_LAB07/id.py - Mousepad
File Edit Search View Document Help
1 tab = [100030845613112,
2 100046799400843,
3 100046799400843,
4 100030845613112,
5 100046799400843,
6 100046799400843,
7 100046799400843,
8 100030845613112,
9 100046799400843,
10 100046799400843,]
11 100030845613112,
12 100046799400843,
13 100046799400843,
14 100030845613112,
15 100030845613112,
16 100046799400843,
17 100030845613112,
18 100030845613112,
19 100046799400843]
20
21 ids = []
22
23 for i in range(len(tab)):
24     if tab[i] not in ids:
25         ids.append(tab[i])
26
27 print(ids)
28 print(len(ids))
29
```

```
(szmpns@kali)-[~/InformatykaSledcza/InfSl_LAB07]
$ python3 id.py
[100030845613112, 100046799400843]
2
```

udział brały 2 osoby.

Ich id: 100030845613112 oraz 100046799400843

f)

```
1 timestamp = [1584888980560,
2 1584888655426,
3 1584888421780,
4 1584888282625,
5 1584888176761,
6 1584888130585,
7 1584887353191,
8 1584887319288,
9 1584887217210,
10 1581271803495,
11 1580583848183,
12 1580583713711,
13 1580583583877,
14 1580583466974,
15 1580583125918,
16 1580583078205,
17 1580583024499,
18 1580583024443,
19 1580582947430]
20
21 import datetime
22
23 def convert(mseconds):
24
25     seconds = mseconds / 1000
26
27     start_date = datetime.datetime(1970,1,1)
28
29     result = start_date + datetime.timedelta(seconds=seconds)
30
31     return result
32
33
34 for i in range(len(timestamp)):
35     print(f"{i+1} data: {convert(int(timestamp[i]))}")
36
```

```
(szmpns@kali)-[~/InformatykaSledcza/InfSl_LAB07]
$ python3 time.py
1 data: 2020-03-22 14:56:20.560000
2 data: 2020-03-22 14:50:55.426000
3 data: 2020-03-22 14:47:01.780000
4 data: 2020-03-22 14:44:42.625000
5 data: 2020-03-22 14:42:56.761000
6 data: 2020-03-22 14:42:10.585000
7 data: 2020-03-22 14:29:13.191000
8 data: 2020-03-22 14:28:39.288000
9 data: 2020-03-22 14:26:57.210000
10 data: 2020-02-09 18:10:03.495000
11 data: 2020-02-01 19:04:08.183000
12 data: 2020-02-01 19:01:53.711000
13 data: 2020-02-01 18:59:43.877000
14 data: 2020-02-01 18:57:46.974000
15 data: 2020-02-01 18:52:05.918000
16 data: 2020-02-01 18:51:18.205000
17 data: 2020-02-01 18:50:24.499000
18 data: 2020-02-01 18:50:24.443000
19 data: 2020-02-01 18:49:07.430000
```

Rozmowa była prowadzona między 2020-02-01 18:49:07.430000, a 2020-03-22 14:56:20.560000.

## ZADANIE 2:

a)

Pliki .plist służą do przekazywania informacji odnośnie konfiguracji aplikacji mobilnych w systemach IOS, informują o wersjach IOS, które dana aplikacja wspiera.

b)

Można je przekonwertować do postaci binarnej, plików JSON lub XML.

c)

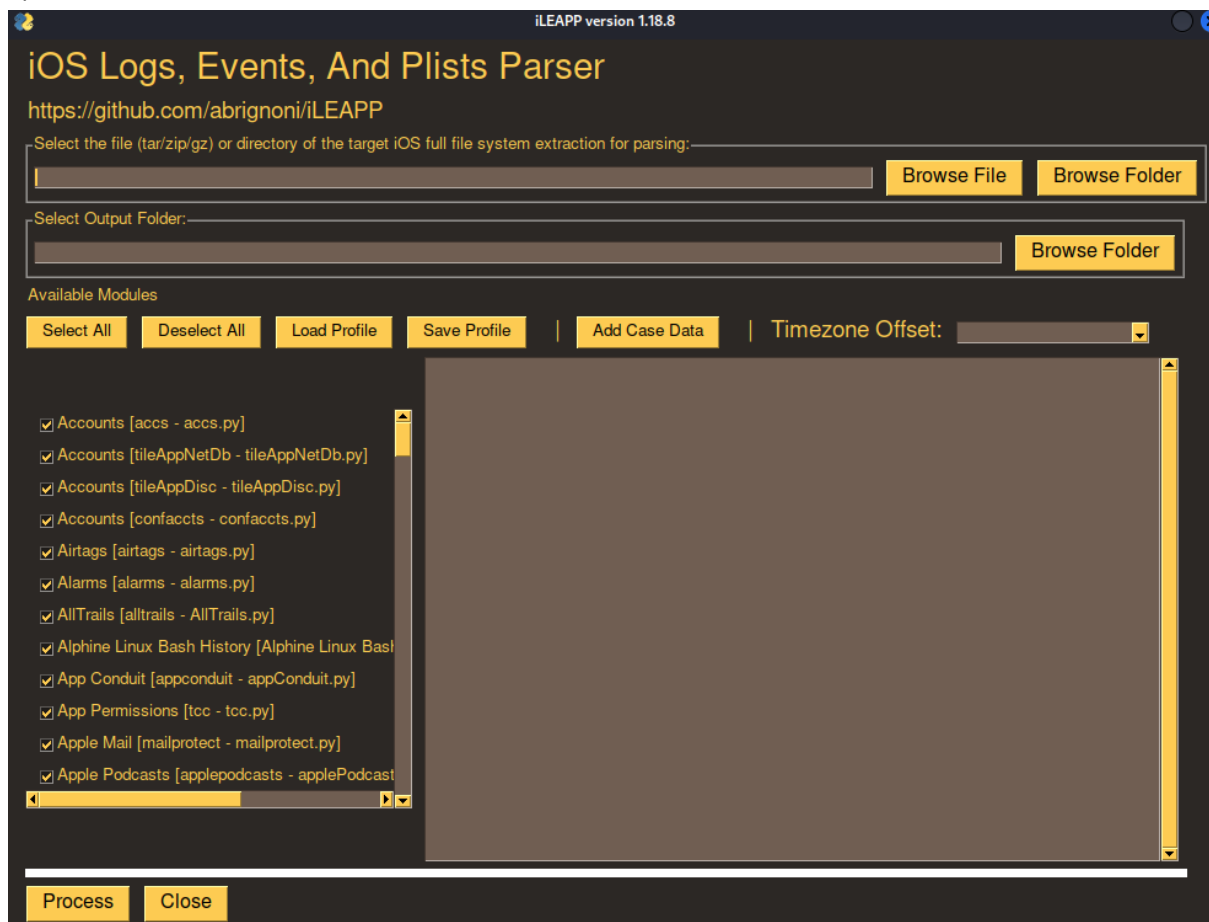
W pliku znajdują się np. listy zapamiętanych sieci WIFI, z którymi łączyła się aplikacja.



Znajdują się tam:  
Daty modyfikacji hasła  
numer SSID  
zużyte pakiety(wykorzystanie sieci)

## ZADANIE 3:

1)



2)





3) i 4) zrobione

5)

