

GSM SMS SNIFFING

אביב דנינו – 209237544 רעות חדד – 305170219 ויקטור קושניר- 208629477

צוות מס' 18

תוכן עניינים

| | |
|------------|--------------------------------------|
| 2..... | פתיח |
| 2..... | סדר פעולות קצר |
| 2..... | הכלים שלנו |
| 3..... | טכנולוגיית ה GSM |
| 4..... | חולשות |
| 5..... | תהליך העבודה |
| 6..... | העברת הסלולרי ל GSM ומציאת ערוץ |
| 7-8..... | אימות הערוץ |
| 9..... | הסנפת התעבורה |
| 10-11..... | הוצאת מפתח הצפנה ומזהה זמני של ה SIM |
| 12..... | מציאת ה TIMESLOT של ה SIM |
| 13..... | מציאת אלגוריתם ההצפנה |
| 14..... | פענוח הודעת ה SMS |
| 15-16..... | קשיים |
| 17..... | מקורות |

פתיח:

בעבר דור השידור העיקרי היה GSM ששימש להעברת הודעות SMS וביצוע שיחות. טכנולוגיית השידור נעשית בגלי רדיו בין האנטנה לטלפון שלנו (וההפך) עד היום. בעזרת כלי ה-hackrf ניתן לפענח את גלי הרדיו למידע שניתן לקרוא במחשב. הקריאה זהה למידע שאנו קולטים ב-WIFI, עם זאת חשוב לציין כי גם WIFI הוא תוצר של גלי רדיו. במטלה זו אנו נתמקד ברעיון תפיסת הודעת SMS פשוטה תוך ניצול החולשות בטכנולוגיית GSM. נשתמש באמצעים פשוטים כדי לזהות את גלי הרדיו סביבנו, תפיסת התקשורת בין האנטנה לבין המכשיר ופיענוח של ההודעה עצמה.

סדר פעולות קצר

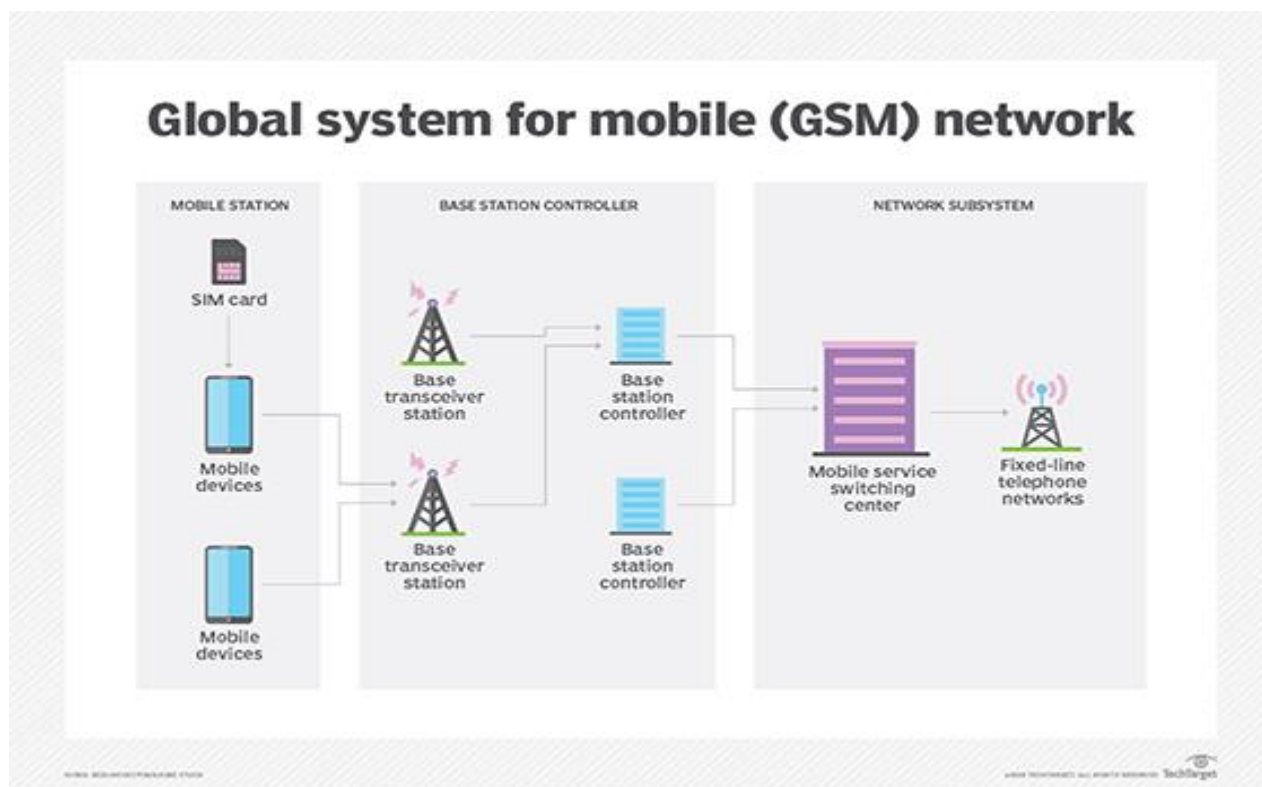
1. פלאפון הנתקף מחובר לרשת GSM (בדור 2).
2. התוקף מאזין לאנטנה.
3. הקורבן מקבל הודעת SMS.
4. התוקף מאזין להודעה ומפענח אותה.

