Data Is In The Air

מאת Disscom

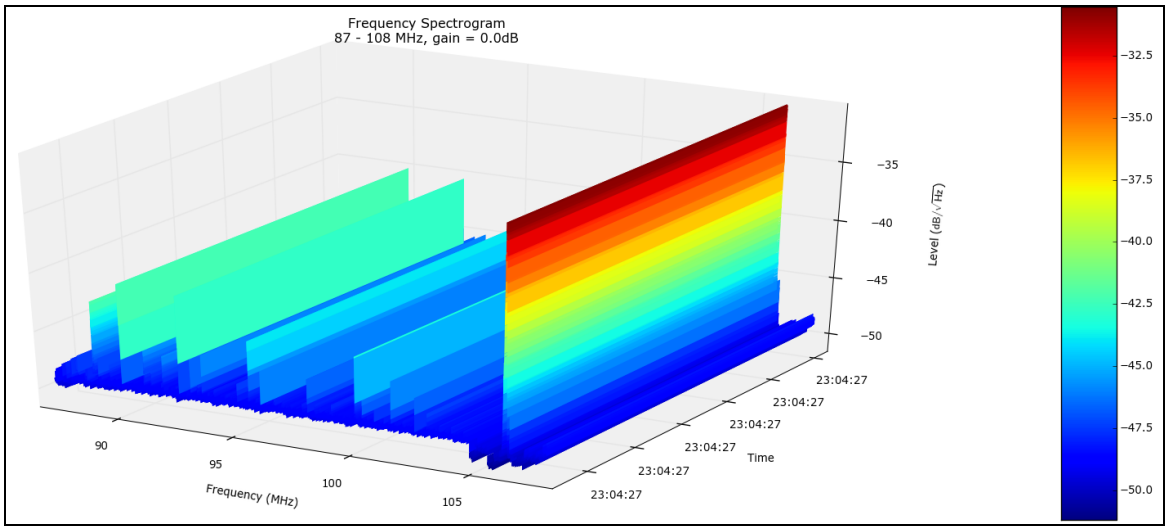
הקדמה

התחום שאני רוצה לדבר עליו הוא תחום רחב מכדי להכניסו למספר עמודים בודדים ואפילו למאות עמודים, לכן בסדרת מאמרים זו אסקור מספר נקודות עניין לשלב הראשון של מאמרים בנושא זה ובעיקר אראה כאן את הכלים הזמינים כיום. בנוסף אדבר על הידע הקיים בתחום ה-SDR-ים, בליווי דוגמאות. במאמרים הבאים בסידרה זו אצלול עוד לעומקי הנושא.

ממעבר קל על הנושאים שראיתי בגיליונות הקודמים לא ראיתי סקירה על הנושא, ואחרי התייעצות עם גוגל ראיתי שקיים רק אזכור יחיד למילה SDR בגיליונות הקודמים, משמע - יש על מה לכתוב!

אז לאחר הבטחות רבות לעצמי וגם כמה לאפיק מצאתי את הנושא שלא ישעמם אף אחד (מקווה), וגם את הזמן לכתוב, אז קדימה, מקווה שתהנו!

אז על מה אנחנו הולכים לדבר? על הדבר הבא:



מה שאנו רואים לפנינו זהו גרף ספקטוגרמי של גלי רדיו המשודרים בסביבתי, בין התדרים 87-108Mhz. במאמר אדבר בעיקר על מקורות מידע שאנו יכולים להפיק מגלי הרדיו שנעים סביבינו.

מבוא

במהלך ההיסטוריה, במרבית מכשירי הרדיו שאנו מכירים (לדוגמא מקלטי AM\FM, מקלטי טלוויזיה, מכשירי קשר מבוססי PTT ועוד דוגמאות רבות) עשינו שימוש בתדר בודד או בזוג תדרים כדי להעביר מידע בין מכשירים יעודיים, לדוגמא, מקלט רדיו FM הינו מכשיר אשר יודע לנצל קליטה של תדר אחד בלבד בזמן נתון ולבצע פעולה שאליה הוא יועד, והיא - להמיר את הגל דרך מספר רכיבים לגלי קול ושידורם דרך ממברנה של רמקול לתוך אוזנינו.

עם השנים, ההתפתחות הטכנולוגית ובעיקר שיתוף הידע במקביל לצמצום הצורך של החוקרים והמתכנתים להכיר את החומרה שעליהם הם עובדים, גרמה לכך שהתחלנו לראות בשוק מכשירי פלא אשר מסוגלים לקלוט גלי רדיו ולהעבירם למחשב כאשר כל ההגדרות נעשות על ידי המחשב. אותם מכשירי פלא מקוטלגים תחת המשפחה "Software Defined Radio", והמפורסם מבינהם הוא ה-HackRF מכשיר נהדר (אך קצת יקר) אשר מספק פלטפורמה לחוקרים. המכשיר מספק לנו רדיו שלם שבו יש לנו שליטה מלאה על כמעט כל צ'יפ שיש לו על הלוח, וזהו בעצם העידן החדש של מכשירי הרדיו מבוססי SDR.

אז מה זה בעצם SDR? - ההגדרה מוויקיפדיה באנגלית:

> **Software-defined radio** (**SDR**) is a radio communication system where components that have been typically implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system.[1] While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics render practical many processes which used to be only theoretically possible.

או בתרגום חופשי:

SDR הוא "רדיו מוגדר תוכנתית" אשר מאפשר מימוש רכיבי חומרה בתוכנה מבוססת מערכות מחשב משובץ, מימושי התוכנה בד"כ הינם מיקסרים, מסננים, אמפליפיירים ומודולטורים וכו'. למרות שהרעיון אינו רעיון חדש ניתן לראות היום התפתחות רבה בתחום של עיבוד תהליכים מעשיים שהיו עד כה תאורתיים בלבד.