```
(szmpns@kali)-[~/InformatykaSledcza/InfSl_LAB07/zad3]
$ ls
iLEAPP_Reports_2024-01-04_Thursday_165540

(szmpns@kali)-[~/InformatykaSledcza/InfSl_LAB07/zad3]
$ cd iLEAPP_Reports_2024-01-04_Thursday_165540

(szmpns@kali)-[~/InformatykaSledcza/InfSl_LAB07/zad3/iLEAPP_Reports_2024-01-04_Thursday_165540]
$ ls
'Script Logs'  temp
```

Narzędzie zwróciło raport, który można przeglądać w postaci strony internetowej.

a)

Nazwa użytkownika telefonu to ThisIsDFIR. Można pomyśleć z poprzednich ćwiczeń, że użytkownik tak naprawdę ma na imię Josh, ale nie da się tego jednoznacznie stwierdzić.

Hey ThisIsDFIR, Thanks for  
registering for an account on  
Discord! Before we get started,  
we just need to confirm that this


b)

W zakładce “Account Data” znajdują się informacje o mailu. Mail użytkownika to:  
[thisisdfr@gmail.com](mailto:thisisdfr@gmail.com)

2020-03-22	iTunes	thisisdfr@gmail.com
01:47:42	Store	


c)

Istnieje wiele zakładek, które pozwalają zapoznać się z działalnością w internecie użytkownika. Można zauważyć, że szukał m. in. kiedy wznawiane są rozgrywki ligi hokejowej NHL.

Last Viewed Time 	Title
2000-12-31 23:59:59	iOS Mobile Installation Logs - DFIR Review
2020-03-28 01:06:05	Is the NHL going to resume? - Google Search
2020-03-28 01:29:45	What Happened to Tiger King's Carole Baskin, Husband Don Lewis?
2020-03-28 01:45:11	dfir.pubpub.org/pub/e5xlbw88

d)

Jeżeli chodzi o jego lokalizację, to znajduje się on prawdopodobnie w okolicach Raleigh w stanie Karolina Północna(USA).

Latitude 	Longitude
35.66613305943978	-78.87629920805553

Analiza pozwoliła na zidentyfikowanie bardzo istotnych danych personalnych użytkownika telefonu. Udało się odnaleźć jego adres email, lokalizację, czy numer telefonu. Do tego dzięki posiadanym zapisom z przeglądarek można nakreślić profil użytkownika(np. zainteresowanie sportem).

Dane nie były zatem zaszyfrowane, użytkownik nie zadbał odpowiednio o swoje bezpieczeństwo, przez co jego prywatność została naruszona.