ANALIZA IOS

ZAWARTOŚĆ BAZ DANYCH

Pierwszą bazą danych do analizy jest Accounts3.sqlite. Zawiera ona dane o użytkowniku systemu. Znajduje się w katalogu private/var/mobile/Library/Accounts

.fullschema pokaże wszystkie dostępne tabele w bazie danych

```
sqlite> .fullschema
CREATE TABLE ZACCESSOPTIONSKEY ( Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZNAME VARCHAR );
CREATE TABLE Z_1OWNINGACCOUNTTYPES ( Z_1ACCESSKEYS INTEGER, Z_4OWNINGACCOUNTTYPES INTEGER, PRIMARY KEY (Z_1ACCESSKEY
S, Z_4OWNINGACCOUNTTYPES) );
CREATE TABLE ZACCOUNT ( Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZACTIVE INTEGER, ZAUTHENTICATED INTE
GER, ZSUPPORTSAUTHENTICATION INTEGER, ZVISIBLE INTEGER, ZACCOUNTTYPE INTEGER, ZPARENTACCOUNT INTEGER, ZDATE TIMESTAM
P, ZLASTCREDENTIALRENEWALREJECTIONDATE TIMESTAMP, ZACCOUNTDESCRIPTION VARCHAR, ZAUTHENTICATIONTYPE VARCHAR, ZCREDENT
IALTYPE VARCHAR, ZIDENTIFIER VARCHAR, ZOWNINGBUNDLEID VARCHAR, ZUSERNAME VARCHAR, ZDATACLASSPROPERTIES BLOB );
CREATE TABLE Z_2ENABLEDDATACLASSES ( Z_2ENABLEDACCOUNTS INTEGER, Z_7ENABLEDDATACLASSES INTEGER, PRIMARY KEY (Z_2ENAB
LEDACCOUNTS, Z_7ENABLEDDATACLASSES) );
CREATE TABLE Z_2PROVISIONEDDATACLASSES ( Z_2PROVISIONEDACCOUNTS INTEGER, Z_7PROVISIONEDDATACLASSES INTEGER, PRIMARY
KEY (Z_2PROVISIONEDACCOUNTS, Z_7PROVISIONEDDATACLASSES) );
CREATE TABLE ZACCOUNTPROPERTY ( Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZOWNER INTEGER, ZKEY VARCHAR
, ZVALUE BLOB );
CREATE TABLE ZACCOUNTTYPE ( Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZENCRYPTACCOUNTPROPERTIES INTEGE
R, ZOBSOLETE INTEGER, ZSUPPORTSAUTHENTICATION INTEGER, ZSUPPORTSMULTIPLEACCOUNTS INTEGER, ZVISIBILITY INTEGER, ZACCO
UNTTYPEDESCRIPTION VARCHAR, ZCREDENTIALPROTECTIONPOLICY VARCHAR, ZCREDENTIALTYPE VARCHAR, ZIDENTIFIER VARCHAR, ZOWNI
NGBUNDLEID VARCHAR );
CREATE TABLE Z_4SUPPORTEDDATACLASSES ( Z_4SUPPORTEDTYPES INTEGER, Z_7SUPPORTEDDATACLASSES INTEGER, PRIMARY KEY (Z_4S
UPPORTEDTYPES, Z_7SUPPORTEDDATACLASSES) );
CREATE TABLE Z_4SYNCABLEDATACLASSES ( Z_4SYNCABLETYPES INTEGER, Z_7SYNCABLEDATACLASSES INTEGER, PRIMARY KEY (Z_4SYNC
ABLETYPES, Z_7SYNCABLEDATACLASSES) );
CREATE TABLE ZAUTHORIZATION ( Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZACCOUNTTYPE INTEGER, ZBUNDLEI
D VARCHAR, ZGRANTEDPERMISSIONS VARCHAR, ZOPTIONS BLOB );
CREATE TABLE ZCREDENTIALITEM ( Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZPERSISTENT INTEGER, ZEXPIRAT
IONDATE TIMESTAMP, ZACCOUNTIDENTIFIER VARCHAR, ZSERVICENAME VARCHAR );
CREATE TABLE ZDATACLASS ( Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZNAME BLOB );
CREATE INDEX Z_1OWNINGACCOUNTTYPES_Z_4OWNINGACCOUNTTYPES_INDEX ON Z_1OWNINGACCOUNTTYPES (Z_4OWNINGACCOUNTTYPES, Z_1A
CCESSKEYS);
CREATE INDEX ZACCOUNT_ZACCOUNTTYPE_INDEX ON ZACCOUNT (ZACCOUNTTYPE);
CREATE INDEX ZACCOUNT_ZPARENTACCOUNT_INDEX ON ZACCOUNT (ZPARENTACCOUNT);
CREATE INDEX Z_2ENABLEDDATACLASSES_Z_7ENABLEDDATACLASSES_INDEX ON Z_2ENABLEDDATACLASSES (Z_7ENABLEDDATACLASSES, Z_2E
NABLEDACCOUNTS);
CREATE INDEX Z_2PROVISIONEDDATACLASSES_Z_7PROVISIONEDDATACLASSES_INDEX ON Z_2PROVISIONEDDATACLASSES (Z_7PROVISIONEDD
ATACLASSES, Z_2PROVISIONEDACCOUNTS);
CREATE INDEX ZACCOUNTPROPERTY_ZOWNER_INDEX ON ZACCOUNTPROPERTY (ZOWNER);
CREATE INDEX Z_4SUPPORTEDDATACLASSES_Z_7SUPPORTEDDATACLASSES_INDEX ON Z_4SUPPORTEDDATACLASSES (Z_7SUPPORTEDDATACLASS
ES, Z_4SUPPORTEDTYPES);
CREATE INDEX Z_4SYNCABLEDATACLASSES_Z_7SYNCABLEDATACLASSES_INDEX ON Z_4SYNCABLEDATACLASSES (Z_7SYNCABLEDATACLASSES,
Z_4SYNCABLETYPES);
CREATE INDEX ZAUTHORIZATION_ZACCOUNTTYPE_INDEX ON ZAUTHORIZATION (ZACCOUNTTYPE);
CREATE TABLE Z_PRIMARYKEY (Z_ENT INTEGER PRIMARY KEY, Z_NAME VARCHAR, Z_SUPER INTEGER, Z_MAX INTEGER);
CREATE TABLE Z_METADATA (Z_VERSION INTEGER PRIMARY KEY, Z_UUID VARCHAR(255), Z_PLIST BLOB);
CREATE TABLE Z_MODELCACHE (Z_CONTENT BLOB);
/* No STAT tables available */
```

