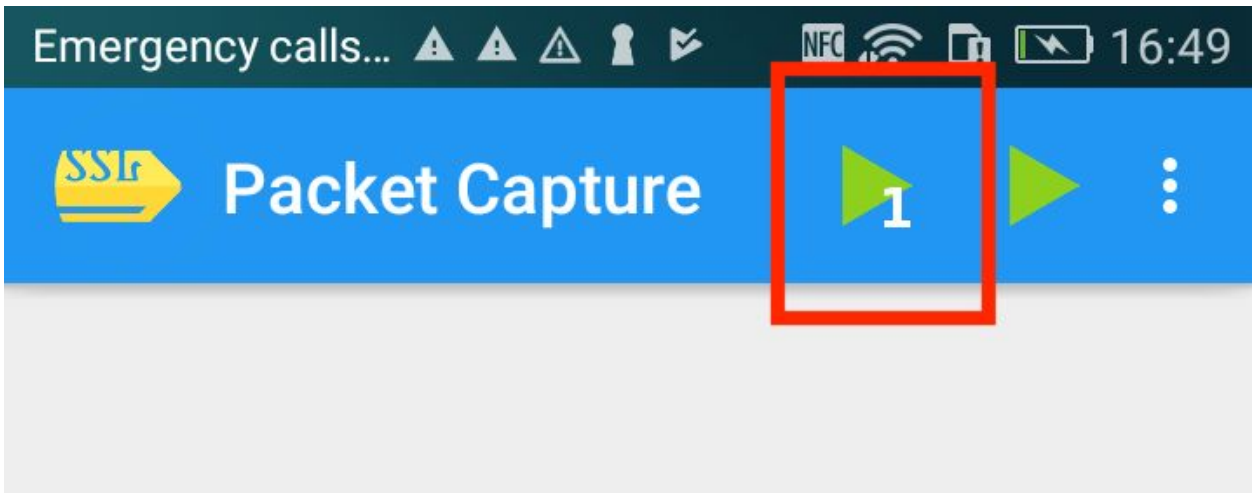
חילוץ הנתונים ממכשיר אנדרואיד **שאינו פרוץ (not rooted)**

יש לוודא שהאפליקציה Switcher V2 מותקנת על מכשיר האנדרואיד שלכם
כנסו לחנות האפליקציות של גוגל הורידו והתקינו את האפליקציה: Packet Capture