הכלים שלנו:

- Hackrf one.
- Dragon-OS: מערכת הפעלה על בסיס DEBIAN עם כלים מובנים לעבודה עם SDR.
- תוכנת WIRESHARK.
- פלאפון galaxy A5[6] שנת 2016.

טכנולוגיית ה-GSM

טכנולוגיית GSM מתבססת על מספר אלמנטים וביניהם קיימת אינטראקציה:



המבנה מחולק בתמונה לארבעה חלקים:

1. סלולרי – בכל מכשיר סלולרי קיים מספר זיהוי הנקרא IMEI.
לכל כרטיס SIM יש מזהה מול הרשת הנקרא IMSI.
ברגע שמכשיר מתחבר לרשת סלולרית בפעם הראשונה (עבור ביצוע הזדהות) הוא שולח את המזהה IMSI ומקבל חזרה מזהה זמני TMSI. מכאן והלאה המנוי מזדהה ב TMSI. הרשת מחליפה את ה-TMSI בכדי למנוע מעקב אחרי מנויים, בד"כ לאחר שיחת טלפון או מעבר בין אנטנות (קישור מחדש).
2. Base Transceiver Station – BTS, אנטנה המספקת שירותי תקשורת באמצעות גלי רדיו למנויים סביבה. מורכב מ-3 אנטנות המכסות ביחד סביבה של 360° כך שכל אנטנה מכסה סביבה של 120° . לכל אנטנה יש מספר מזהה Cell ID. תחנת הבסיס נקראת גם BTS.
3. Base Station Controller – BSC: תפקידו לנהל את ערוצי הרדיו של מספר אנטנות שונות. ברשת מסוימת יתכנו מספר BSC שינהלו קבוצות שונות של אנטנות.
4. Mobile service Switching Center – MSC. תפקידו לנהל את התקשורת בין המנויים, לתת הרשאות ולתקשר מול הרשתות מחוץ לרשת הסלולרית. האימות של המנוי מתבצע מול ה-MSC.

חולשות

אלגוריתם A5/1 הוא אלגוריתם שמשמש להצפנה של מידע המועבר בהודעות טקסט ושיחות קוליות, עם הזמן התגלו באלגוריתם זה חולשות וזו הפרצה שאנו מנצלים בתקיפה שלנו. בשביל לפרוץ את האלגוריתם השתמשו במבנה נתונים בשם Rainbow tables, שבד"כ משמש למציאת פרצות שבאלה.

מאחר ותוך כדי ההאזנה ל SIM ניתן למצא את ה TIMESLOT ואת אלגוריתם ההצפנה, נוכל להוסיף את ה KC בשביל להשלים את פענוח ההודעות.

בנוסף, ב-3G אחת מסוגי ההתקפות שנתקלנו בה היא DOWNGRADE אשר גורמת לפלאפון לבצע הנמכה מדור 3 לדור 2 וכך בעצם ניתן להשתמש בפרצה זו גם עבור מכשירי 3G.

תהליך העבודה

- העברת המכשיר הסלולרי לתקשורת GSM ובדיקת ערוץ התקשורת שלו.
- חיבור ה `hackrf` ואימות של ערוץ התקשורת באזור שלנו באמצעות תוכנת `kalibrate`.
- מסניפים את תעבורת הערוץ ותוך כדי שולחים הודעת SMS בזמן ההסנפה ושומרים בקובץ.
- מחברים את הפלאפון למחשב ומוציאים את מפתח ההצפנה ואת המזהה הזמני מול האנטנה באמצעות פקודות AT (ניתן להשתמש בפקודות APDU במקרה שיש קורא כרטיסים).
- נמצא את המרווח זמן שניתן לפלאפון שלנו מול האנטנה באמצעות `grgsm_decode` ונפלטר באמצעות המזהה הזמני שלנו.
- נשתמש במרווח זמן שמצאנו ונמצא את אלגוריתם ההצפנה המצפין את תעבורת המידע של הנתקף גם באמצעות `grgsm_decode`.
- נשתמש במרווח זמן, אלגוריתם ההצפנה ומפתח ההצפנה על מנת לפענח את הודעת ה SMS שנשלחה באמצעות `grgsm_decode`.