אז מה נדרש ממני?

אני הצטיידתי בסט פשוט בעלות של כמה דולרים מ-eBay שכולל:

מה שמקבלים בחבילה זה מקלט פשוט, הכחול שאתם רואים, שלט ואנטנה.

ה-SDR שאנו רואים מולינו הוא בעצם מקלט (בלבד) בעל צ'יפ RTL2832U שבמקרה של הרכיב הזה יועד לשמש כמקלט טלוויזיה ורדיו למרות שרוחב הסרט שהצ'יפ תומך הינו בתחום התדרים 64mHz-1700mHz.

תחום התדרים הנ"ל מכיל הרבה יותר מסתם טלוויזיה ורדיו וזאת היא בדיוק הסיבה שבגינה התכנסנו כאן.

במאמר זה אני מעוניין לסקור מספר תחומי תדרים שניתן באמצעות מקלט בסיסי לקלוט ולהפיק את הנתונים שמועברים על-גבי הגל.

הגדרות מונחים בסיסיים:

- **מקמ"ש** - מקלט משדר, מכשיר אשר מסוגל לקלוט ולשדר למידע (בדרך כלל על גבי גלי רדיו).
- **גל רדיו** - גל רדיו הוא גל אלקטרומגנטי אשר נע בין תחומי תדרים שגבוהים מ-3kHz ונמוכים מ-300gHz, גלים אלה הם חלק מתנועה יום יומית שנעשית ממש לנגד עינינו כל הזמן בכל מקום, לצורך העניין, התמונה שאתם כרגע רואים היא אוסף צבעים שהמסך שלכם משדר. אוסף הצבעים אשר מרכיב את התמונה של המאמר הזה הם אוסף גלים שהעיינים שלנו קולטות. אור השמש גם הוא אוסף גלים שמגיעים אלינו וניתנים לפיענוח על ידי העין, רק שאלה סוג שונה של גלים. לעומתם גלי רדיו אינם ניתנים לקליטה על ידי העין אך קיימת תכונה אחרת שמאוד מעניינת בגלים האלה, עם השנים למדנו כיצד ניתן להפיק גלי רדיו **בעלי אפנון**.

- **אפנון** - אפנון הוא תהליך של "הלבשת מידע" על גבי גל נושא, קיימים מספר אפנונים בינהם אפנונים דיגיטליים ואנלוגיים, אני לא ארחיב בנושא ניתן לקרוא עוד כאן, אבל למאמר זה מספיקה ההכרות עם שתי ההגדרות, אפנון דיגיטלי ואנלוגי.

- **Simplex** - הינה שיטת העברת מידע מצד A לצד B בלבד, במצב זה ישנו צד אחד משדר וצד אחד שקולט ללא אפשרות החלפה בין הצדדים, הדוגמא הקלאסית היא הרדיו שיש לנו באוטו, אנו קולטים רק כאשר תחנת השידור משדרת.

- **Half-duplex** - שיטה זאת היא שיטה אשר מאפשרת העברת מידע בין צד A לצד B ולהפך, אבל כל אחד בתורו, לדוגמא מכשירי הווקי-טוקי שאנו מכירים, ניתנים לשידור של צד אחד בלבד בזמן נתון, אך שניהם מסוגלים לקלוט ולשדר.

- **Full duplex** - זוהי שיטת תקשורת שמאפשרת העברת מידע בין נקודה A לנקודה B באופן שוטף בין שני הצדדים, וכאן הדוגמא הקלאסית היא הטלפון הנייד שלנו, שמאפשר לנו לדבר בטלפון ללא ניהול תור של אחד הצדדים, ניתן להרחיב על כך בקישור הבא.

- **db** - הוא מערך נומרי המציין את עוצמת הגל גם ביחס קליטה וגם ביחס שידור, המדידה נעשת על ידי התרחקות מהאפס, לדוגמא קליטה בעוצמה 20db- היא קליטה חזקה יותר מ-80db-, כך גם ביחסי שידור.

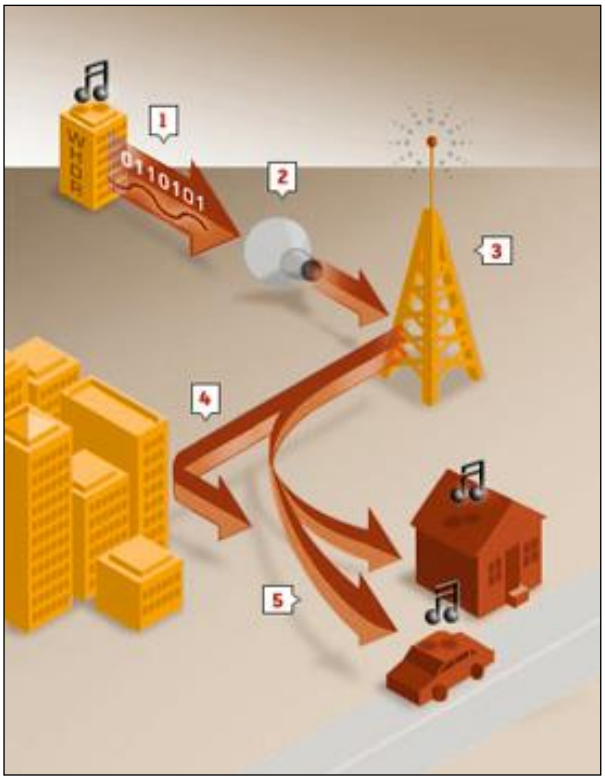
אז במה נתחיל? במה שהכי קל - אפנון FM, מי מאיתנו לא עושה שימוש בטכנולוגיה המדהימה הזאת של רדיו באוטו (או בקסדה לאופנועים שבניינו), במשרד או בכל מקום אחר?