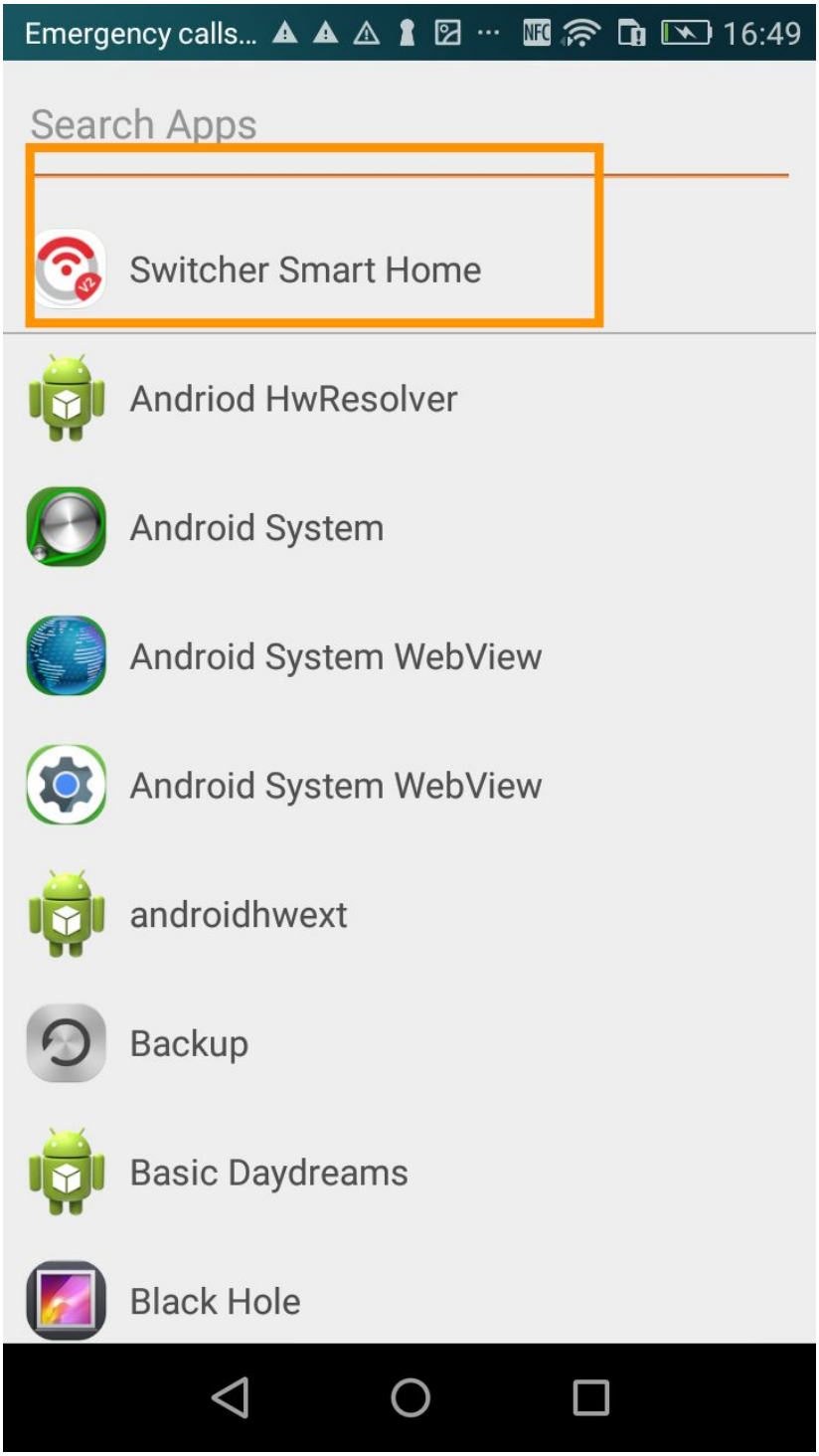
https://play.google.com/store/apps/details?id=app.greyshirts.sslcapture&hl=en

יש להתקין ולהפעיל את האפליקציה packet capture

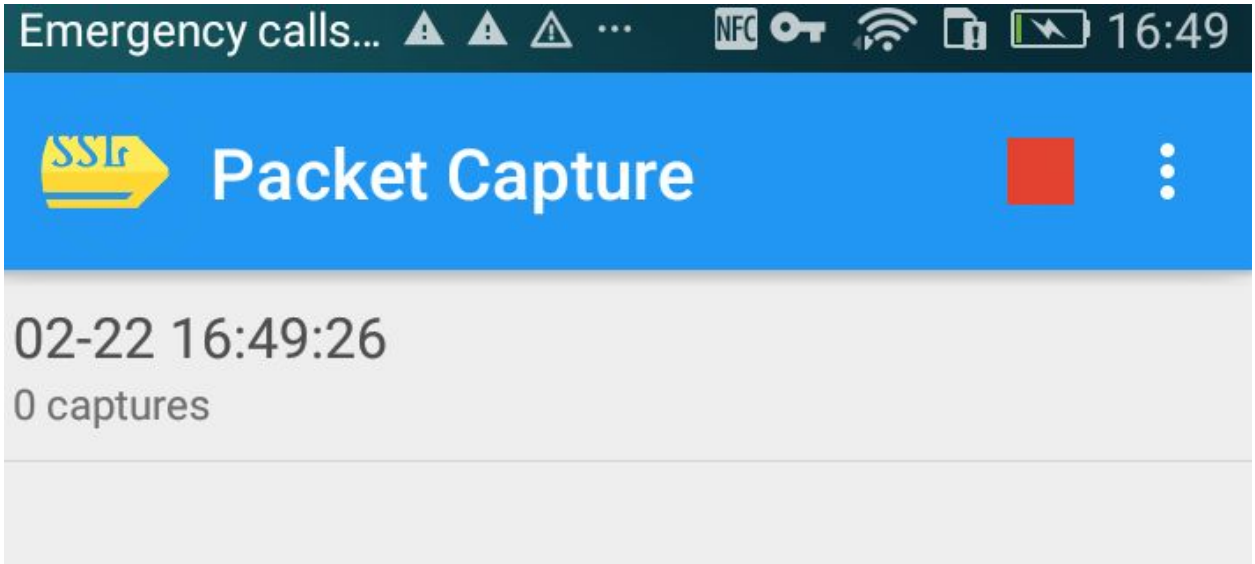
ללחוץ על הכפתור כפי שמסומן בצילום המסך:



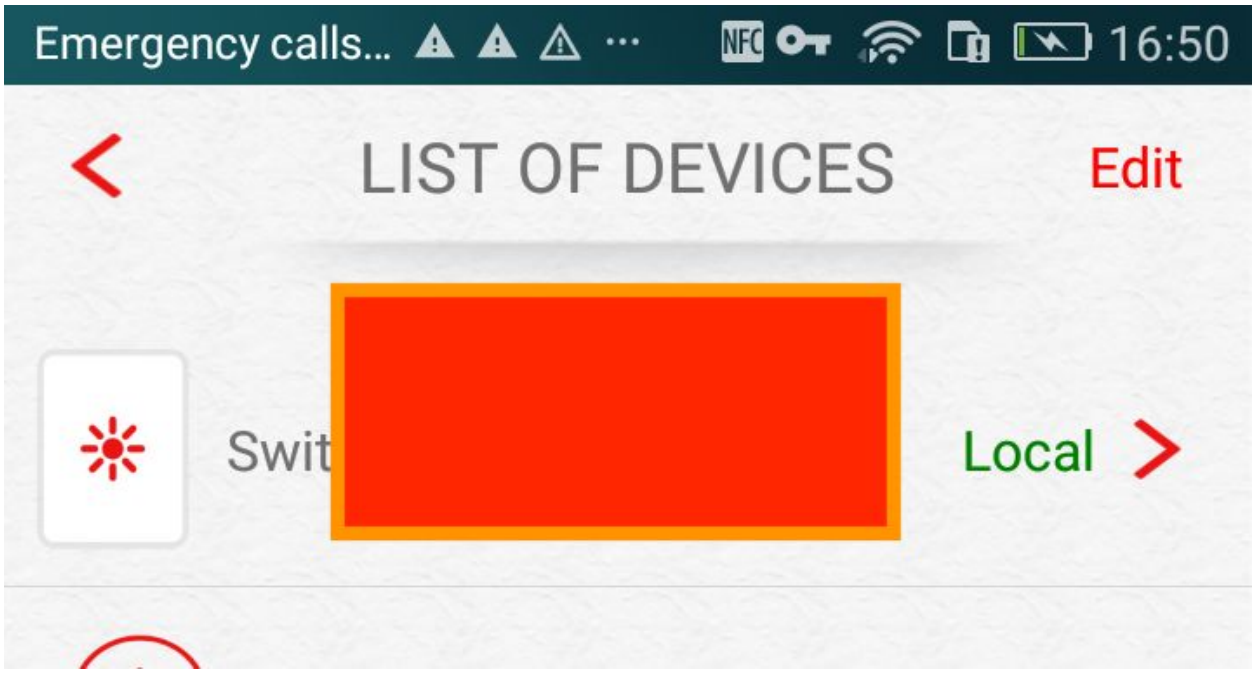
מתוך רשימת האפליקציות יש לבחור ב Switcher Smart Home