1. העברת הסלולרי ל-GSM ומציאת ערוץ

מאחר והיום רשתות התקשורת מגיעות לתקשורת 5G, אנו נעביר את תעבורת המכשיר שלנו ל-GSM.

בשביל למצוא את הערוץ של הפלאפון שלנו נכניס את הקוד *#0011#

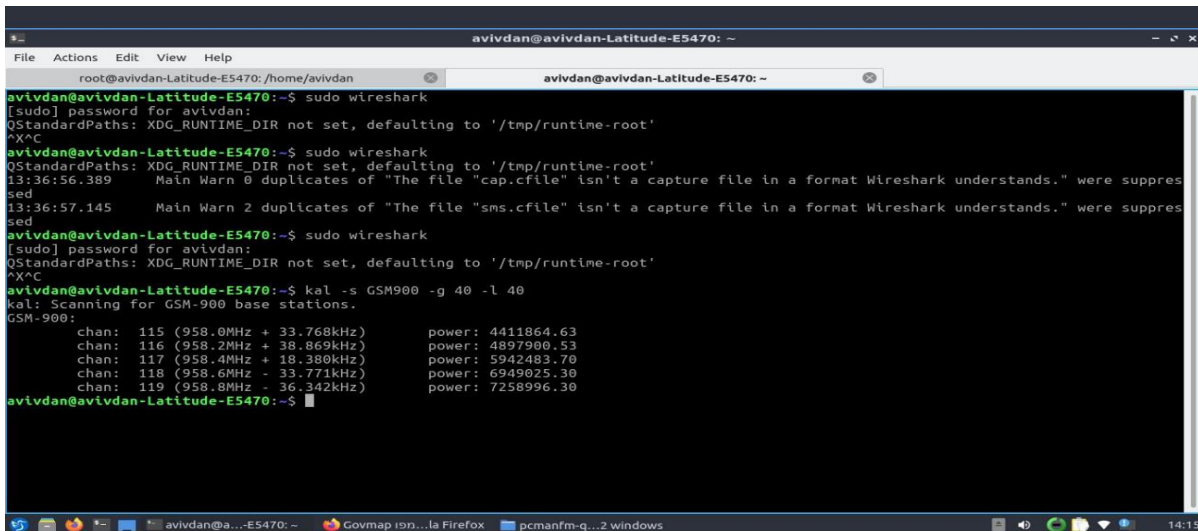
לאחר מכן יפתח לנו מסך עם מידע על הסים והוא כולל את arfcn - ערוץ התקשורת שלנו.

במקרה שלנו הוא 119.