מה זה FM?

> **FM broadcasting** is a VHF Broadcasting technology, pioneered by Edwin Howard Armstrong, which uses frequency modulation (FM) to provide high-fidelity sound over broadcast radio. The term "FM band" describes the frequency band in a given country which is dedicated to FM broadcasting. This term is slightly misleading, as it equates a modulation method with a range of frequencies.

ובתרגום חופשי - מדובר בטכנולוגיה אשר מאפשרת לאפנן גלים שנעים בתדר VHF (בעברית: תדר גבוה מאוד - תג"מ, 30-300MHz) שמשודרים בשיטת Broadcast ולהעביר על גביהם סאונד באיכות גבוהה (או במילים אחרות - רדיו) לדוגמא גלגל"צ וחבריו. ואם שאלתם איך זה עובד אז אתם במקום הנכון.

הסתכלו על התמונה.



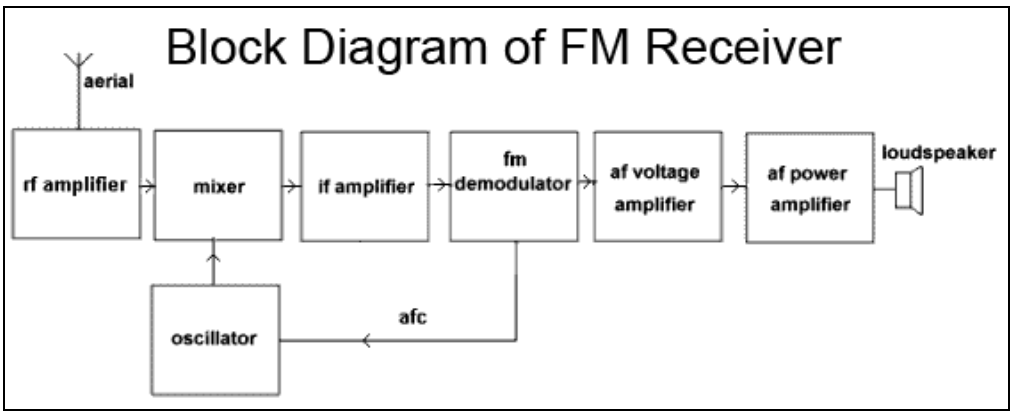
משמעותה היא כזו: קיימת **תחנת שידור** אשר משדרת מידע דיגיטלי שיכול מבחינתינו לעבור בכל דרך שרק תירצו, על-גבי רשת האינטרנט, על גבי כבל ממחשב יעודי או בעזרת כל דרך שלדעתכם יכולה להעביר אפסים ואחדות מנקודה A לנקודה B כך אנו רואים שזה נעשה בנקודה **1** שבתמנה.

נקודה מספר **2** מציינת את ה**משדר**, המשדר הוא רכיב דיגיטלי אשר בצידו האחד מקבל מידע דיגיטלי ומבצע מספר שלבים (מיד נדבר עליהם) ובסופם המידע מועבר בצורה אנלוגית לאנטנה, ומכאן ממשיכים לנקודה הבאה.

נקודה מספר **3** הינה ה**אנטנה**, האנטנה משמשת כאובייקט שמטרתו להעביר בצורה היעילה ביותר את הגלים שהוא מקבל מהמשדר לאויר, ומשם בעצם חוקי הפיזיקה מעבירים את הגלים דרך החלל שבו הם נעים עד שנקלטים בנקודות מספר **4** ו-**5** במקלטים שלנו.

ה**מקלט** עצמו הוא מערכת יחסית פשוטה ברמה האלקטרונית, אך לעיניים שאינם מהתחום - הוא בהחלט יכול להראות מורכב.

וכך נראה מבנה בסיסי של מקלט:

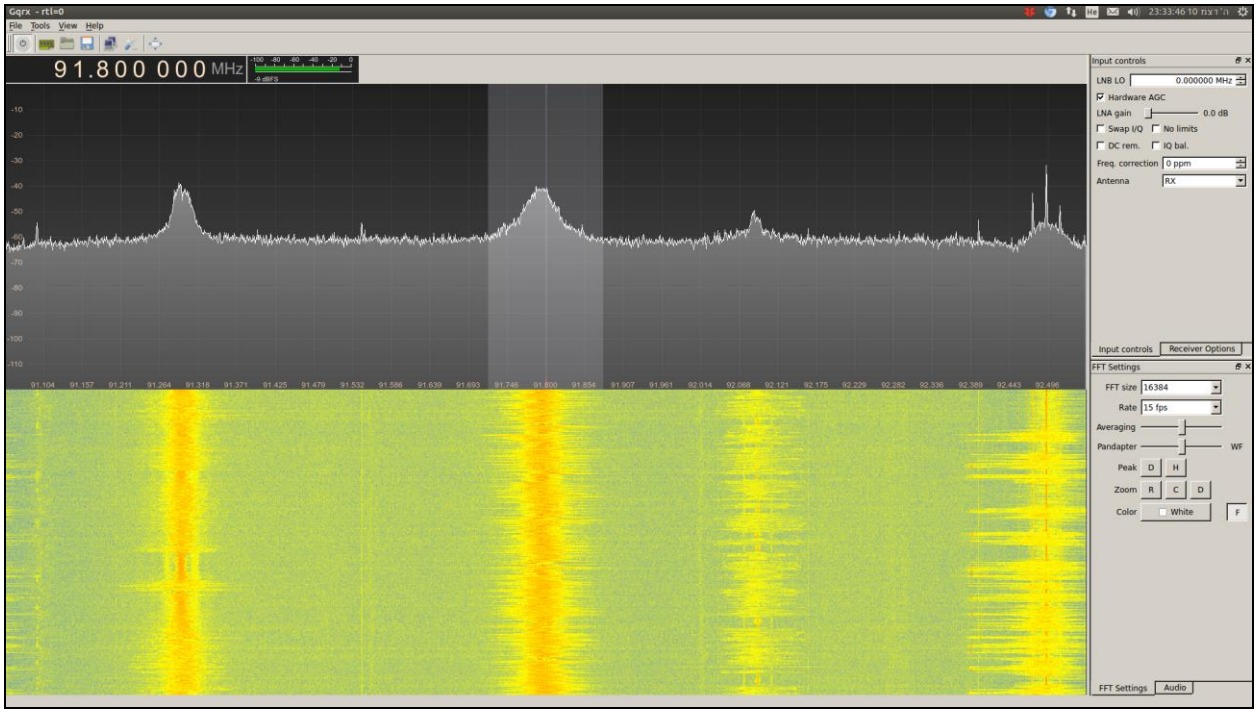


ככל הנראה, במאמרים הבאים ארחיב על נושא זה, ובעיקר על המבנה ותפקידו של כל רכיב. העניין מאוד רלוונטי כאשר נתחיל לגעת ב-GNURadio אבל נכון לחלק זה של המאמר אני רוצה לדבר על היכולת של ה-SDR שתפקידו הוא להקל עלינו - אנשי התוכנה.

החלק הרלוונטי ביותר של נושא ה-SDR-ים הוא הפטור שמקבלים אנשי התוכנה מהצורך להבין מה קיים בתרשים. בעזרתו, מספיקה הבנה בסיסית בתחום. כדי לייצר את מה שלפני מספר לא רב של שנים נדרשנו צוות פיתוח שלם שכלל (בין השאר): אנשי חומרה, אנשי קושחה, אנשי תוכנה low-level, ואם רצינו גם ממשק בסיסי, ברגע אחד זכינו למספר שנות אדם יקרות מאוד והמון המון זמן עבודה.

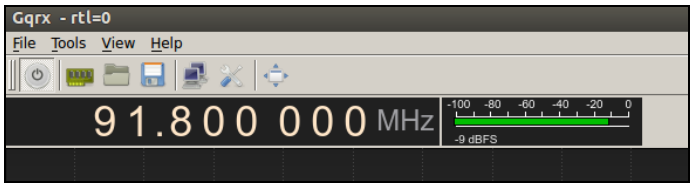
ההקלה הזאת הגיעה ברגע שבו נוצרו פלטפורמות הרדיו. המוכרת ביותר לדעתי היא ה-GNURadio, אשר מאפשרת הרכבה של המודולים שאנו רואים בתרשים, אך באופן תוכנתי בלבד. משמעות הדבר היא שמקלט הפך להיות כשמו - מקלט בלבד. והתוכנה היום היא הממשת העיקרית של רוב התהליכים אותם עוברים גלי הרדיו עד להפקה של התוצר הסופי כמו מוזיקה, ואם במוזיקה עסקינן אז למה לא להפעיל רדיו תוך כדי שאנחנו דנים בו.

תכירו בבקשה את Gqrx, מקלט רדיו שעושה שימוש ב-GNU Radio ומאפשר ניצול פשוט לכל מקלט שתומך בתדרי VHF, כמובן שהוא מבוסס על הסיפריה הגראפית של QT והוא מקל על חיינו בצורה מדהימה, הינה דוגמא:



כך ניראת האפליקציה, היא מותקנת על Ubuntu (הינה עוד קוד פתוח... למה יש משהו אחר?) אני אחלק את המסך לשלושה חלקים ואסביר מה אנו רואים.

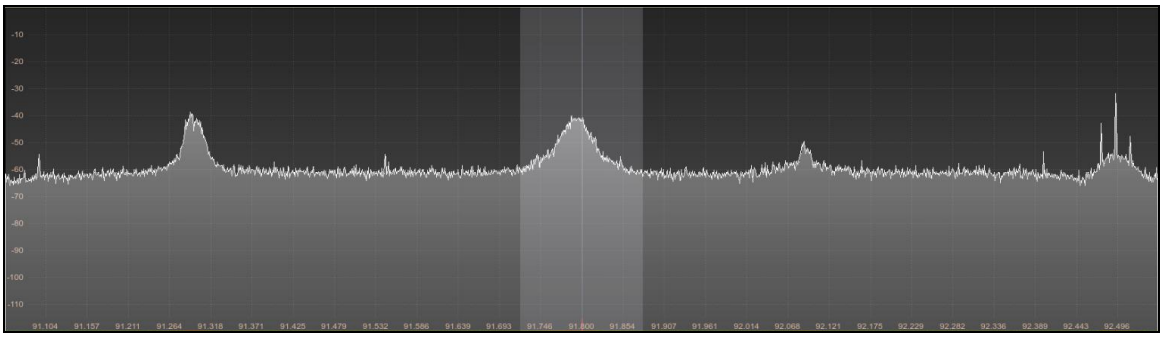
1. בצידו שמאלי העליון - **תדר**:



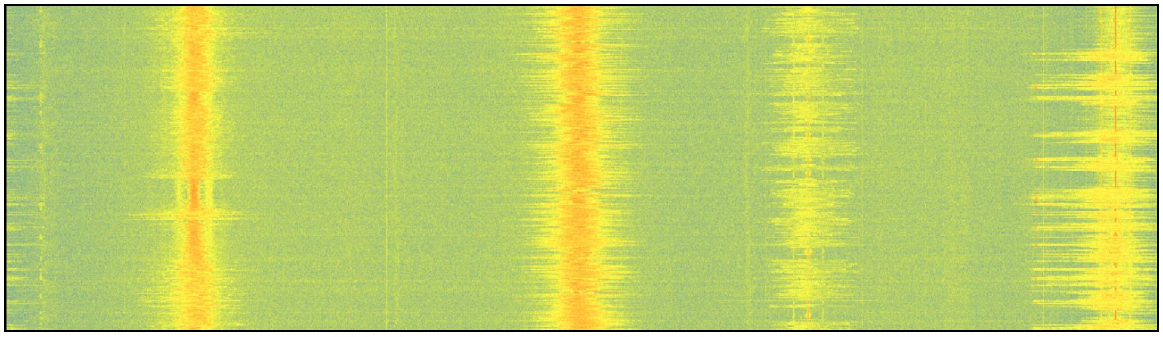
תדר, נתון בסיסי ביותר שאנו צריכים לקבוע באופן ידני, זהו בעצם תדר הגל אותו אנו מעוניינים לקלוט, התדר שאנו רואים מולנו הינו 91.8MHz - גלגלצ באיזור המרכז.

לידו אנו רואים בר ירוק הינו ה-dBFS (או בקיצור - DB), הוא בר שמראה את עוצמת הגל אותו אנו קולטים, מדד זה הינו מדד שמתיחס לכך שנקודת ה-0 היא הנקודה האולטימטיבית (כאילו הגל עובר דרך כבל) וככל שאנו מגיעים קרוב יותר ל-100- אנו לא נשמע כלום, בד"כ סף הקליטה של מקלטים אלו נע בין 70- ל-90- שזה אומר שלאחר שנעבור את אותו הרף הרחק מהאפס נאבד את יכולת הקליטה שלנו.

2. התמונה השניה היא תמונה מרשימה למדיי למקלט כל-כך פשוט: זוהי תמונה אשר נקראת **ספקטרוגרמה**, היא מציגה לנו על ציר ה-X את התדר אותו אנו שומעים ועל ציר ה-Y את עוצמת הקליטה, כאן אנו מתייחסים אך ורק למה שנקלט בזה הרגע, משמע: הגרף הינו גרף בזמן נתון:



3. התמונה השלישית היא תמונה זהה לגרף הספקטרוגרמה רק שכאן אנו רואים מפת חום אשר נפרשת על גבי ציר הזמן:



4. אם אתם שואלים מה עם ההסבר על סט ההגדרות בצד - עליו נרחיב מאוחר יותר.

בשלב זה של המאמר, רכשנו סט מושגים והגדרות כדי ליצר שפה משותפת, מכאן ואילך אדבר על שני נושאים שלדעתי נותנים השראה ורעיונות מדהימים לאיזה מידע עובר סביבינו כל הזמן, בחלק זה של המאמר אקדיש זמן רב יותר במיצוי התוכן שניתן להפיק מגלי הרדיו ובחלקו השני של המאמר נצלול עמוק יותר לכיוון המקלטים והמשדרים ומהן האפשרויות שכלי open source מספקים לנו.

Automatic Dependent Surveillance - Broadcast

הקדמה:

מערכת ADS-B היא מערכת לשירות מיקום ומצב של כלי טייס, נכון להיום כל מטוס שחג בשמיים מחוייב לשדר פולס של מידע אודותיו, המידע הזה מוגדר על ידי פרוטוקול ברור וגלובאלי אשר מהווה בסיס לכל כלי הטייס.

נכון להיום חלק חשוב מאוד באיתור כלי טייס באויר הוא באמצעות המערכת הזו, והיא משרתת כל נמל תעופה בעולם למיפוי השטח האוירי שבאחראיותו, ומעבר לכך - מערכת זאת מספקת מידע אודות כל כלי הטייס בעולם.

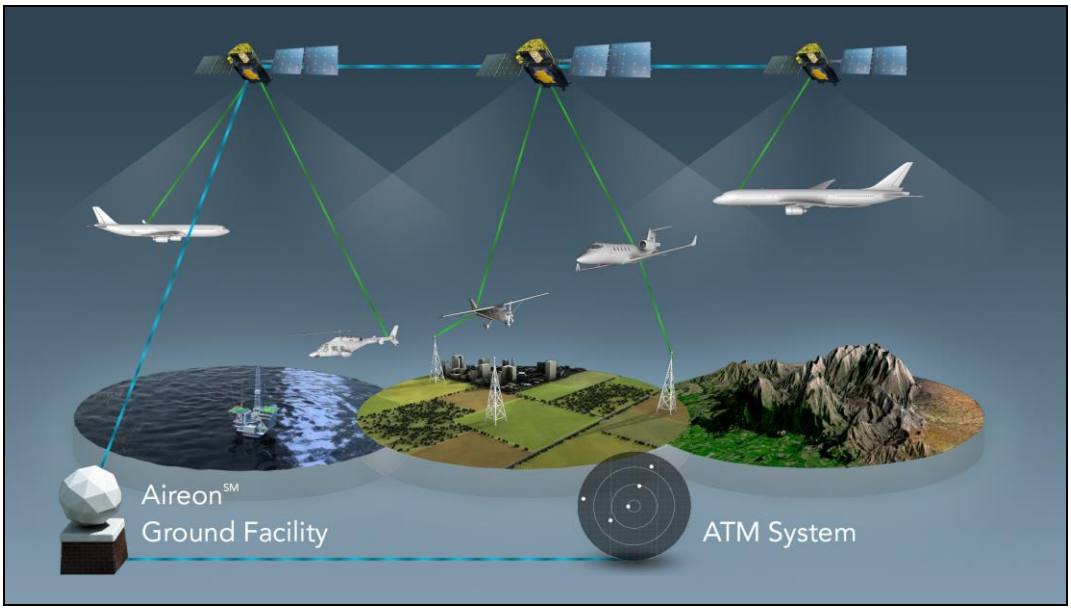
הכיצד?!