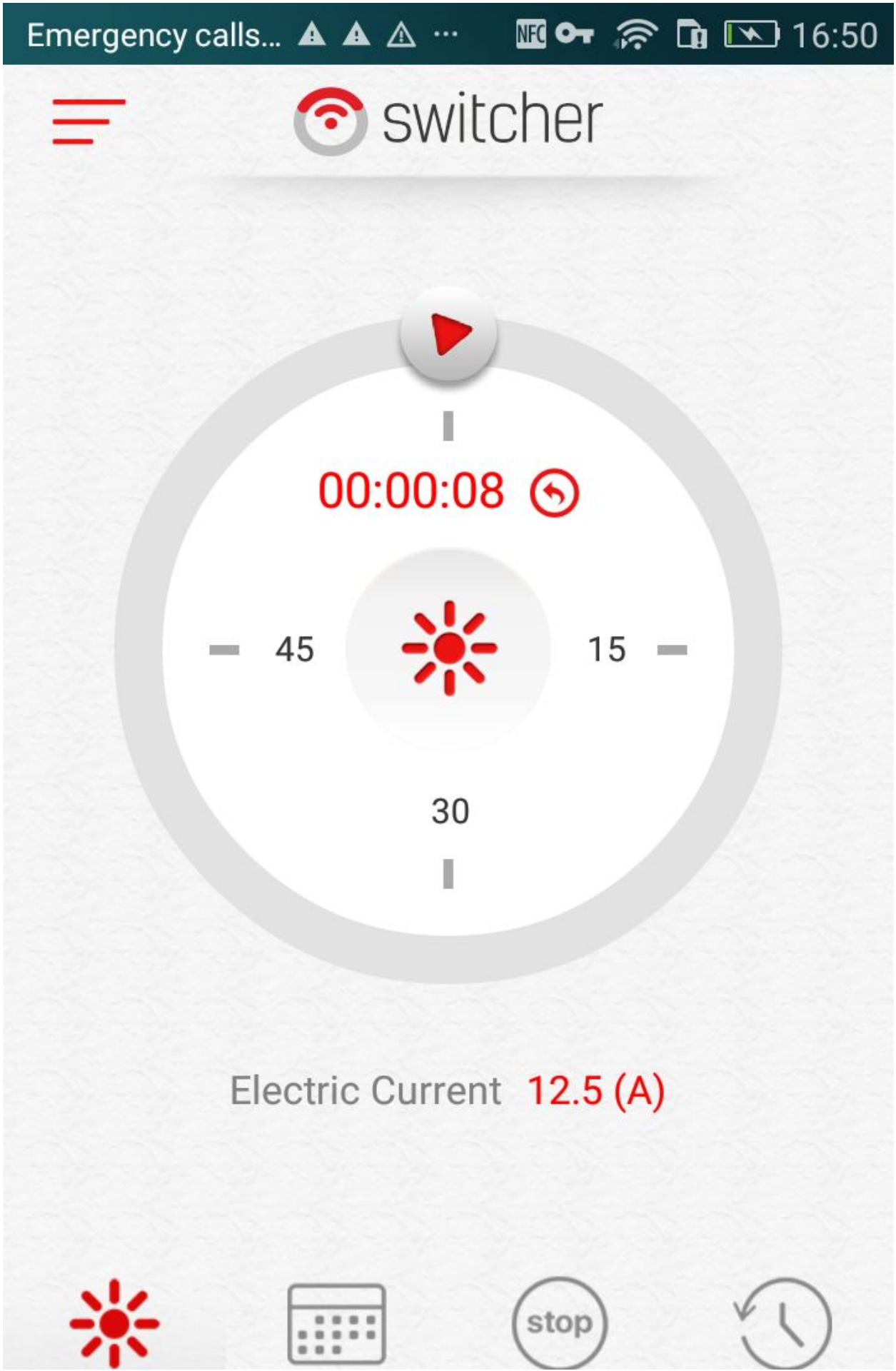
תהליך לכידת התקשורת החל כעת יש לפתוח במקביל (מבלי לסגור את אפליקציית ה packet capture) את אפליקציית Switcher V2