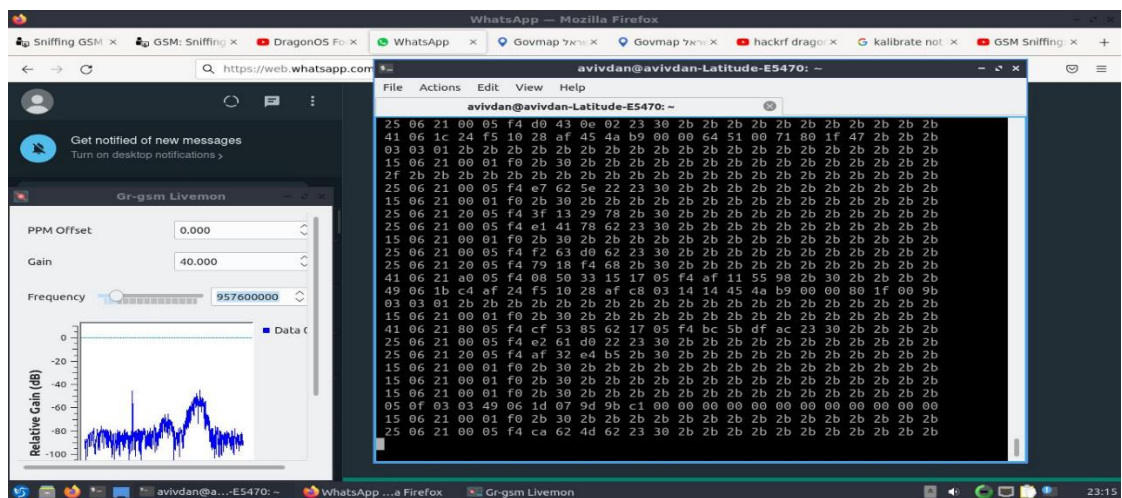
2. אימות הערוץ

בשלב זה אנו רוצים לאמת שהערוץ אכן נמצא באזורנו. לשם כך נפעיל את תוכנת kalibrate, נחבר את מכשיר ה-hackrf ונאמת את האנטנות באזורנו. נוכל לראות בתמונה שאנו קולטים את ערוץ 119.



```
avivdan@avivdan-Latitude-E5470: ~  
File Actions Edit View Help  
root@avivdan-Latitude-E5470: /home/avivdan  
avivdan@avivdan-Latitude-E5470:~$ sudo wireshark  
[sudo] password for avivdan:  
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'  
^X^C  
avivdan@avivdan-Latitude-E5470:~$ sudo wireshark  
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'  
13:36:56.389 Main Warn 0 duplicates of "The file "cap.cfile" isn't a capture file in a format Wireshark understands." were suppressed  
13:36:57.145 Main Warn 2 duplicates of "The file "sms.cfile" isn't a capture file in a format Wireshark understands." were suppressed  
avivdan@avivdan-Latitude-E5470:~$ sudo wireshark  
[sudo] password for avivdan:  
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'  
^X^C  
avivdan@avivdan-Latitude-E5470:~$ kal -s GSM900 -g 40 -l 40  
kal: Scanning For GSM-900 base stations.  
GSM-900:  
chan: 115 (958.0MHz + 33.768kHz) power: 4411864.63  
chan: 116 (958.2MHz + 38.869kHz) power: 4897980.53  
chan: 117 (958.4MHz + 18.380kHz) power: 5942483.70  
chan: 118 (958.6MHz - 33.771kHz) power: 6949025.30  
chan: 119 (958.8MHz - 36.342kHz) power: 7258996.30  
avivdan@avivdan-Latitude-E5470:~$
```

אם נרצה לראות גם את התעבורה נשתמש בgsm_livemon



בשלב זה נתקלנו בבעיות שונות והן:

- אי מציאת אנטנה - לכן נסענו לאזור של האנטנה להתגבר על בעיות קליטה.
- חוסר הפקת תעבורה למרות שראינו כי הערוץ קיים – יש ערוצים שככל הנראה אין בהם תעבורה ולכן צריך למצוא את הערוץ המתאים ולפי מה שראינו זה הערוץ שאנו נמצאים עליו.
- לא קיבלנו מספרים כמו בתמונה השנייה המסמלים את הנראות של התעבורה – לכן בדקנו את הgain והצבנו בו מספר 40 וכתוצאה קיבלנו את התעבורה.
- לא מוצאים את הספרייה `airprobe_rtlsdr.grc` – הספרייה התקדמה לעומת המדריכים, כיום ניתן למצוא בשם `grgsm_livemon`.

3. הסנפת התעבורה

בשלב זה אנו מאזינים לפרק זמן מתעבורת הערוץ, פרק זמן זה צריך לכלול שליחת SMS של המכשיר המותקף וקבלתו במכשיר אחר.

נשתמש בספריית grgsm המובנית בdragon-OS בעזרת הפקודה:

```
grgsm_capture -f 958800000 -g 40 -c aviv.cfile -T 30
```

ניתן גם להשתמש בפקודה

```
grgsm_capture -a 119 -g 40 -c aviv.cfile -T 30
```

אשר משתמשת בערוץ ולא בתדירות

דגל c- שם הקובץ, T- זמן ההאזנה, a,f- תדר/ערוץ (בהתאמה).

לאחר ההסנפה נקבל קובץ בשם שכתבנו (aviv.cfile)

לאחר שיש לנו את הקובץ נוציא את הhackrf מהמחשב ולעשות את שלבי הפענוח.

לאחר שלב זה ניתן לנתק את האנטנה.

בעיות שקרו לנו בשלב זה:

- לא קיבלנו מידע – ככל הנראה לא היינו על 2G או על הערוץ הנכון.
- התכנית לא עוצרת – הוספת דגל T-.
- לא מוצאים את הספרייה airprobe_rtlsdr_capture.py – הספרייה התקדמה לעומת המדריכים, כיום ניתן למצוא בשם grgsm_capture.