Ciekawe informacje można znaleźć w tabeli ZACCOUNT

```
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|thisisdfir@gmail.
com|
3|2|73|1|1|1|1|40||606520062.507476|||||381B0D37-7962-43E6-BF7D-139B59033D1C|com.apple.identityservicesd|thisisdfir@
gmail.com|
4|2|38|1|1|1|1|10||606520077.068197||iCloud|||1589F4EC-8F6C-4F37-929F-C6F121B36A59|com.apple.purplebuddy|thisisdfir@
gmail.com|bplist00◆
5|2|13|1|1|0|1|24|4|606520075.27839|||||798A0EA2-0B24-4857-B19C-3C048732B77D|com.apple.accounts.accountsd|thisisdfir
@gmail.com|
6|2|44|1|1|0|1|19|4|606520075.243605|||||94F572A1-6ECA-4ECC-B7B3-FF927D48C7E4|com.apple.accounts.accountsd|thisisdfi
r@gmail.com|
7|2|19|1|1|1|1|46|4|606520062.363132|||||3B835298-47A1-458F-ADAB-0DEF5B898C2F|com.apple.accounts.accountsd|thisisdfi
r@gmail.com|
8|2|1|1|1|1|1|23|4|606520075.446426|||parent||8618BBCD-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|43|4|606520075.373321|||parent||EE84958A-E52C-425E-9171-70DEB1CB5DEB|com.apple.accounts.accountsd||
11|2|30|1|1|0|1|44||606520077.847509|||||8F4A8F1B-DAD9-40F6-A06E-18B6A73D044F|com.apple.AuthKit|thisisdfir@gmail.com
|
12|2|26|1|1|1|1|15||606520078.027195|||||5B9A4BE7-A9AC-4798-A8EE-67EB19537748|com.apple.AuthKit|thisisdfir@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|51||606520787.089834||thisisdfir@gmail.com|||9BBC69AE-9F27-497B-8B94-D8AD8156181E|com.apple.AuthKit|t
hisisdfir@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|43|18|606532289.508673|||parent||98491756-59C0-4798-9EB6-1714C936158F|com.apple.accounts.accountsd||
18|2|37|1|1|1|1|42||606532289.572603||Gmail|||4FD35256-CE13-47FE-9840-EBEB5B9FD9C1|com.apple.Preferences|thisisdfir@
gmail.com|
```

Z użyciem tego polecenia jest to czytelniejsze:

```
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
```

Widnieje tu adres email użytkownika: thisisdfir@gmail.com

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

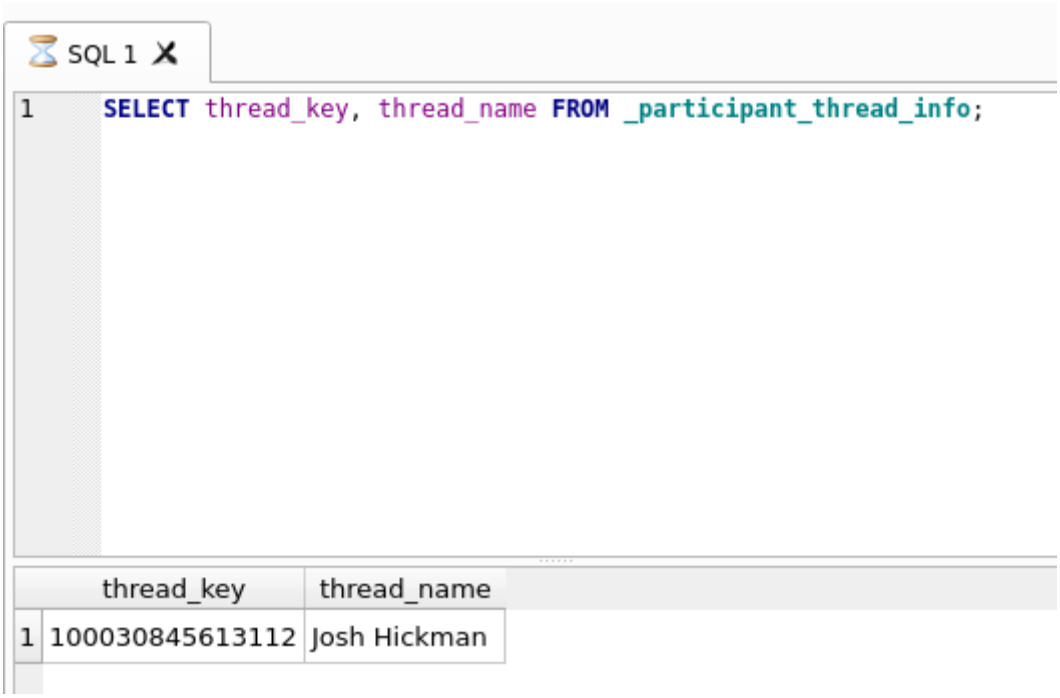
Mail ten został podpięty pod serwis iCloud, Holiday Calendar oraz Gmail

Kolumna ZDATE pokazuje datę w formacie podobnym do Unix Time

Lightspeed Database

W bazie lightspeed-100046799400843.db znajdują się informacje na temat ID właściciela urządzenia
Znajduje się on w tablicy _participant_thread_info

Do której można się dostać w taki sposób:



Jak widać ID właściciela to 100030845613112
Imię i nazwisko właściciela to Josh Hickman

```
1  SELECT COUNT(*) FROM emojis;
2
```

	COUNT(*)
1	1579

W bazie znajduje się 1579 emotek

W tablicy messages znajdziemy również wiadomości:

```
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!
```

```
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 you've read messages.
100030845613112|Hey, how are you?
100046799400843|Hi there!
```

Zauważyć też można, że rozmówców jest dwóch

W tabeli kolumnie timestamp_ms można znaleźć datę wysłania wiadomości
Są one jednak podane w unix time, ale można je zamienić na czytelną datę za pomocą prostego skryptu w pythonie:

timestamp.py > ...

```python
from  datetime import datetime


dates = [ ⋯

for date in dates:
    print(datetime.fromtimestamp(date / 1000))

```

```
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
```

Zwrócił on takie daty.
Jak widać wiadomości były wysyłane 01.02.2020, 09.02.2020 oraz 22.03.2020

PLIKI PLIST

Pliki .plist czyli Property List File to pliki zawierające informacje systemowe na temat tego jak on działa

Pliki te można konwertować do plików tekstowych, xml i binarnych

Dla przykładu plik com.apple.accounts.exists.plist zawiera informacje o tym czy konto w danej aplikacji istnieje lub ile ich jest:

```
┌──(kali㉿kali)-[~/…/private/var/preferences/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>
        <integer>1</integer>
        <key>com.apple.account.CalDAV.exists</key>
        <integer>1</integer>
        <key>com.apple.account.idms.count</key>
        <integer>1</integer>
        <key>com.apple.account.Google.exists</key>
        <integer>1</integer>
```

Plik preferences.plist zawiera informacje na temat:

```
</dict>
<key>CurrentSet</key>
<string>/Sets/C612A594-E2C8-4930-9B48-2E03540BC901</string>
<key>Model</key>
<string>N69AP</string>
<key>System</key>
<dict>
        <key>Network</key>
        <dict>
                <key>HostNames</key>
                <dict>
                        <key>LocalHostName</key>
                        <string>This-Iss-iPhone</string>
                </dict>
        </dict>
        <key>System</key>
        <dict>
                <key>ComputerNameEncoding</key>
                <integer>134217984</integer>
                <key>ComputerName</key>
                <string>This Is's iPhone</string>
                <key>HostName</key>
                <string>This-Iss-iPhone</string>
```