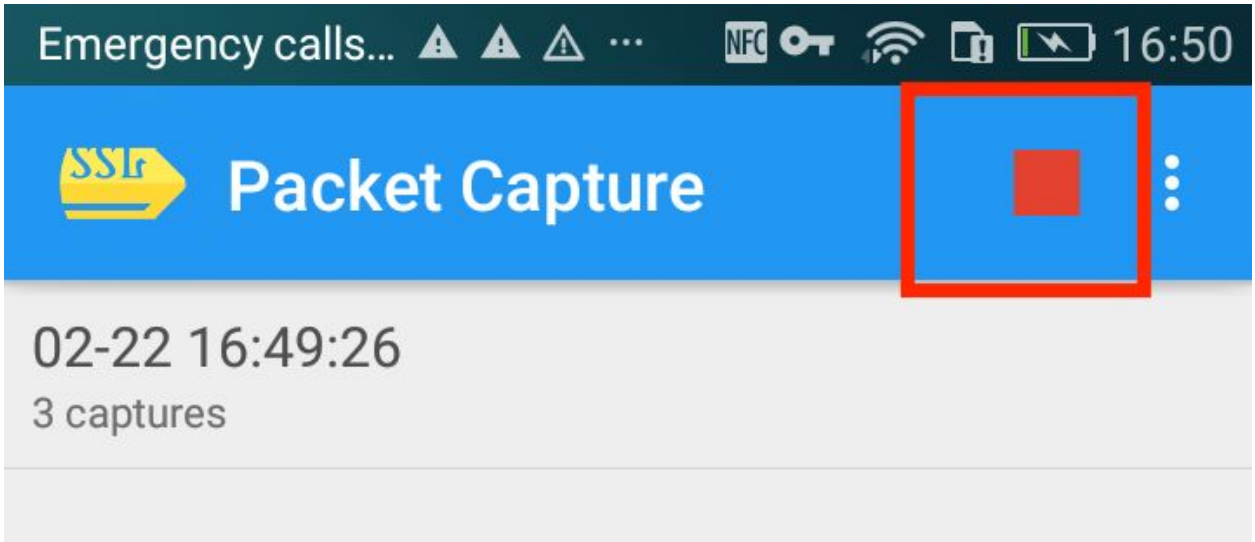
יש לוודא שאתם מחוברים לרשת האלחוטית שאליה מחובר גם ה Switcher ושהאפליקציה מציגה אותו במצב Local



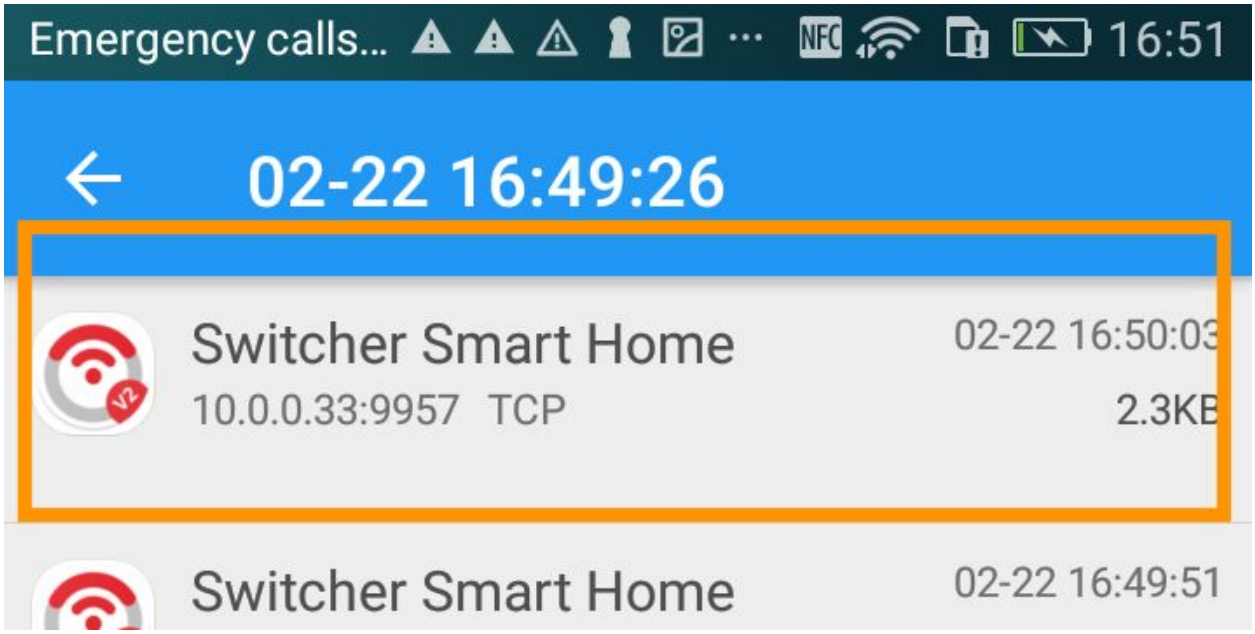
כעת יש לבצע פעולת הדלקה וכיבוי ולאחר מכן יש לחזור אל מסך אפליקציית ה Packet Capture