4. הוצאת מפתח הצפנה ומזהה זמני של ה-SIM

השתמשנו בפקודות AT ולא בפקודות APDU כמו שהוצע לנו בגלל קוצר זמן. הפקודות מאפשרות לנו לחבר את הפלאפון למחשב ולהוציא את המידע שאנו צריכים מהסים בלי להשתמש בקורא כרטיסים, אבל הפלאפון שעבד עם התוכנה הוא פלאפון דיי ישן (2016) בשונה משאר הפלאפונים העדכניים שקיימים לכולם היום. לכן היינו צריכים למצוא פלאפון מתאים וסים מתאים שמוכן להתנדב עבור התהליך.

התקנו ספריה בשם libusb שחיונית לשימוש בפקודות AT דרך המחשב.

השתמשנו בתוכנת busybox ככלי לתקשר עם הסים. ייעוד התוכנה הוא לאפשר ממשק עם הסים ולשלוח אליו פקודות:

```
busybox minicom /dev/ttyACM0
```

הפקודה מאפשרת לנו לקבל את ה-TMSI (מזהה זמני מול האנטנה)

```
AT+CRSM=176,28448,0,0,9
```

הפקודה מאפשרת לנו לקבל את ה-kc של הסים (מפתח ההצפנה)

```
AT+CRSM=176,28542,0,0,11
```

הפקודות של AT הם פקודות שלרוב לא עובדות לעומת זאת פקודות APDU יהיו יותר פשוטות לשימוש רחב, אך שימוש בפקודות אלה צורך קורא כרטיסים (כמו של הרב קו).

5. מציאת ה- TIMESLOT של ה- SIM

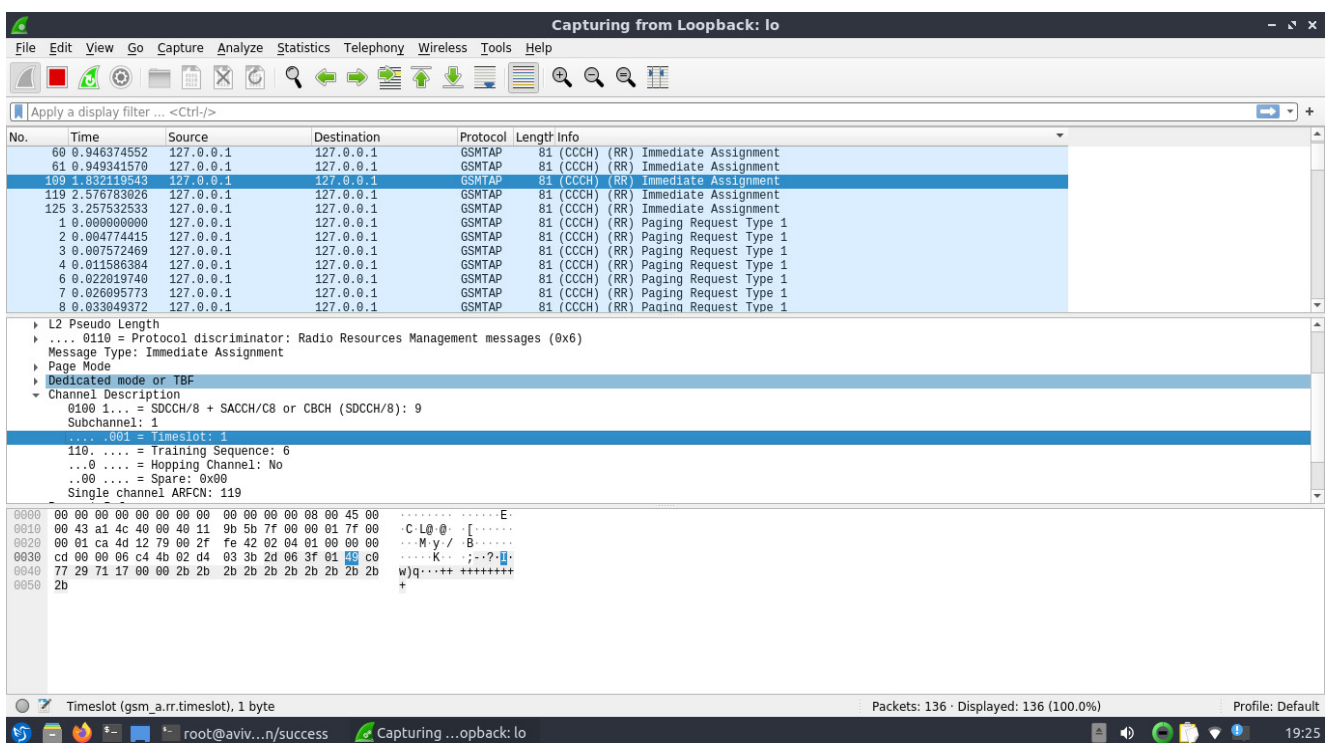
לאחר שיש לנו את ה TMSI ואת קובץ ההאזנה "aviv.cfile" נפעיל את WIRESHARK ונאזין דרך LOOPBACK, לאחר מכן נפעיל את הפקודה הבאה:

```
grgsm_decode -c aviv.cfile -a 119 -m BCCH
```

הדגל -m מסמן את אופי הערוץ.