אז מה בעצם קורה כאן ואיך זה עובד? לכל מטוס יש מערכת מחשב בסיסית שמקבלת מיקום ממקלט GPS שנמצא בכל מטוס. המערכת שומרת נתונים אודות מספר הטיסה או נתיב הטיסה (בד"כ שתי אותיות בצירוף שלוש ספרות) ועוד נתונים שהינם אופציונאלים, מחשב זה אחראי על הפקדת הודעה חוקית ושידורה לכל עבר (broadcasting) כאשר ישנן שתי נקודות יציאה באמצעותן יעשה השידור:

1. שליחת הודעה על-גבי גלי רדיו בתדר 1090mHz/1030mHz או 978mHz, השידור יעשה בעזרת אנטנה רב כיוונית כדי להיקלט על ידי אחת משתי האפשרויות הבאות:
   a. תחנת קרקע כגון נתב"ג.
   b. מטוס אחר שחג גם הוא באויר בקרבת מקום (מדובר על כ-5.5 קילומטרים בערך) ושהוא יעביר את ההודעה לעמדה קרקעית.
2. שליחת המידע על גבי תווך לוויני לתחנת ניטור קרקעית.

כך או כך, כלל המידע הנ"ל יגיע בסופו של דבר לנקודה בה ישותף עם כל העולם לדוגמא האתר הזה אשר משתף נתונים אודות כל מטוס שנמצא באויר. המידע הנ"ל עובר הצלבות רבות והוא קריטי ברמה הגבוהה ביותר לניהול תקין של המרחב האוירי, אך לא זו הסיבה שלשמה התכנסנו....

בתמונה ניתן לראות את דרכי שליחת ההודעות:

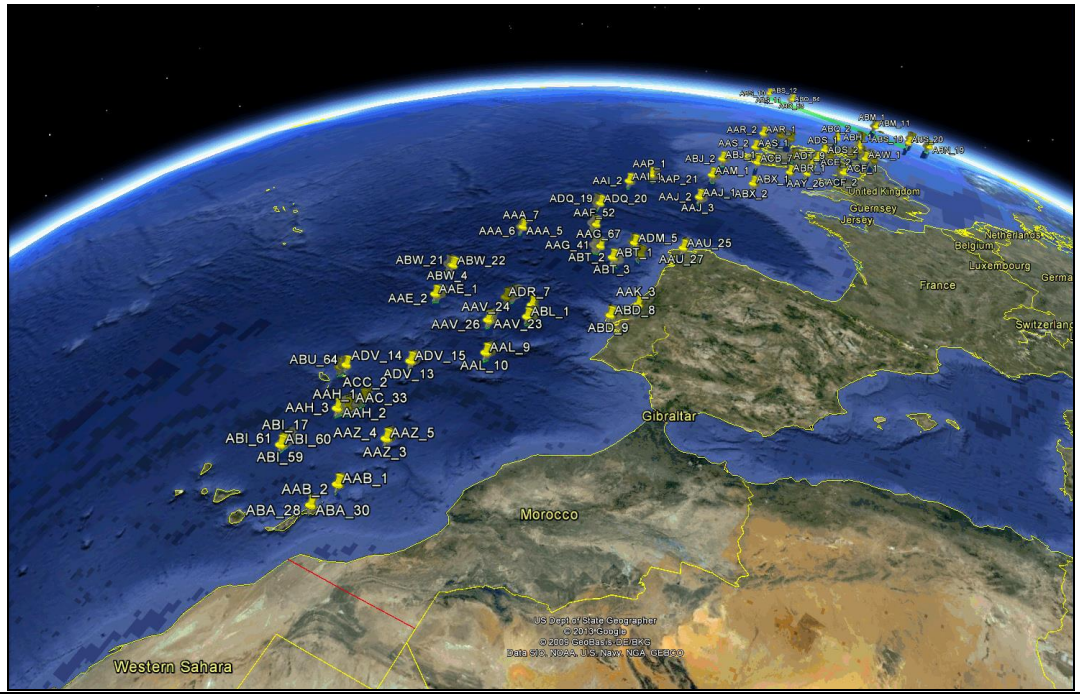


וזה לא מוצפן?!

לא (פה חשדתי בפעם הראשונה, הפעם השניה הייתה בתקשורת בין המטוסים).

אז מה עושים?

לוקחים את אותו המקלט בדיוק, לוקחים כבל ארוך ומוציאים את האנטנה מהחלון. עכשיו עוברים לחלק המעניין... ברצוני להגיע למשהו בסיגנון הבא (רק, כמובן, באיזור שלנו...):



אז איך עושים את זה? כאן הנושא נהיה **קצת** יותר מורכב (משום שכאן אנו מתחילים לעסוק בקידוד מידע והעברת מידע דיגיטלי על-גבי התווך שלנו), מידע דיגיטלי הוא בעצם מידע סיפרתי שמאופיין במספר דרכים שונות (שכרגע לא ניכנס אליהן) כאשר כל צד חייב להכיר את הקידוד והאפיון כדי להצליח להפיק את המידע שהועבר.

מה זה מצריך מאיתנו?