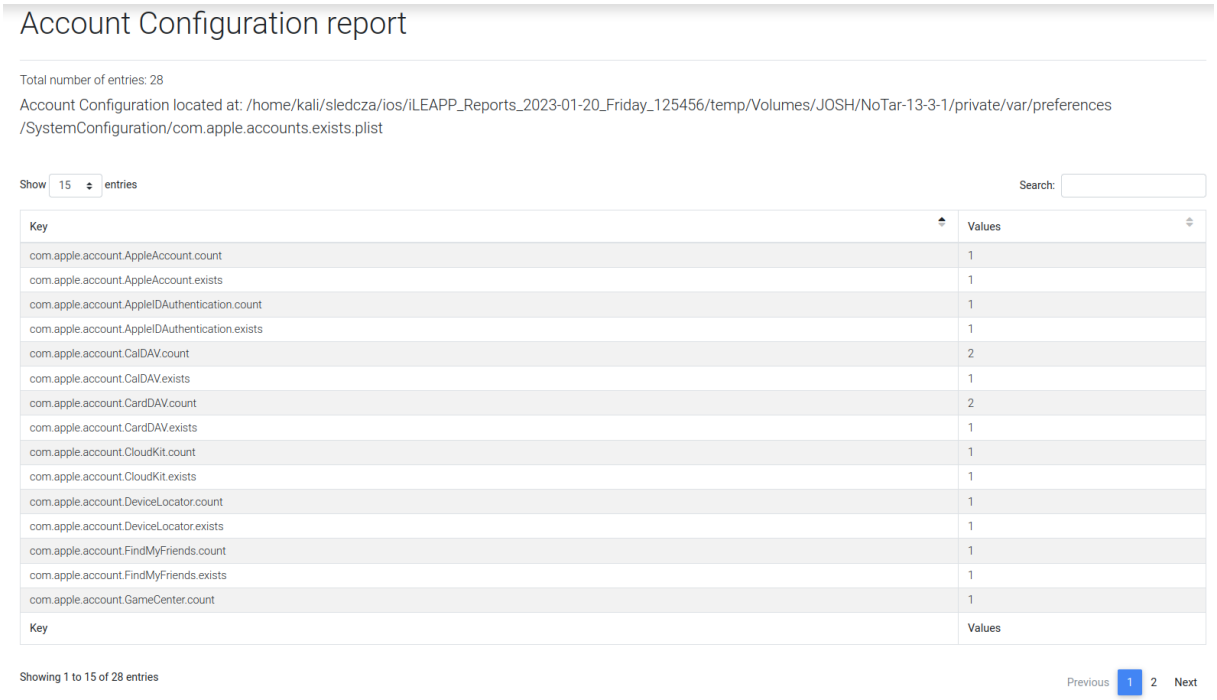
Nazwy użytkownika
Nazwy urządzenia
Modelu urządzenia

Hasła prawdopodobnie do sieci

iLEAPP

iLEAPP to aplikacja, która automatyzuje zbieranie informacji o urządzeniach z systemem iOS. Przedstawia je w formie raportu

Informacje o tym czy konto w danej aplikacji istnieje i ile ich jest. Te informacje zostały pokazane wcześniej za pomocą plistutil:



Account Configuration report

Total number of entries: 28

Account Configuration located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/preferences/SystemConfiguration/com.apple.accounts.exists.plist

Show 15 entries

Search:

Key	Values
com.apple.account.AppleAccount.count	1
com.apple.account.AppleAccount.exists	1
com.apple.account.AppleIDAuthentication.count	1
com.apple.account.AppleIDAuthentication.exists	1
com.apple.account.CalDAV.count	2
com.apple.account.CalDAV.exists	1
com.apple.account.CardDAV.count	2
com.apple.account.CardDAV.exists	1
com.apple.account.CloudKit.count	1
com.apple.account.CloudKit.exists	1
com.apple.account.DeviceLocator.count	1
com.apple.account.DeviceLocator.exists	1
com.apple.account.FindMyFriends.count	1
com.apple.account.FindMyFriends.exists	1
com.apple.account.GameCenter.count	1
Key	Values

Showing 1 to 15 of 28 entries

Previous 1 2 Next

Account3.sqlite
faktycznie istnieje tylko jeden email, tak jak wskazałem wcześniej
Na podstawie podanego timestampa wywnioskować można, że wcześniejsza liczba w bazie oznacza czas w sekundach od 1 stycznia 2001 roku (Prawdopodobnie ta data została wybrana, ponieważ tego dnia rozpoczęłą się drugie tysiąclecie

Account Data located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/Accounts/Accounts3.sqlite

Show All entries Search:

Timestamp	Account Desc.	Username	Description	Identifier	Bundle ID
2020-03-22 01:39:51	iTunes Store		Local	iTunesLocal-421A04EA-479A-4E46-B49D-556F7144518D	locationd
2020-03-22 01:47:42	iTunes Store	thisisdfir@gmail.com		6B35410D-85C2-4DCD-823A-CE1D598597E5	com.apple.purplebuddy
2020-03-22 01:47:42	Messages	thisisdfir@gmail.com		381B0D37-7962-43E6-BF7D-139B59033D1C	com.apple.identityservicesd
2020-03-22 01:47:42	CloudKit	thisisdfir@gmail.com		3B835298-47A1-458F-ADAB-0DEF5B898C2F	com.apple.accounts.accountsd
2020-03-22 01:47:55	Find My Friends	thisisdfir@gmail.com		798A0EA2-0B24-4857-B19C-3C048732B77D	com.apple.accounts.accountsd
2020-03-22 01:47:55	Device Locator	thisisdfir@gmail.com		94F572A1-6ECA-4ECC-B7B3-FF927D48C7E4	com.apple.accounts.accountsd
2020-03-22 01:47:55	IMAPNotes			8618BBCD-F392-48D3-8D75-4346ADE75FC8	com.apple.accounts.accountsd
2020-03-22 01:47:55	CalDAV			E9B5703B-F844-4845-AD3D-08DE58806F82	com.apple.accounts.accountsd
2020-03-22 01:47:55	CardDAV			EE84958A-E52C-425E-9171-70DEB1CB5DEB	com.apple.accounts.accountsd
2020-03-22 01:47:57	iCloud	thisisdfir@gmail.com	iCloud	1589F4EC-8F6C-4F37-929F-C6F121B36A59	com.apple.purplebuddy
2020-03-22 01:47:57	IDMS	thisisdfir@gmail.com		8F4A8F1B-DAD9-40F6-A06E-18B6A73D044F	com.apple.AuthKit
2020-03-22 01:47:58	Apple ID	thisisdfir@gmail.com		5B9A4BE7-A9AC-4798-A8EE-67EB19537748	com.apple.AuthKit
2020-03-22 01:49:16	Holiday Calendar		Holiday Calendar	A57F9D65-8AB3-4D80-897A-70F512299C37	dataaccessd
2020-03-22 01:59:47	Game Center	thisisdfir@gmail.com	thisisdfir@gmail.com	9BBC69AE-9F27-497B-8B94-D8AD8156181E	com.apple.AuthKit
2020-03-22 05:11:29	CalDAV			03CF4555-027D-4CBB-87FD-462FC610F64D	com.apple.accounts.accountsd
2020-03-22 05:11:29	IMAPNotes			CEA1DA02-7BCC-4C0B-8CB0-2677865D0E03	com.apple.accounts.accountsd
2020-03-22 05:11:29	CardDAV			98491756-59C0-4798-9EB6-1714C936158F	com.apple.accounts.accountsd
2020-03-22 05:11:29	Gmail	thisisdfir@gmail.com	Gmail	4FD35256-CE13-47FE-9840-EBEB5B9FD9C1	com.apple.Preferences
Timestamp	Account Desc.	Username	Description	Identifier	Bundle ID