ניתן לפלטר את הפאקטות בעזרת 8 האותיות הראשונות ב TMSI אך במקרה שלנו לא הייתה תעבורה של GSM אחרת חוץ מאיתנו.

לאחר מכן ננסה למצוא פאקטת gsm_tap עם תיאור של immediate assignment, ונמצא שם פרק בשם channel description, נצפה לקחת משם את ה TIMESLOT. נוכל גם לראות כי ה mode channel הוא SDCCH8.



בעיות שנתקלנו בהן:

- Packet channel description – לא מה שאנו מחפשים אבל אותו תיאור פאקטה.
- Hopping channel – הלכנו קרוב לאנטנה וראינו מתי אנו לא משתמשים בכזה.
- מרווחי זמן שונים – TMSI שונה יכול להיות ואז ניתן לפלטר על פי ה TMSI הרצוי בשורת חיפוש.

6. מציאת אלגוריתם ההצפנה

לאחר שמצאנו את המרווח זמן של הסיים אנו יכולים למצוא את האלגוריתם הצפנה בעזרת הפקודה הבאה :

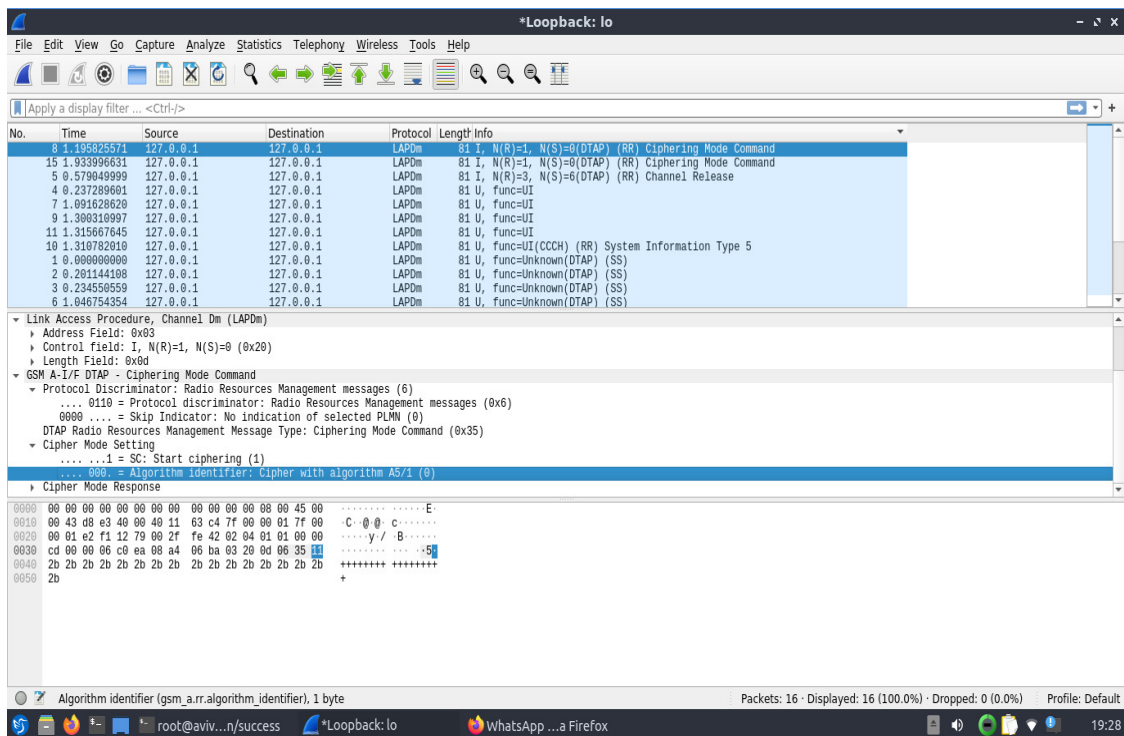
```
grgsm_decode -c aviv.cfile -a 119 -m SDCCH8 -t 1
```

כאשר -t הוא דגל של timeslot.

שינינו גם את שיטת השידור בהתאמה לכתוב בפאקטה

אנחנו נחפש פאקטה מפרוטוקול LAPDm אשר בתיאור תראה לנו כי יש מידע על ההצפנה.