Emergency calls...
16:50
switcher
00:00:08
45
15
30
Electric Current 12.5 (A)
stop

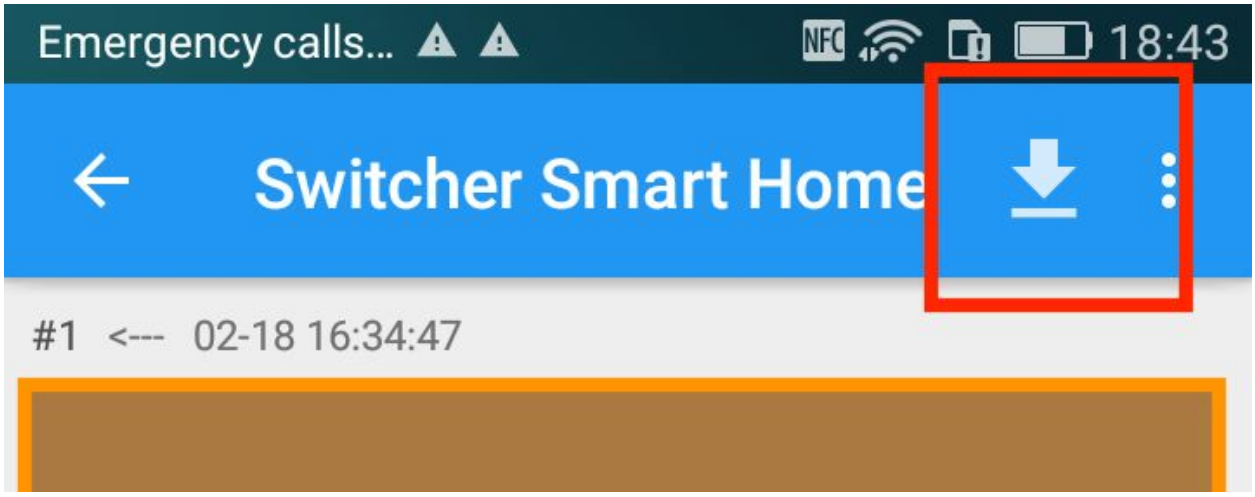
לחצו על כפתור ה stop כדי לעצור את תהליך לכידת התקשורת

