חילוץ הנתונים **ממכשיר פרוץ (rooted)**

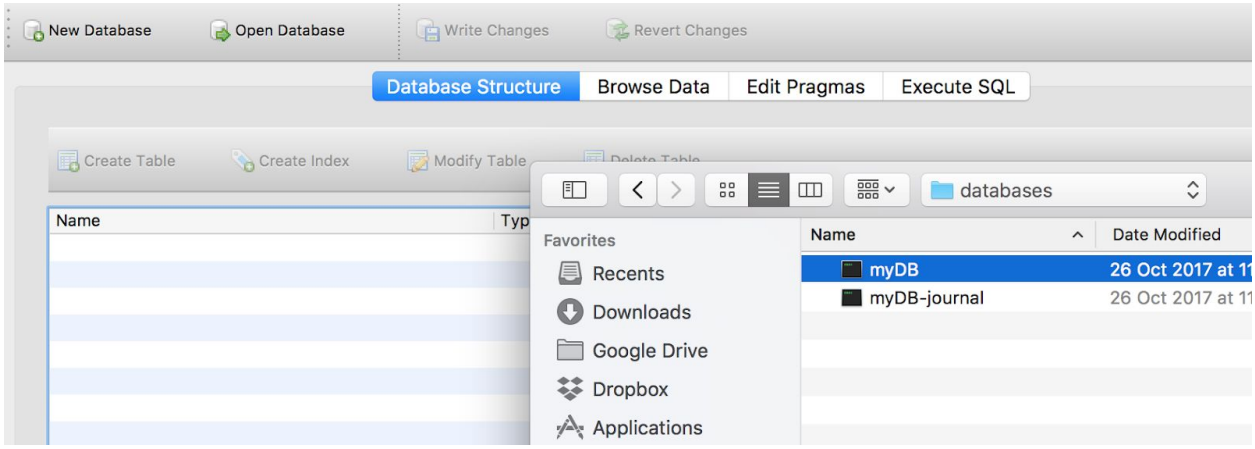
יש לוודא שהאפליקציה Switcher V2 מותקנת על מכשיר והאנדרואיד שלכם, מוגדרת לפעולה ושהמכשיר פרוץ (rooted)

באמצעות סייר קבצים root explorer או באמצעות adb יש לגשת למיקום הבא:

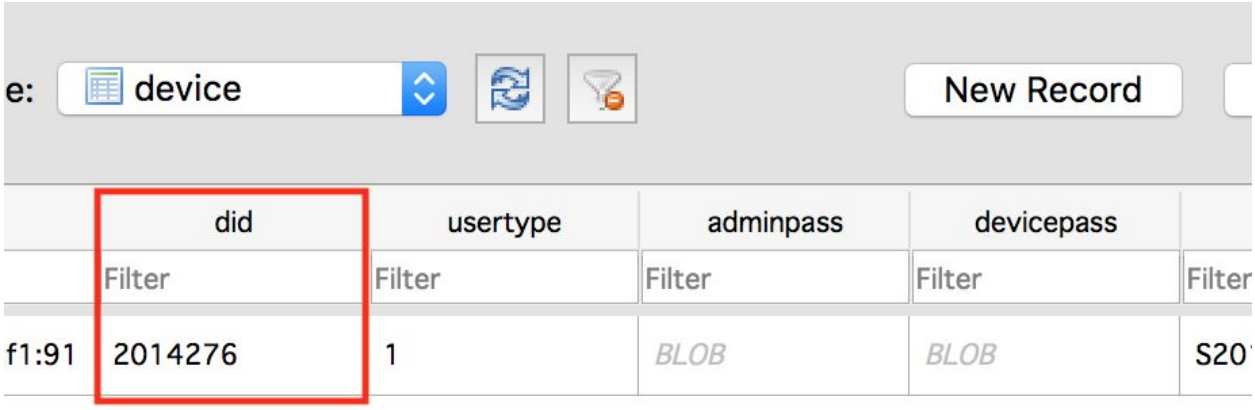
/data/data/com.ogemary.smarthome/databases/