נוכל לקבל משם את אלגוריתם ההצפנה כפי שנראה בתמונה:



בעיות שנתקלנו בהן:

- לא מצאנו פאקטה שכזו – או שהמרווח זמן שהכנסנו לא תואם או שלא הספקנו לכלול SMS בזמן ההאזנה.
- יש מדריכים שכתוב בהם בצורה שונה - ניתן לכתוב גם את התדירות במקום הערוץ.

7. פענוח הודעת ה SMS

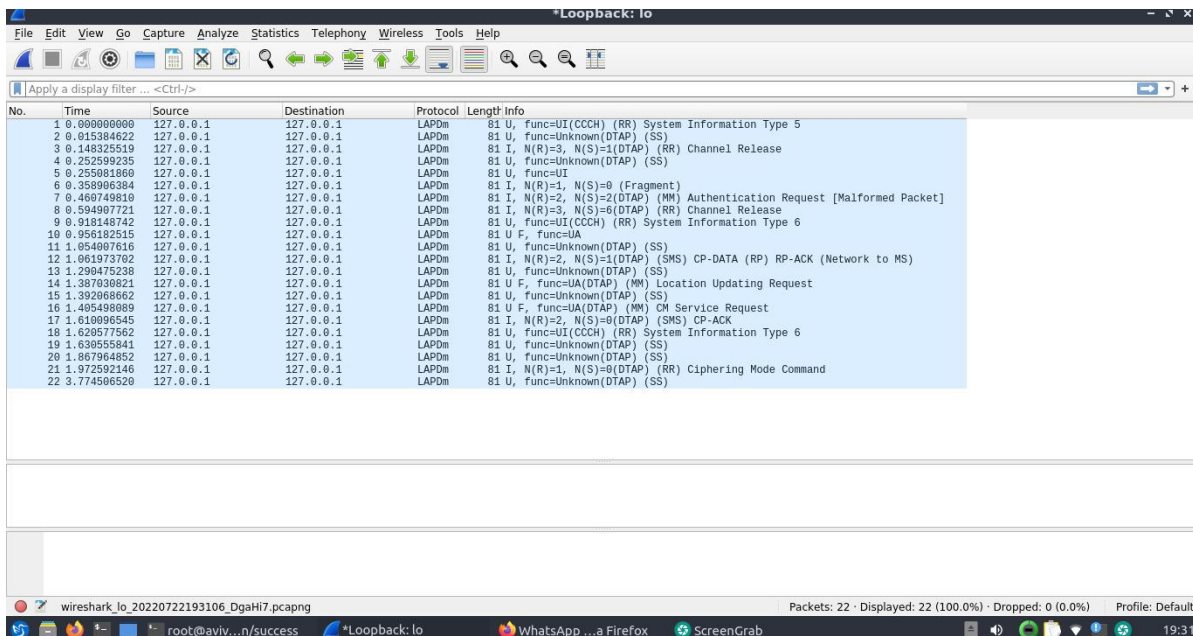
הגענו לשלב הסופי בו יש לנו:

- Timeslot
- Key cypher
- Algorithm

נשתמש בכל אלה על מנת לחלץ את הודעת ה SMS בעזרת הפקודה הבאה:

```
grgsm_decode -c aviv.cfile -a 119 -m SDCCH8 -t 1 -e 1 -kc 0123456789abcdef
```

כאשר ה KC שלנו הוא זה שקיבלנו בשלב 4 ו e- הוא דגל בשביל סוג האלגוריתם ההצפנה שמצאנו קודם לכן היינו צריכים לקבל פאקטה בפרוטוקול GSM SMS.



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-----------|-------------|----------|--------|---|
| 1 | 0.000000000 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=UI(CCH) (RR) System Information Type 5 |
| 2 | 0.015384622 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=Unknown(DTAP) (SS) |
| 3 | 0.148325519 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 I | N(R)=3, N(S)=1(DTAP) (RR) Channel Release |
| 4 | 0.252599235 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=Unknown(DTAP) (SS) |
| 5 | 0.255081860 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=UI |
| 6 | 0.358906384 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 I | N(R)=1, N(S)=0 (Fragment) |
| 7 | 0.460749810 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 I | N(R)=2, N(S)=2(DTAP) (MM) Authentication Request [Malformed Packet] |
| 8 | 0.594907721 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 I | N(R)=3, N(S)=6(DTAP) (RR) Channel Release |
| 9 | 0.918148742 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=UI(CCH) (RR) System Information Type 6 |
| 10 | 0.956182515 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | F, func=UA |
| 11 | 1.054007616 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=Unknown(DTAP) (SS) |
| 12 | 1.061973702 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 I | N(R)=2, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-ACK (Network to MS) |
| 13 | 1.290475230 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=Unknown(DTAP) (SS) |
| 14 | 1.387030821 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | F, func=UA(DTAP) (MM) Location Updating Request |
| 15 | 1.392068662 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=Unknown(DTAP) (SS) |
| 16 | 1.405498089 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | F, func=UA(DTAP) (MM) CM Service Request |
| 17 | 1.610096045 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 I | N(R)=2, N(S)=0(DTAP) (SMS) CP-ACK |
| 18 | 1.620577562 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=UI(CCH) (RR) System Information Type 6 |
| 19 | 1.630555841 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=Unknown(DTAP) (SS) |
| 20 | 1.867964852 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=Unknown(DTAP) (SS) |
| 21 | 1.972592146 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 I | N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Command |
| 22 | 3.774506520 | 127.0.0.1 | 127.0.0.1 | LAPdm | 81 U | func=Unknown(DTAP) (SS) |