Showing 1 to 18 of 18 entries Previous 1 Next

Numer telefonu
Widoczny jest tutaj numer telefonu właściciela.
Z numeru można wyciągnąć dużo informacji
+1 oznacza, że numer jest zarejestrowany w Ameryce Północnej
919 oznacza USA, Karolinę Północną
579 Oznacza Sanford
Mamy więc bardzo przybliżoną lokalizację, gdzie zarejestrowany jest numer

Address Book Contacts report

Total number of entries: 2

Address Book Contacts located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/AddressBook/AddressBook.sqlitedb

Show 15 entries 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

Showing 1 to 2 of 2 entries Previous 1 Next

Informacje o alarmie

Alarms report

Total number of entries: 1

Alarms located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/Preferences/com.apple.mobiletimerd.plist

Show 15 entries Search:

Alarm Title	Alarm Enabled	Fire Date	Dismiss Date	Last Modified	Repeat Schedule	Alarm Sound	Is Sleep Alarm	Bedtime Not Disturbed	Bedtime Fire Date
Test Alarm	False	2020-04-12 13:30:00	2020-04-12 13:30:07.734946	2020-04-12 13:30:07.739067	Never	system:Radar	False	False	
Alarm Title	Alarm Enabled	Fire Date	Dismiss Date	Last Modified	Repeat Schedule	Alarm Sound	Is Sleep Alarm	Bedtime Not Disturbed	Bedtime Fire Date

Showing 1 to 1 of 1 entries Previous 1 Next

Właściciel łączył z telefonem prawdopodobnie zegarek

App Conduit report

The AppConduit log file stores information about interactions between iPhone and other iOS devices, i.e. Apple Watch

Total number of entries: 1

App Conduit located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/Logs/AppConduit/AppConduit.log.0, /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/Logs/AppConduit/AppConduit.log.1

Show 15 entries Search:

Device ID	Device type and version	Device extra information
752E8F13-7BDE-4974-A011-A03492737221	Watch4,3	40mm

Showing 1 to 1 of 1 entries Previous 1 Next

Total number of entries: 40

Show All entries Search:

Time	Device interaction	Device ID	Log File Name
2020-04-03 10:18:35	Disconnected	752E8F13-7BDE-4974-A011-A03492737221	AppConduit.log.1
2020-04-03 10:19:43	Connected	752E8F13-7BDE-4974-A011-A03492737221	AppConduit.log.1
2020-04-03 14:14:33	Disconnected	752E8F13-7BDE-4974-A011-A03492737221	AppConduit.log.1
2020-04-03 14:16:41	Connected	752E8F13-7BDE-4974-A011-A03492737221	AppConduit.log.1
2020-04-03 14:17:12	Disconnected	752E8F13-7BDE-4974-A011-A03492737221	AppConduit.log.1
2020-04-03 14:17:16	Connected	752E8F13-7BDE-4974-A011-A03492737221	AppConduit.log.1
2020-04-03 14:17:46	Disconnected	752E8F13-7BDE-4974-A011-A03492737221	AppConduit.log.1

Dużo informacji na temat uprawnień aplikacji:

TCC - Permissions report

Total number of entries: 130

TCC - Permissions located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/TCC/TCC.db

Show 15 entries Search:

Bundle ID	Permissions	Last Modified Timestamp
ch.protonmail.protonmail	kTCCServiceAddressBook	2020-04-05 19:17:19
ch.protonmail.protonmail	kTCCServicePhotosAdd	2020-04-05 19:27:17
ch.protonmail.protonmail	kTCCServicePhotos	2020-04-05 19:39:37
co.babypenguin.imo	kTCCServiceUbiquity	2020-03-22 01:27:41
co.babypenguin.imo	kTCCServiceAddressBook	2020-03-22 15:15:10
co.babypenguin.imo	kTCCServiceCamera	2020-03-22 17:23:44
co.babypenguin.imo	kTCCServiceMicrophone	2020-03-22 17:23:45
co.babypenguin.imo	kTCCServicePhotos	2020-03-22 18:20:12
com.adhoclabs.burner	kTCCServiceAddressBook	2020-04-12 01:03:13
com.apple.accessibility.AccessibilityUIServer	kTCCServiceLiverpool	2020-04-12 15:38:51
com.apple.DocumentsApp	kTCCServiceUbiquity	2020-03-21 21:48:15
com.apple.Health	kTCCServiceMotion	2020-04-07 00:29:08
com.apple.iCloudNotification	kTCCServiceLiverpool	2020-04-12 18:05:06
com.apple.MailCompositionService	kTCCServiceUbiquity	2020-03-21 21:48:14
com.apple.Maps	kTCCServiceLiverpool	2020-04-01 17:33:17
Bundle ID	Permissions	Last Modified Timestamp

Showing 1 to 15 of 130 entries

Previous 1 2 3 4 5 … 9 Next

Właściciel interesował się cyberbezpieczeństwem, na podstawie oglądanych podcastów:

Apple Podcasts - Episodes report

Total number of entries: 1024

Apple Podcasts - Episodes located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Containers/Shared/AppGroup/01E684DD-87C4-4387-93C7-BAC81954D68E/Documents/MTLibrary.sqlite

Show 15 entries Search:

Import Date	Metadata Timestamp	Date Last Played	Play State Last Modified	Download Date	Play Count	Author	Title	Subtitle	Asset URL	Web Page URL	Duration	Size
2020-03-25 19:18:32			2020-03-25 19:18:32		0		DFSP # 120 - Rita	This week I talk about Rita, a free Threat Hunting Tool from Black Hills Information Security		https://digitalforensicsurvivalpodcast.libsyn.com/dfsp-120-rita	1013.0	827666
2020-03-25 19:18:32			2020-03-25 19:18:32		0		DFSP # 138 - OWASP Top 10	This week I talk about OWASP and why you should be paying attention.		https://digitalforensicsurvivalpodcast.libsyn.com/dfsp-138-owasp-top-10	1185.0	967863
2020-03-25 19:18:32			2020-03-25 19:18:32		0		DFSP # 024 - RAM Extraction Tools - Part 1	This episode is a two-parter looking at RAM extraction tools. Part 1 will take a look at why RAM extraction is an important part of forensic analysis. Part 2 will go over an experiment I did		https://digitalforensicsurvivalpodcast.libsyn.com/dfsp-024-ram-extraction-tools-part-1	1244.0	102007

Numer podpiętej karty kredytowej:

Cards report

Total number of entries: 1

Cards located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/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 Previous 1 Next

Podłączone urządzenia Bluetooth:

Bluetooth Paired report

Total number of entries: 4

Bluetooth Paired located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/containers/Shared/SystemGroup/97313D94-1DE6-4735-814C-74A5E3C0A85F/Library/Preferences/com.apple.MobileBluetooth.devices.plist

Show 15 entries Search:

Last Seen Time	MAC Address	Name Key	Name	Device Product ID	Default Name
	B4:EC:02:73:FF:93				
	F8:6F:C1:4E:FF:6A		Apple Watch		
2020-03-30 05:14:06	7C:04:D0:89:89:A0		Josh's AirPods	8194	Headphones
2020-04-10 08:59:13	38:EC:0D:E2:49:CF	This Is's AirPods Pro	AirPods Pro	8206	Headphones
Last Seen Time	MAC Address	Name Key	Name	Device Product ID	Default Name

Showing 1 to 4 of 4 entries Previous 1 Next

Bluetooth Paired LE report

Total number of entries: 5

Bluetooth Paired LE located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/containers/Shared/SystemGroup/97313D94-1DE6-4735-814C-74A5E3C0A85F/Library/Database/com.apple.MobileBluetooth.ledevices.paired.db

Show 15 entries Search:

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
UUID	Name	Name Origin	Address	Resolved Address	Last Connection Time

Showing 1 to 5 of 5 entries Previous 1 Next

Wszystkie wydarzenia z kalendarza:

Calendar Items report

Total number of entries: 119

Calendar Items located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/Calendar/Calendar.sqlitedb

Show All entries Search:

Start Date	Start Timezone	End Date	End Timezone	All Day?	Summary	Calendar ID	Last Modified
2018-01-01 00:00:00	_float	2018-01-01 23:59:59	_float	1	New Year's Day	14	2019-05-31 22:46:33
2018-01-15 00:00:00	_float	2018-01-15 23:59:59	_float	1	Martin Luther King, Jr. Day	14	2019-05-31 22:46:33
2018-02-02 00:00:00	_float	2018-02-02 23:59:59	_float	1	Groundhog Day	14	2019-05-31 22:46:33
2018-02-14 00:00:00	_float	2018-02-14 23:59:59	_float	1	Valentine's Day	14	2019-05-31 22:46:33
2018-02-16 00:00:00	_float	2018-02-16 23:59:59	_float	1	Lunar New Year	14	2019-05-31 22:46:33
2018-02-19 00:00:00	_float	2018-02-19 23:59:59	_float	1	President's Day	14	2019-05-31 22:46:33
2018-03-02 00:00:00	_float	2018-03-02 23:59:59	_float	1	Holi	14	2019-05-31 22:46:33
2018-03-11 00:00:00	_float	2018-03-11 23:59:59	_float	1	Daylight Saving Time	14	2019-05-31 22:46:33
2018-03-17 00:00:00	_float	2018-03-17 23:59:59	_float	1	St. Patrick's Day	14	2019-05-31 22:46:33
2018-03-25 00:00:00	_float	2018-03-25 23:59:59	_float	1	Palm Sunday	14	2019-05-31 22:46:33
2018-03-30 00:00:00	_float	2018-03-30 23:59:59	_float	1	Good Friday	14	2019-05-31 22:46:33
2018-03-31 00:00:00	_float	2018-03-31 23:59:59	_float	1	Passover	14	2019-05-31 22:46:33
2018-04-01 00:00:00	_float	2018-04-01 23:59:59	_float	1	April Fools' Day	14	2019-05-31 22:46:33
2018-04-01 00:00:00	_float	2018-04-01 23:59:59	_float	1	Easter	14	2019-05-31 22:46:33
2018-04-08 00:00:00	_float	2018-04-08 23:59:59	_float	1	Orthodox Easter	14	2019-05-31 22:46:33
2018-04-17 00:00:00	_float	2018-04-17 23:59:59	_float	1	Tax Day	14	2019-05-31 22:46:33
2018-04-22 00:00:00	_float	2018-04-22 23:59:59	_float	1	Earth Day	14	2019-05-31 22:46:33

Historia połączeń

Właściciel wykonywał dużo połączeń do Saint Jose, California, które jest po drugiej stronie USA

Pojawiły się też połączenia do Fuquay-Varina, New Carolina, które jest bardzo blisko Sanford, NC

Są też połączenia do Goldsboro, NC, które również jest niedaleko oraz Fairway, NC, które jest dalej

Call History report

Total number of entries: 32

Call History located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/CallHistoryDB/CallHistory.storedata

Show All entries Search:

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

Numer IMEI

Key	Values
imei	355800076093966
imei_svn	23
imei_svns	[{'second': '23', 'first': '1:kOne'}]
imeis	[{'second': '355800076093966', 'first': '1:kOne'}]

EnhancedLQMLinkQualityFingerPrintRegistration	True

Udostępnione pliki

Note Sharing report

CloudKit Note Sharing - Notes information shared via CloudKit. Look up the Record ID in the ZICCLOUDSYYNCINGOBJECT.ZIDENTIFIER column.

Total number of entries: 8

Note Sharing located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Containers/Shared/AppGroup/1AA2421A-3D36-4566-B577-0BAC64154976/NoteStore.sqlite

Show 15 entries Search:

Record ID	Record Type	Creation Date	Creator ID	Modified Date	Modifier ID	Modifier Device
1589F4EC-8F6C-4F37-929F-C6F121B36A59	MigrationState	2020-03-28 00:36:28.382000	__defaultOwner__	2020-03-28 00:36:39.231000	__defaultOwner__	This Is's iPhone
2909234A-0865-4D1A-A5DE-840F123FAD42	Folder	2020-03-28 00:47:53.263000	__defaultOwner__	2020-03-28 00:48:42.095000	__defaultOwner__	This Is's iPhone
6CFCD8F3-864D-4064-9D03-F653F6C1CC23	PasswordProtectedNote	2020-03-28 00:50:34.056000	__defaultOwner__	2020-03-28 00:50:34.056000	__defaultOwner__	This Is's iPhone
_2059b5c2ab5206967ff351966be73cf9	Users	2020-03-28 00:36:27.358000	__defaultOwner__	2020-03-28 00:45:39.838000	__defaultOwner__	This Is's iPhone
BC49B362-F4C5-462A-80CB-03FF75C3D93E	PasswordProtectedNote	2020-03-28 00:45:42.187000	__defaultOwner__	2020-03-28 00:45:42.187000	__defaultOwner__	This Is's iPhone
DefaultFolder-CloudKit	Folder	2020-03-28 00:36:28.317000	__defaultOwner__	2020-03-28 00:36:54.667000	__defaultOwner__	This Is's iPhone
ED99B707-E353-401A-AAA8-5610066BD280	Note	2020-03-28 00:36:54.816000	__defaultOwner__	2020-03-28 00:37:45.085000	__defaultOwner__	This Is's iPhone
TrashFolder-CloudKit	Folder	2020-03-28 00:36:28.318000	__defaultOwner__	2020-03-28 00:45:42.049000	__defaultOwner__	This Is's iPhone
Record ID	Record Type	Creation Date	Creator ID	Modified Date	Modifier ID	Modifier Device