להוריד או לשלוח לעצמכם למייל או לגוגל דרייב את הקובץ: **myDB**

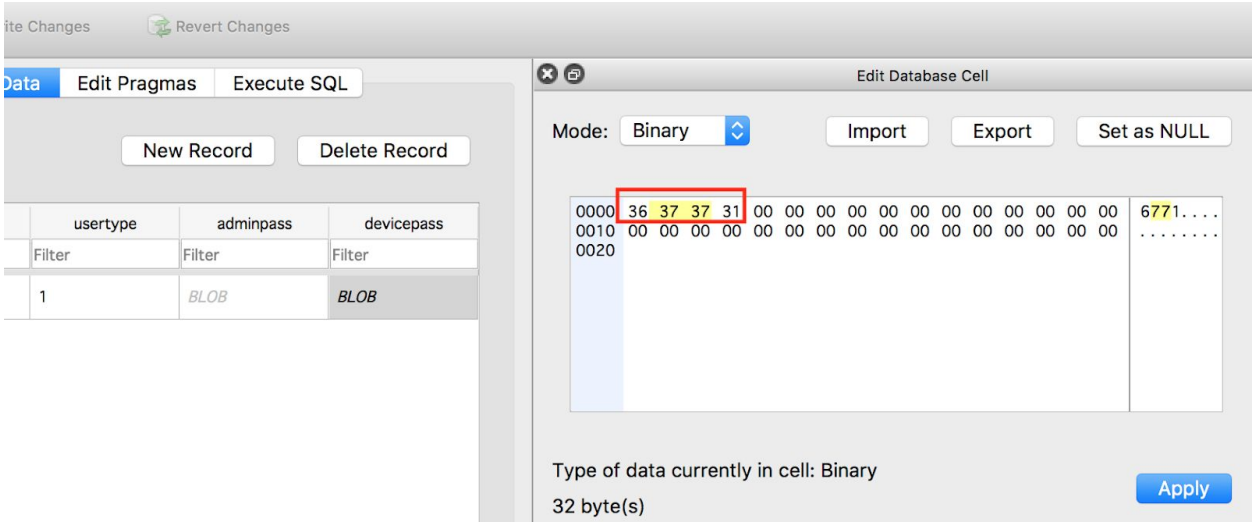
יש להוריד למחשב את התוכנה "**SQLite Database Browser**" ובאמצעותה לפתוח את הקובץ **myDB** שהורדתם ממכשיר האנדרואיד



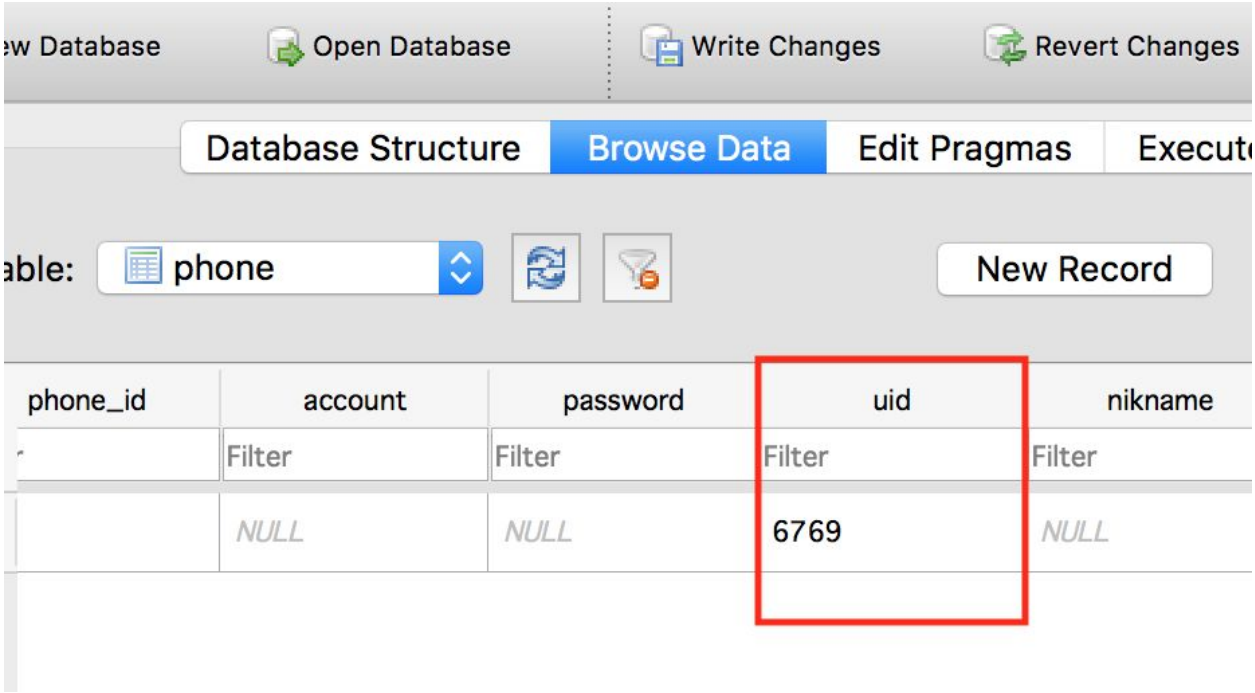
יש לבחור בלשונית "Browse Data" ולבחור ב Table שנקרא "**device**"
שם למצוא את העמודות שנקראות "**did**" ו "**devicepass**" ולהעתיק את הנתונים.