לא הצלחנו את הפענוח של הודעת ה SMS.

קשיים שניתן להיתקל בהם:

- KC לא נכון.
- הודעה שבורה.
- אלגוריתם פענוח לא נכון.
- הכנסת KC במלואו ולא רק את 16 הביטים הראשונים (מקבלים שגיאה).

קשיים נוספים

ניסינו בהתחלה להשתמש בKALI אך נתקלנו בכמה קשיים כמו:

- Gnuradio – בגרסאות החדשות שלהם כאשר מורידים על ידי apt לא ניתן להפעיל את המודלים של grgsm, לכן ניסינו להתקין גרסאות קודמות ונראה שהיה סלידה משימוש בpyBombs בין הפורומים השונים, למרות זאת ניסינו את ההתקנות ועדיין לא צלחנו.
- בכל update היה עדכון של ה gnuradio ככה שאם נרצה להתקין מודולים נוספים או לעדכן אנחנו נהיה בבעיה.
- הצעות לתוכנות שונות אך ללא מדריכים שנמצאו באינטרנט במשך כמה ימים ניסינו ולא מצאנו כלום בנושא.
- ניסינו להתקין גם lubuntu אך דברים השתבשו.
- בנוסף מחקנו את kali Linux מווינדוס במחשב עליו עבדנו לאחר מכן שניסינו להדליק לא הייתה מערכת הפעלה להיכנס אליה (מחקנו את grub).

פתרון שמצאו זה להשתמש בDOCKER, אנחנו השתמשנו בdragonOS.

בנוסף יצא לנו להיתקל בmailing list.

עם האנטנה נתקלנו בקשיים כמו:

- לא היה ניתן למצוא קליטה.
- לא ידענו אילו אנטנות לחבר בדיוק.
- לא הצלחנו לשלוח הודעת SMS דרך 2G.
- Gain נמוך מדי בתוכנת kalibrate.

נעזרנו בחברים אחרים בנוגע לסים שלא שלח הודעות ונסענו לאנטנה הקרובה על מנת שהקליטה לדמו תהיה טובה ונצמצם תקלות טכניות, שינינו את הgain ל-40 וזה עזר מאוד.

לא היה hopping channel וזה הקל עלינו מבחינת המידע והמדריכים שעוזרים לנו בנושא.

אחד מהדברים שבדקנו בהתחלה הוא האם hackrf עובד, בשביל הבדיקה הזאת חיברנו את המכשיר למחשב, התקנו דרייברים תואמים והפעלנו את Gqrx, הוא מאפשר לנו להאזין לגלי רדיו שניתן לקלוט, ניסינו לקלוט את ערוץ 101.5 והצלחנו לשמוע את שידור הרדיו של התחנה.

מקורות

- <https://www.ckn.io/blog/2015/11/01/sniffing-gsm-traffic> ○
- https://en.wikipedia.org/wiki/Rainbow_table ○
- <https://opensource.srlabs.de/projects/a51-decrypt> ○
- <https://www.cellmapper.net/arfcn> **מציאת אנטנות בסביבה** ○
- <https://github.com/ptrkrysik/gr-gsm> ○
- [/https://greatscottgadgets.com](https://greatscottgadgets.com) ○
- [/https://www.crazydanishhacker.com](https://www.crazydanishhacker.com) ○
- [/https://www.gnuradio.org](https://www.gnuradio.org) ○
- [/https://sourceforge.net/projects/dragonos-focal](https://sourceforge.net/projects/dragonos-focal) ○
- [/https://gqrx.dk](https://gqrx.dk) ○
- [/https://www.mail-archive.com/discuss-gnuradio@gnu.org](https://www.mail-archive.com/discuss-gnuradio@gnu.org) ○