הקלטה באמצעות adb של אנדרואיד .

1. צריך לחבר בכבל למחשב מכשיר פלאפון עם הרשאות root.
2. בשביל להפעיל מצב מפתח צריך ללחוץ 7-8 פעמים על build "בלה בלה" שנמצא בפרטי המכשיר בהגדרות
3. בשביל לפעיל debugging mode אתה צריך להפעיל מצב מפתח
4. בשביל שתוכל לעבוד עם adb צריך להפעיל debugging mode
5. נכנסים לתיקיה הנמצאת במסלול הבא :

C:\Users\**userName**\AppData\Local\Android\sdk\platform-tools

כאשר ה**"userName"**\ זה השם של המחשב עליו עובדים.

1. כדי לפתוח את הטרמינל נלחץ על shift, כפתור ימני של העכבר, נבחר את "פתח חלון פקודה כאן" . ויפתח לנו הטרמינל.
2. בשביל לבדוק שהמכשיר מחובר למחשב כמו שצריך, צריך לכתוב בטרמינל adb devices ולראות שבפלט יש שם של מכשיר (בדרך כלל רצף של תווים לא קשורים) והמילה device .
3. א. בשביל להריץ פקודה צריך להשתמש adb shell command ושם הפקודה

ב. או שאפשר פשוט לכתוב adb shell ואז תקבל טרמינל מדומה לתוך המכשיר.(נעדיף אופציה זו).

9. נעבור למצב su (פשוט כותבים su)

10. א. כדי להתחיל הקלטה נכתוב :

Tcpdump –I **interfaceName**

\*כאשר במקום ה- **interfaceName** נכתוב אם שם ה- interface בו אנו נמצאים.

ב. אם נרצה להתחיל הקלטה וגם לשמור אותה במכשיר :

ננווט לתיקיית אחסון בה נרצה שהקובץ ישמר (ע"י הפקודה cd **folderName** ) ונכתוב:

Tcpdump –i  **interfaceName**  –w **filename**.pcap

(לדוגמא אם אנחנו על וויפי בשם wlan0 נריץ פשוט :

Tcpdump -I wlan0 –w **filename**.pcap )

\*כאשר במקום ה- **folderName**  נרשום את שם התיקייה אליה נרצה להיכנס למכשיר

\*\*ובמקום ה **filename** נרשום את שם הקובץ שנבחר להקלטה הנוכחית

12. כדי לדעת מה ה-interface:

נריץ ifconfig ונחפש משהו בסגנון:

אם זה סלולר: rmnet0

אם זה וויפי: wlan0

13. בשביל לסיים הרצה פשוט לוחצים cntl+c כרגיל

14. כדי להעתיק למחשב מריצים בטרמינל של המחשב adb pull source\_path dest\_path

15. כדי להעתיק תקיה שלימה פשוט כותבים במקור את הנתיב עד התקיה.