Showing 1 to 8 of 8 entries Previous 1 Next

Połączone urządzenia:

Connected Devices report

Total number of entries: 1

Connected Devices located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_
/iTunes_Control/iTunes/iTunesPrefs

Show 15 entries

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

Konfiguracja DHCP:

DHCP Received List report

Total number of entries: 6

DHCP Received List located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volun
/en0-1,a0_d7_95_79_dd_a1

Show 15 entries

Key	Value
IPAddress	192.168.11.20
LeaseLength	28800
LeaseStartDate	2020-04-12 19:04:02
RouterHardwareAddress	b'\xf8\xbb\xbf\x1e\xfa\xf0'
RouterIPAddress	192.168.11.1
SSID	CcookiesDcastleR5 Guest
Key	Value

Informacje z discorda
Połączony email
USER ID
Wysłane wiadomości

Discord Account report

Total number of entries: 4

Discord Account located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/\
/Data/Application/1A366D76-74D8-46EC-91C0-B1F8378D8828/Documents/mmkv/mmkv.default

Show 15 entries

Key	Value
EMAIL_CACHE	thisisdfir@gmail.com
EMAIL_CACHE	thisisdfir@gmail.com
USER_ID_CACHE	672145484864815124
USER_ID_CACHE	672145484864815124
Key	Value

				Thanks for helping out.				
2020-02-01T01:42:59.779000+00:00		josh_hickman1			https://cdn.discordapp.com/attachments/622810296226152474/672980186001702912/image0.jpg	579257851646574644	622810296226152474	
2020-02-01T02:09:38.714000+00:00		ThisIsDFIR		Thanks!		672145484864815124	622810296226152474	
2020-02-01T02:18:18.030000+00:00		ThisIsDFIR			https://cdn.discordapp.com/attachments/622810296226152474/672989069986496512/Nintendo-Famicom-Disk-System.jpg	672145484864815124	622810296226152474	
2020-03-22T13:06:41.072000+00:00		josh_hickman1		Good morning!		579257851646574644	622810296226152474	
2020-03-22T13:07:53.078000+00:00		ThisIsDFIR		Good morning. How are you? The pollen is in full force so my allergies are kicking!		672145484864815124	622810296226152474	
2020-03-22T13:09:34.142000+00:00		josh_hickman1			https://cdn.discordapp.com/attachments/622810296226152474/691272360807890944/image0.png	579257851646574644	622810296226152474	
2020-03-22T13:12:22.413000+00:00		ThisIsDFIR		Got it. Thank you!		672145484864815124	622810296226152474	
Timestamp	Edited Timestamp	Username	Bot?	Content	Attachments	User ID	Channel ID	Emb Auth

Na facebooku również można znaleźć zapisy z konwersacji

Timestamp	Sender Name	Sender ID	Message	Attachment	Attachment Name	Attachment Size	Title Text
2020-02-01 18:49:07	ThisIs Dfir	100030845613112	Hi there!				
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.				
2020-02-01 18:50:24	Josh Hickman	100030845613112	Hey, how are you?				
2020-02-01 18:51:18	ThisIs Dfir	100030845613112	Good. Hope you are.				
2020-02-01 18:52:05	Josh Hickman	100030845613112	I am. Thanks!				
2020-02-01 18:57:46	Josh Hickman	100030845613112		Yes	image-517951378846562	59655	
2020-02-01 18:59:43	ThisIs Dfir	100030845613112		Yes	image-486276645606085	40025	
2020-02-09 18:10:03	ThisIs Dfir	100030845613112		Yes		0	Location sharing ended
2020-03-22 14:26:57	ThisIs Dfir	100030845613112	Switched over to FB Messenger.				
2020-03-22 14:28:39	Josh Hickman	100030845613112	I see. I also see some of our previous Android 10 convo's are here.				
2020-03-22 14:29:13	ThisIs Dfir	100030845613112	Yep!				
2020-03-22 14:42:10	ThisIs Dfir	100030845613112	Lol!!				
2020-03-22 14:42:56	ThisIs Dfir	100030845613112		Yes	image-553242018649906	104371	
2020-03-22 14:44:42	Josh Hickman	100030845613112	That's about right. Wonder if it will actually happen this year.				
2020-03-22 14:47:01	ThisIs Dfir	100030845613112	Good question.				
Timestamp	Sender Name	Sender ID	Message	Attachment	Attachment Name	Attachment Size	Title Text

Sekretne konwersacje są zaszyfrowane

Widnieje tu też dokument

Files App - Filenames report

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

Total number of entries: 1

Files App - Filenames located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/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 Las Hit Date	Creation Date	Modification Date	User Info	Child Item Count	Flags
2020-04-12 09:22:19.983254	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, 'cstm': 0}	2	{'_userExecutable': False, '_userWritable': True, '_hidden': False, '_pathExtensionHidden': True, '_userReadable': True}
Last Hit Date	Folder ID	Filename	Frequency at Las Hit Date	Creation Date	Modification Date	User Info	Child Item Count	Flags

Showing 1 to 1 of 1 entries

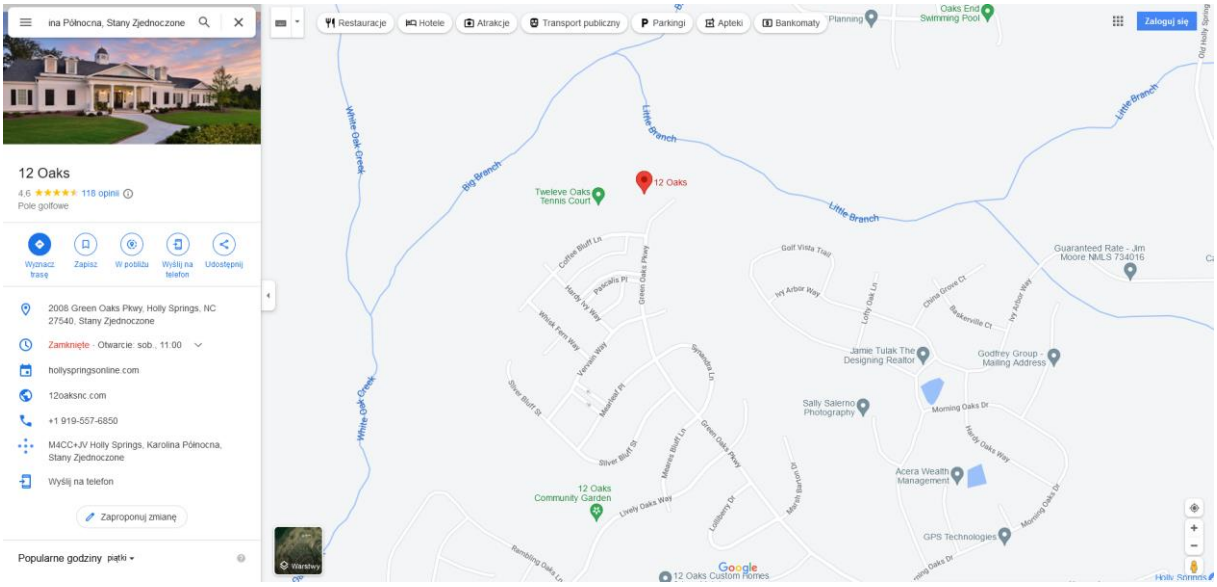
Previous 1 Next

Widoczna jest lokalizacja z metadanych ze zdjęć

Show 15 entries Search:

last access time	requestkey	pdplacehash	expire time	pd place
2020-04-12 13:35:17	d184b3db348781c24ab34bdc576a0ca5	muid-1784751386105042749 9	2020-04-13 01:54:18	Ehttps://s3-media0.fl.yelpcdn.com/bphoto/DfVosRhjOvWMXblt6zYafg/ls.jpg0 $67DDB5CC-9100-44C9-A7C0-7ABBDDC46A1E BU"S Green Oaks ParkwayZ golfb Twelve Oaks: \tn=normal\ Green Oaks Parkway Holly Springs: \tn=normal\ Green Oaks Parkway* pAZ8 A@13 Golf" golf placesJ com.yelp 12 Oaks Country ClubZ United States LI-YN3_tpe3N22-UybYxKg"%yelp5.3:///biz/LI-YN3_tpe3N22-UybYxKg"#yelp4:///biz/LI-YN3_tpe3N22-UybYxKg"'yelp:///biz/LI-YN3_tpe3N22-UybYxKg"*http://yelp.com/biz/LI-YN3_tpe3N22-UybYxKgB2 Wake2 12 Oaks Country Club Holly SpringsB o.Yp active.golf https://theclubat12oaks.com/R 2004b DfVosRhjOvWMXblt6zYafg New clubhouse!* LI-YN3_tpe3N22-UybYxKg` 37183J places2 fromLegacy" North Carolina* 7.3.2 Golf*

Dla przykładu to zdjęcie zostało zrobione tutaj:



Parametry dotyczące zdrowia:
Głośność muzyki

Bicie serca

Health - Heart Rate report

Total number of entries: 3665

Health - Heart Rate located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/Health/healthdb_secure.sqlite

Show 15 entries Search:

Start Timestamp	End Timestamp	Type	Heart Rate	Key	Data ID
2020-03-22 00:52:59	2020-03-22 00:52:59	Heart Rate	73.0	_HKPrivateHeartRateContext	23
2020-03-22 00:57:17	2020-03-22 00:57:17	Heart Rate	71.0	_HKPrivateHeartRateContext	35
2020-03-22 01:00:10	2020-03-22 01:00:10	Heart Rate	69.0	_HKPrivateHeartRateContext	40
2020-03-22 01:06:03	2020-03-22 01:06:03	Heart Rate	65.0	_HKPrivateHeartRateContext	47
2020-03-22 01:10:31	2020-03-22 01:10:31	Heart Rate	57.0	_HKPrivateHeartRateContext	54
2020-03-22 01:16:36	2020-03-22 01:16:36	Heart Rate	61.0	_HKPrivateHeartRateContext	64
2020-03-22 01:19:31	2020-03-22 01:19:31	Heart Rate	65.0	_HKPrivateHeartRateContext	72
2020-03-22 01:23:40	2020-03-22 01:23:40	Heart Rate	60.0	_HKPrivateHeartRateContext	78
2020-03-22 01:29:52	2020-03-22 01:29:52	Heart Rate	63.0	_HKPrivateHeartRateContext	85
2020-03-22 01:33:31	2020-03-22 01:33:31	Heart Rate	61.0	_HKPrivateHeartRateContext	91
2020-03-22 01:40:23	2020-03-22 01:40:23	Heart Rate	65.0	_HKPrivateHeartRateContext	98
2020-03-22 01:47:27	2020-03-22 01:47:27	Heart Rate	62.0	_HKPrivateHeartRateContext	106
2020-03-22 01:52:11	2020-03-22 01:52:11	Heart Rate	63.0	_HKPrivateHeartRateContext	117
2020-03-22 01:56:49	2020-03-22 01:56:49	Heart Rate	67.0	_HKPrivateHeartRateContext	123
2020-03-22 01:58:33	2020-03-22 01:58:33	Heart Rate	61.0	_HKPrivateHeartRateContext	128
Start Timestamp	End Timestamp	Type	Heart Rate	Key	Data ID

Health - Workouts report

Total number of entries: 6

Health - Workouts located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Library/Health/healthdb_secure.sqlite

Show 15 entries Search:

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	Goal	Flights Climbed
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	Workout Type	Workout Duration	Duration (In Mintues)	Distance (In KM)	Distance (In Miles)	Calories Burned	Total Basel Energy Burned	Goal Type	Goal	Flights Climbed

Showing 1 to 6 of 6 entries Previous 1 Next

Właściciel lubi biegać

Numer osoby, z którą Josh się kontaktował

Contact Name	Contact Alias	Contact Phone	Profile Pic URL
Josh Hickman	John Hicks	(919) 579-0479	
Josh Hickman	Lil Enusynt	(919) 391-2507	https://cdn.imoim.us/s/object/.43ExumInRuRjDhVlPRBpxbPiFdn/
Contact Name	Contact Alias	Contact Phone	Profile Pic URL

Więcej chatów:

IMO HD Chat - Messages report

Total number of entries: 5

IMO HD Chat - Messages located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/mobile/Containers/Shared/AppGroup/ABDEB3FD-6DB8-45A7-BD0F-F06125AC4C5D/IMODb2.sqlite

Show 15 entries Search:

Timestamp	Sender Name	Sender Alias	Sender Phone	Message	Message Status	Item Action	Attachment URL	Attachment
2020-03-22 17:23:26	Josh Hickman	Josh Hickman	9195790479	Took a break. I'm back now.	Received			
2020-03-22 17:24:57				Ok good. I was having some service issues but I think it's ok now.	Sent			
2020-03-22 18:02:52	Josh Hickman	Josh Hickman	9195790479	uploaded photo: https://cdn.imoim.us/s/object/.42VJIUYYejXeKmGOCzinzrnXDjE/	Received	photo_uploaded	https://cdn.imoim.us/s/object/.42VJIUYYejXeKmGOCzinzrnXDjE/	
2020-03-22 18:20:27					Sent	photo_uploaded	https://cdn.imoim.us/s/object/.40wFDgEsqKmgqJGbcXaBPLINOKF/	
2020-03-30 11:26:18	Josh Hickman	Josh Hickman	9193912507	is now on imo!	Received	just_joined		
Timestamp	Sender Name	Sender Alias	Sender Phone	Message	Message Status	Item Action	Attachment URL	Attachment

Wersja systemu

iOS Build report

Total number of entries: 9

iOS Build located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/private/var/installd/Library/MobileInstallation/LastBuildInfo.plist

Show 15 entries Search:

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

Previous 1 Next

Chat z instagrama:

Timestamp	Sender ID	Username	Message	Chat Title
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 friends list, or whatever it is called.	