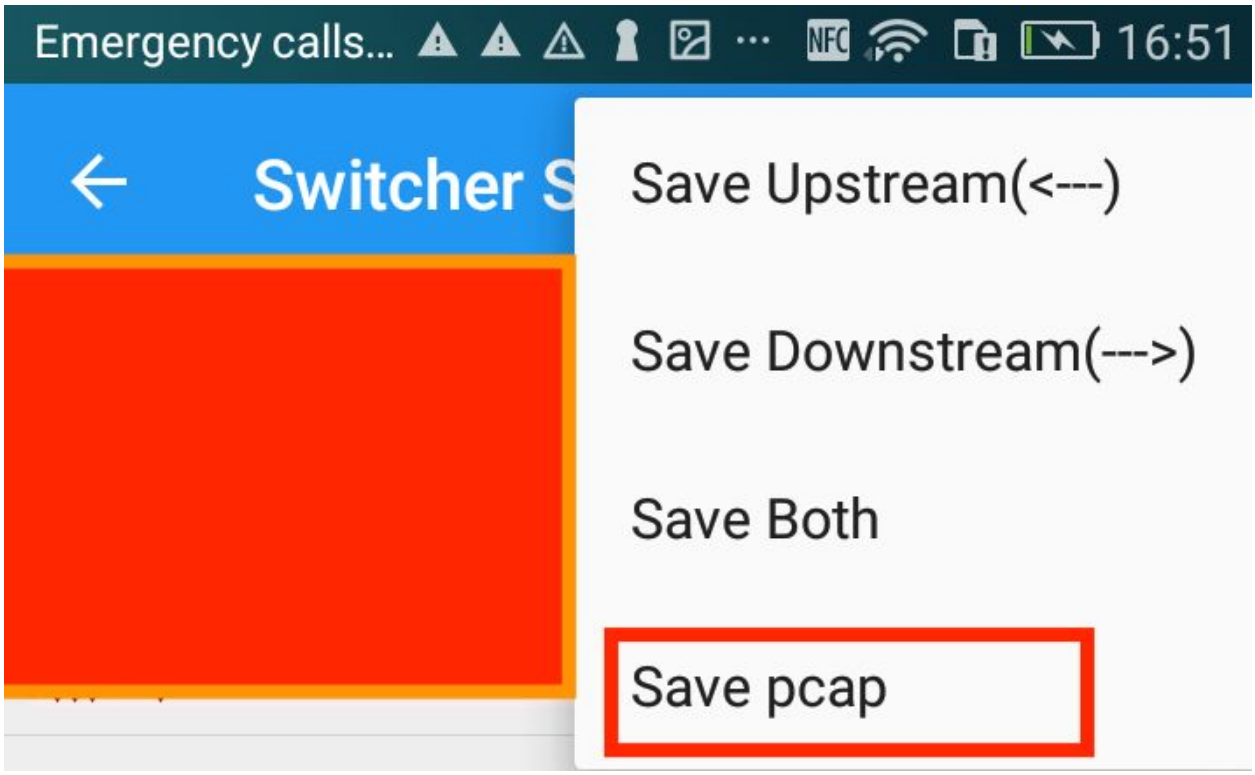


יש ללחוץ על התאריך שבו בוצעה לכידת התקשורת ומתוך הרשימה שמוצגת יש לבחור בתקשורת שהתבצעה אל מול כתובת האיי.פי הפנימית שלכם בפורט 9957



עכשיו יש לייצא את הקובץ ע״י לחיצה על הכפתור של ההורדה ולבחור באפשרות "Save pcap"