על מנת להעתיק את הנתונים מעמודת ה **devicepass** יש לעבור למצב **Binary** ולהעתיק את **4 הבתים הראשונים (8 ספרות) ללא הרווחים**



לאחר מכן יש לעבור ל Table שנקרא "**phone**" ולחלץ את הנתון מעמודת "**uid**"



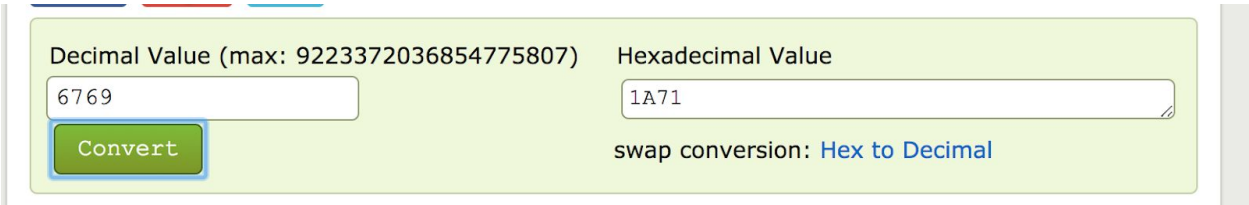
כעת יש לבצע המרה לערכים **uid** ו **did** שחילצנו מה Database לפורמט של hex ניתן לבצע זאת באמצעות האתר הבא:

https://www.binaryhexconverter.com/decimal-to-hex-converter

ולאחר מכן את ערכי ה HEX שהתקבלו עבור ה **uid** וה **did** יש להמיר ל Little Endian באמצעות האתר הזה:

https://www.scadacore.com/tools/programming-calculators/online-hex-converter/

דוגמה להמרה של ה **UID** ל HEX:



המרת ערך ה hex של **uid** ל Little Endian יש להעתיק את התוצאה ללא האפסים שהתווספו אליה:

HexString Input

1A71

AnalyzeData

ASCII	Binary		
q	#	Raw	Binary
	0	1A 71	0001101001110001

Float - Big Endian (ABCD)			Float - Little Endian (DCBA)			Float - Mid-Big Endian (BADC)			Float - Mid-Little Endian (CDAB)		
#	Raw	Float	#	Raw	Float	#	Raw	Float	#	Raw	Float
0	1A 71 00 00	4.98376319e-23	0	00 00 71 1A	4.05732e-41	0	71 1A 00 00	7.625711e+29	0	00 00 1A 71	9.485389e-42

UINT32 - Big Endian (ABCD)			UINT32 - Little Endian (DCBA)			UINT32 - Mid-Big Endian (BADC)			UINT32 - Mid-Little Endian (CDAB)		
#	Raw	UINT32	#	Raw	UINT32	#	Raw	UINT32	#	Raw	UINT32
0	1A 71 00 00	443613184	0	00 00 71 1A	28954	0	71 1A 00 00	1897529344	0	00 00 1A 71	6769

דוגמה להמרת ה **DID** ל HEX:

Facebook Google+ Twitter

Decimal Value (max: 9223372036854775807)

2014276

Convert

Hexadecimal Value

1EBC44

swap conversion: Hex to Decimal

המרת ערך ה hex של **did** ל Little Endian יש להעתיק את התוצאה ללא האפסים שהתווספו אליה:

HexString Input

1EBC44

AnalyzeData

ASCII

¼D

Binary

#	Raw	Binary
0	1E BC	0001111010111100
2	44 00	0100010000000000

Float - Big Endian (ABCD)

#	Raw	Float
0	1E BC 44 00	1.99333984e-20

Float - Little Endian (DCBA)

#	Raw	Float
0	00 44 BC 1E	6.312297e-39

Float - Mid-Big Endian (BADC)

#	Raw	Float
0	BC 1E 00 44	-0.009643618

Float - Mid-Little Endian (CDAB)

#	Raw	Float
0	44 00 1E BC	512.4802

UINT32 - Big Endian (ABCD)

#	Raw	UINT32
0	1E BC 44 00	515654656

UINT32 - Little Endian (DCBA)

#	Raw	UINT32
0	00 44 BC 1E	4504606

UINT32 - Mid-Big Endian (BADC)

#	Raw	UINT32
0	BC 1E 00 44	3156082756

UINT32 - Mid-Little Endian (CDAB)

#	Raw	UINT32
0	44 00 1E BC	1140858556

זהו, יש לנו את כל הנתונים הדרושים עבור הסקריפט:

```
# Reverse Engineering and coding Aviad Golan @AviadGolan and Shai Rod @NightRang3r

#!/usr/bin/env python

import binascii as ba
import time
import struct
import socket
import sys

##### CHANGE TO YOUR PARAMS #########
switcherIP = "10.0.0.11" # Change IP Address to your switcher IP
phone_id = "711a"  # Can be found in the sqlite db on a rooted android device (/data/data/com.ogemary.smarthome/databases/myDB) in "phone" table "uid"
# or from packet capture of an "on/off" command (93 bytes data length frame or 147 bytes packet length in wireshark) copy  4 chars value from 89-93
device_id = "44bc1e" # Can be found in the sqlite db on a rooted android device  (/data/data/com.ogemary.smarthome/databases/myDB) in "device" table "d
# or from packet capture of an "on/off" command (93 bytes data length frame or 147 bytes packet length in wireshark) copy 6 chars value from 81-87
device_pass = "36373731" # Can be found in the sqlite db on a rooted android device  (/data/data/com.ogemary.smarthome/databases/myDB) in "device" tabl

# or from packet capture of an "on/off" command (93 bytes data length frame or 147 bytes packet length in wireshark) copy 8 chars value from 97-105

##### DO NOT CHANGE BYOND THIS LINE  #########
```