Najwyraźniej właściciel nie rozumie czemu ludzie używają tej aplikacji

Screenshoty

App Snapshots (screenshots) report

Josh Hickman
You called Josh
1 sec
Your free call sponsored by
Call Recorder
TapeACall makes it easy to record calls you're already on, or calls yo...
Josh called you
1 min 20 sec
Call back
Today 8:31 PM
Message just to keep my number.
Type a message

Inbox
Edit
Mailboxes
Apple
2:03 AM
Your receipt from Apple.
Your Apple ID was used to purchase 3
Credit Pack. Receipt Save 3% on all yo...
Facebook
Friday
Holly Springs Residents and 7 others a...
This!, join groups to connect with
people who share your interests. Face...
Venmo
Thursday
Your March 2020 Transaction History
Hi Joshua, Your transaction history for
March 2020 is now available. View Hist...
Fitbit
Thursday
Congrats on earning your Marathon ba...
Share: Impressive! You've earned the
Marathon badge You're 26 miles into y...
Updated Just Now

Josh
My phone has gotten hot and the battery drain is crazy.
Wow. We should move on quickly.
Mar 24, 2020 at 9:17 pm
Send a Message

Josh Hickman
online
Thu, Mar 26
JUST DON'T DO IT.
8:38 PM
Today
2:23 PM
Live location ended
2:24 PM

2:34 PM
Holly Springs
72°
11:34 AM
Santa Clara
59°
2:34 PM
New York
55°
11:34 AM
Cupertino
59°
°C | °F
The Weather Channel

John Hicks
Fart
SOUNDCLOUD
John Hicks
Lol!! Fantastic!
TODAY
Here I am
Rambling Oaks Ln
Maps
Legal
Type Message
Me
We
GIF

Inbox
Josh Hickman
number.
Got it. It's showing up as a 704 number. Is that right?
Yes. I can not send pictures or videos.
My subscription is not high enough.
That is fine. Just do a call and we will call it a day.
Completed call
Missed Call
Voicemail 9:15 PM
Speaker off
Type message here
Send

Meatleaf Pl
Sour Mash Ct
Holly Springs New Hill Rd
68°
AQI 42
Search for a place or address

Kik Messages report

Kik Messages

Total number of entries: 6

Kik Messages located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023
/AppGroup/52B76AC9-C286-47D5-9C26-02FF13BCD37C/cores/private

Show 15 entries

Received Time	Timestamp	Message	Type
2020-03-22 19:14:55	2020-03-22 19:14:55	I forgot there are ads in Kik now.	Sent
2020-03-22 19:15:50	2020-03-22 19:15:50	Yeah, unfortunately. They take up most of the chat screen.	Received
2020-03-22 19:16:46	2020-03-22 19:16:46	I wonder if they're going to offer an ad-free version at some point.	Sent
2020-03-22 19:17:36	2020-03-22 19:17:35	Seems reasonable.	Received
2020-03-22 19:18:03	2020-03-22 19:18:03		Sent

Apple Maps Search History report

Total number of entries: 14

Apple Maps Search History located at: /home/kali/sledcza/ios/iLEAPF
/Data/Application/9059248A-7FA9-455C-A212-6805F124F180/Library

Show 15 entries

Timestamp	App	Location	Short Address	Place Name	Latitud
2020-04-01 17:45:35.736000		Manhattan Pizza, Holly Springs			
2020-04-01 17:45:35.736000		Manhattan Pizza, Holly Springs			

Wiele informacji wskazuje na to, że Josh mieszka w Holly Springs

Safari Browser located at

Show 15 entries

Visit Time	Search Term
2020-03-28 00:58:36	when does mlb start 2020
2020-03-28 00:58:37	when does mlb start 2020
2020-03-28 01:00:17	when does mlb start 2020
2020-03-28 01:02:05	when does mlb start 2020
2020-03-28 01:02:44	Is the NHL going to resume%3F
2020-03-28 01:02:44	Is the NHL going to resume%3F

Interesuje się też sportem (MLB – Major League Baseball, NHL – National Hockey League)

Po wiadomościach na tik toku można wywniosokować, że Josh nie jest młody

Show 15 entries

Timestamp	Sender	Custom ID	Nickname	Message
2020-02-08 21:07:02	6791183665130374150	user8828007582568	user8828007582568	
2020-02-08 21:08:52	6787436503258760198	user2812914319221	ThisIsDFIR	People love this app. I don't see the appeal.
2020-02-08 21:11:38	6787436503258760198	user2812914319221	ThisIsDFIR	I do not see the appeal of this app.
2020-02-08 21:12:42	6791183665130374150	user8828007582568	user8828007582568	That's because you are old.
2020-04-12 01:46:29	6787436503258760198	user2812914319221	ThisIsDFIR	Let's just get this over with.
2020-04-12 01:51:12	6629695160186863622	user8242525	user824252	
2020-04-12 01:52:25	6787436503258760198	user2812914319221	ThisIsDFIR	Can we please knock this one out and move on?
2020-04-12 01:53:44	6629695160186863622	user8242525	user824252	Absolutely.
2020-04-12 01:54:32	6787436503258760198	user2812914319221	ThisIsDFIR	Awesome.

Show 15 entries

Timestamp	Sender Name	From ID	Receiver	To ID	Message
2020-03-26 18:42:57	Josh Hickman	19195790479@s.whatsapp.net	Local User	19195794674@s.whatsapp.net	
2020-03-26 18:42:57	Local User		Josh Hickman	19195790479@s.whatsapp.net	What's up?!
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?
2020-03-26 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.
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 18:47:12	Local User		Josh Hickman	19195790479@s.whatsapp.net	Not yet but the effects of this will be felt later I'm sure.

iOS Mail report

Total number of entries: 176

iOS Mail located at: /home/kali/sledcza/ios/iLEAPP_Reports_2023-01-20_Friday_125456/temp/Volumes/JOSH/NoTar-13-3-1/pri

Show 15 entries

Date Sent	Date Received	Address	Comment	Subject	Summary
2020-01-29 15:41:06	2020-01-29 15:41:07	no-reply@accounts.google.com	Google	Security alert	New device signed in to thisisdfir@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
2020-01-29 15:41:06	2020-01-29 15:41:07	no-reply@accounts.google.com	Google	Security alert	New device signed in to thisisdfir@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
2020-01-29 18:27:44	2020-01-29 18:27:46	noreply@discordapp.com	Discord	Verify Email Address for Discord	Hey ThisIsDFIR, Thanks for registering for an account on Discord! Before we get started, we just need to confirm that this is you. Click below to verify your email address: Verify Email Need help? Contact our support team or hit us up on Twitter @discordapp. Want to give us feedback? Let us know what you think on our feedback site. FUN FACT #17 Starting with version 6.29 of the original Dota, each update ending in a "9" contained a secret quest, usually showing off an upcoming hero such as Invok
2020-01-29 18:27:44	2020-01-29 18:27:46	noreply@discordapp.com	Discord	Verify Email Address for Discord	Hey ThisIsDFIR, Thanks for registering for an account on Discord! Before we get started, we just need to confirm that this is you. Click below to verify your email address: Verify Email Need help? Contact our support team or hit us up on Twitter @discordapp. Want to give us feedback? Let us know what you think on our feedback site. FUN FACT #17 Starting with version 6.29 of the original Dota, each update ending in a "9" contained a secret quest, usually showing off an upcoming hero such as Invok

Znajdują się tu też maile

To wszystkie ciekawe rzeczy na temat Josha