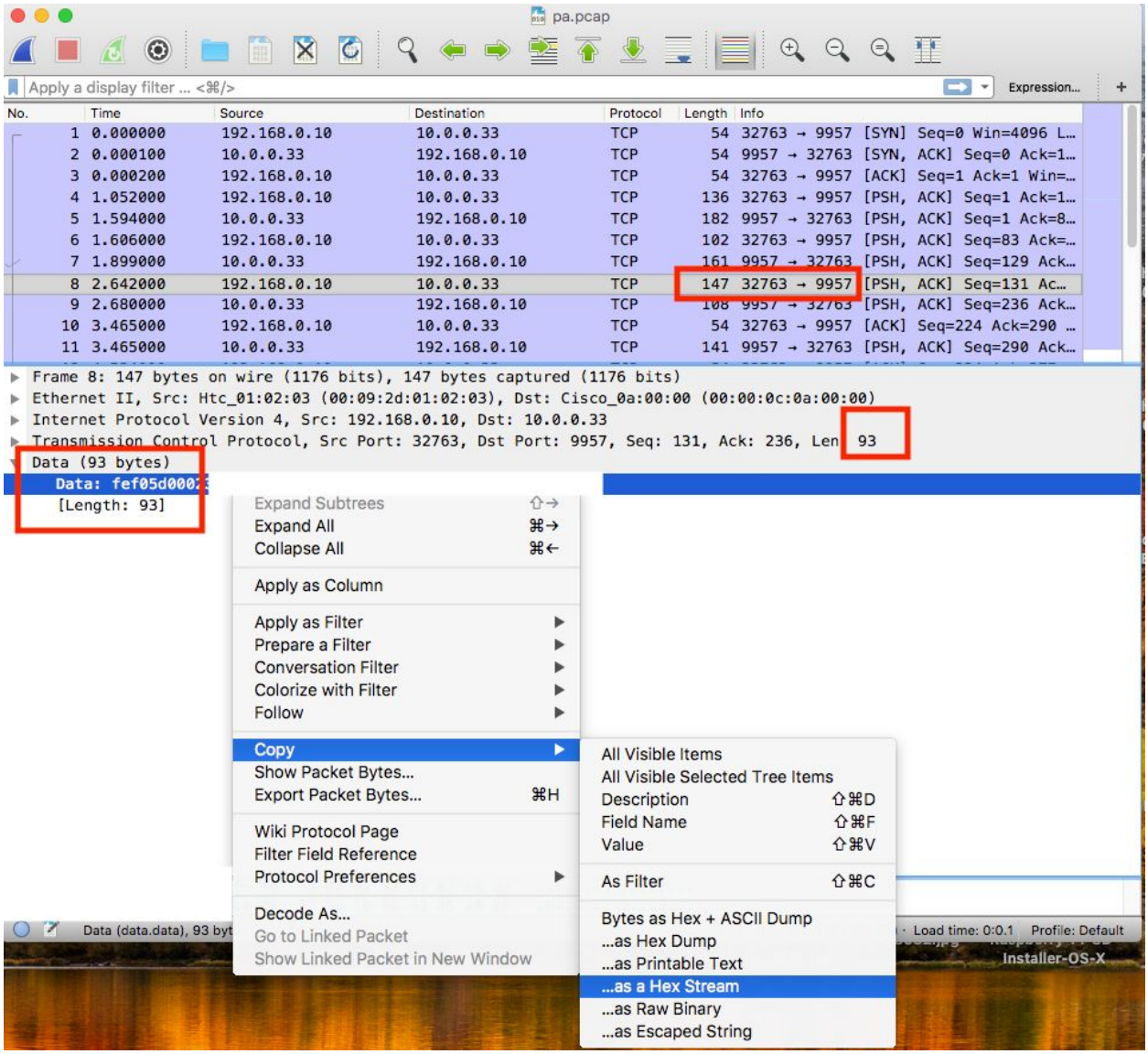


כעת יש להעביר את קובץ ה pcap ששמרתם למכשיר אל המחשב שלכם

ניתן להוציא את הנתונים בצורה ידנית באמצעות Wireshark:

לשם כך יש לפתוח את קובץ ה pacp באמצעות wireshark לאתר רשומה באורך 147 וגודל ה data הוא 93 בתים (186 תווים) לפורט 9957

יש לבחור בפקטה זו להעתיק את הערך שלה data כ hex stream כפי שמופיע בצילום המסך הבא:



מיקום הערכים בתוכן ה data הוא כך:

phone_id

4 תווים במיקום 89-93 או 2 בתים 44-46

device_id

6 תווים במיקום 81-87 או 3 בתים 40-43

device_pass

8 תווים במיקום 97-105 או 4 בתים 48-52

<u>להלן דוגמה לפקטה שנלכדה על גבי חיבור לסוויצ'ר ברשת הלוקאלית (הנתונים הנדרשים מודגשים):</u>

fef05d0002320102c49d8448340001000000000000000000bccbb05a00000000000000000000f0
fe**44bc1e**00**711a**0000**36373731**0000000000000000000000000000000000000000000000000000
00000001060001000000000073290d1d

כעת נשאר לנו רק לעדכן את הסקריפט switcher.py עם הערכים שהוצאנו

```
# 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  #########
```