בגדול את אותו מקלט בדיוק, כיוונון לתדר הרלוונטי, קליטה של האות תוך פענוח הקידוד ואפיון הגל. סה"כ לא מורכב, אז בואו נתחיל בכלל מאיך ההודעות האלה נראות...

אורך ההודעה שמטוס משדר היא 112bit של סטאטוס על מצבו. 112 הביטים האלה מכילים את המידע הבא:

1. Downlink format
2. Message Subtype
3. ICAO frame - מזהה של המטוס
4. Data Frame - כאן נמצא כל המידע הרלוונטי על מצבו ומיקומו של המטוס
5. Parity check

הודעה נראת בערך כך: 8d73806e99c0589528300b6570a3. לא משהו מורכב במיוחד או עמוס בתוכן אבל מספק די הרבה. אם נרצה להסתכל על זה בצורה קצת יותר מסודרת נציג אותו כך:

CRC	DATA	ICAO24	Downlink Format
6570a3	99c0589528300b	73806e	8d

במידה ותרצו להמשיך להתעמק בתוכן של ההודעות וסוגיהן תוכלו לקבל הסבר מפורט יותר: כאן.

כעת, אני רוצה לעבור לחלק שבו אנו עושים שימוש אמיתי ב-SDR שלנו כדי לקלוט את המטוסים שעפים מעלינו, כאן אעשה שימוש באותו מקלט בדיוק אך אשתמש בכלי שניתן לראותו כאן, הוא נקרא dump1090 והוא כלי ללא ממשק גרפי אשר עושה בשבילנו את כל העבודה, ערכתי אותו קצת כדי שאוכל להציג את תוכן ההודעה בכל רגע שמתקבלת הודעה, וזהו הפלט שמתקבל:

```
*8d4baa0f99405e96c00c0d522484;
CRC: 522484 (ok)
DF 17: ADS-B message.
  Capability     : 5 (Level 2+3+4 (DF0,4,5,11,20,21,24,code7 - is on airborne))
  ICAO Address   : 4baa0f
  Extended Squitter  Type: 19
  Extended Squitter  Sub : 1
  Extended Squitter  Name: Airborne Velocity
    EW direction      : 0
    EW velocity       : 94
    NS direction      : 1
    NS velocity       : 182
    Vertical rate src : 0
    Vertical rate sign: 0
    Vertical rate     : 3
```

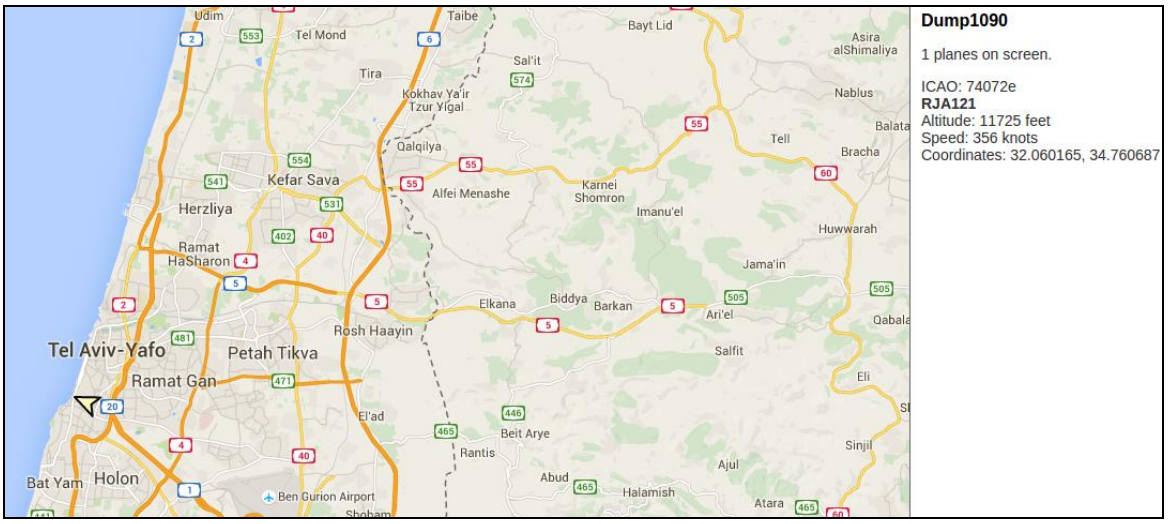
כל שנעשה כאן הוא לקודד את המידע שמגיע אלינו מהמטוסים שבאויר ולהציגו בצורה ראויה למראה.

בתמונה אנחנו יכולים לראות את הערך שנקלט ותחתיו את כל הפענוח. שוב, אתם יותר ממוזמנים להתעמק בתוכן הקישור, אך כרגע מעניין אותי להציג את כל המידע בצורה גרפית ויפה! את זה אותו כלי יודע לספק לי ע"י הרצה של הכלי עם הארגומנטים הבאים:

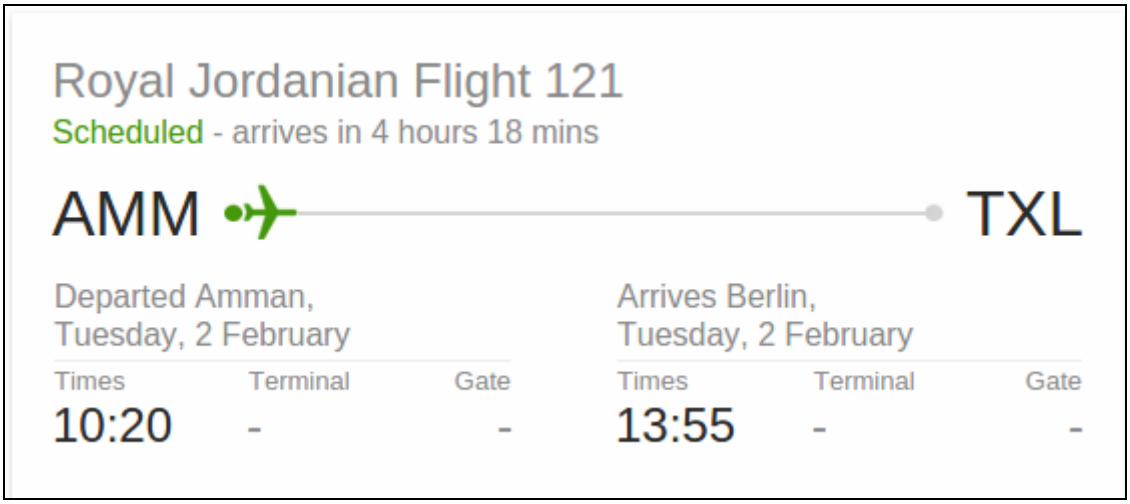
```
./dump1090 --interactive –net
```

הראשון מציין שהפעילות היא אינטרקטיבית והשני פותח האזנה בפורט 8080 ועל ידי גישה בעזרת הדפדפן, ניתן לקבל תמונת מצב נהדרת של מה שקורה סביבנו, (באופן אישי, כשאר ביצעתי את ההקלטות הללו הייתי במקום עם קליטה שאינה מקסימאלית לכן לא ראיתי יותר מ-4 מטוסים בו זמנית).

וכך זה נראה:



ניתן לראות בצידו הימני את פרטי הטיסה ובצידו השמאלי את האייקון שמסמן את המטוס, לאחר בירור אחר פרטי הטיסה בגוגל ניתן לראות שזו היא טיסה מאמן לברלין שפשוט עברה מעלינו:



כדי לוודא את אמינות הדברים נעזרתי באתר flightradar24 שמציג את כל הטיסות בעולם בזמן אמת. וכך זה נראה:

[התמונות צולמו בזמנים שונים לכן ההבדל במיקום, אבל המסלול מסביר את עצמו]

ומכאן - אנחנו ממשיכים בשידור ישיר לעבר הנושא הבא: סלולר!

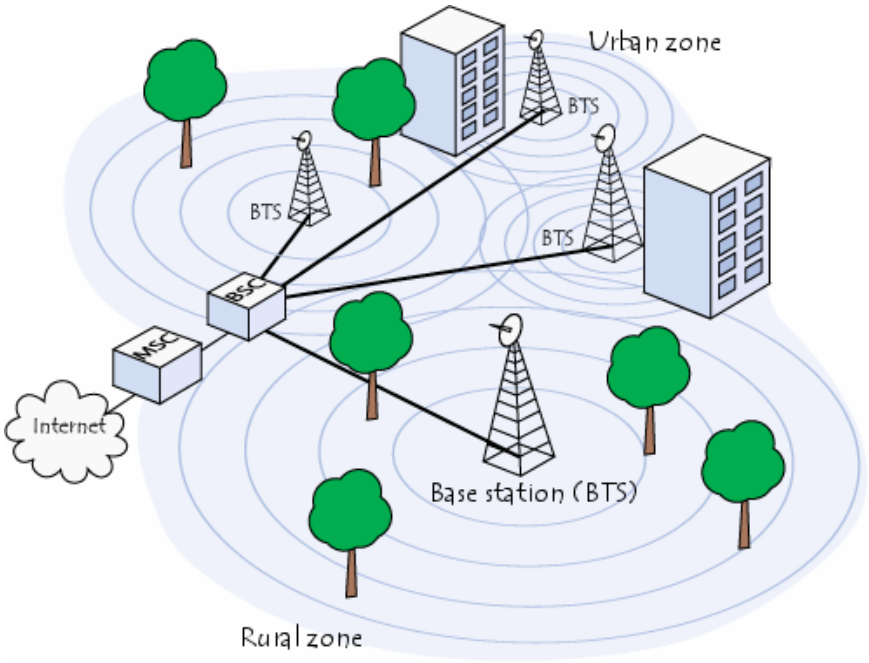
סלולר

נושא הסלולר הוא הנושא הקרוב ביותר לכל אחד מאיתנו מהסיבה הפשוטה: כל אחד ממי שקורא כרגע את המילים במאמר קולט ומשדר ללא הפסקה בעזרת הטלפון הנייד שלו מידע לרשת הסלולרית הלוך ושוב, רגע לפני כל ההסברים בואו נראה (בגדול מאוד) איך נראת הרשת הסלולרית.

מבוא לרשת סלולרית:

הרשת הסלולרית שונה לחלוטין מהרשת שאותה אנו מכירים כרשת האינטרנט, למרות השימוש הנרחב וקשרי הגומלין ההדוקים הקיימים בין השתיים (בעיקר בתקופה האחרונה: רמז 4G ו-LTE) אשר מספקים לנו גישה ברוחב פס רחב לרשת האינטרנט - לא כך הדבר, לפחות לא במלואו.

רשת הסלולר נפרסת על בסיס ציוד משדרים ומקלטים אשר נקראים BTS, הרכיבים האלה נקראים בעברית "תא סלולרי" והם בעצם רכיבים שמנהלים את התקשורת בין הטלפון הסלולרי למרכזיה (ספק תקשורת) הקישור אשר נעשה בין ה-BTS לבין הספק הוא בד"כ חיבור קווי (לפחות ברובו) ולכן לא אדבר אליו במאמר זה.



הקישור המחבר בין ה-BTS לטלפון הנייד שלנו נעשה ע"י קליטה ושידור נתונים המתבססים על מספר תדרים או תקני תקשורת שאותם אנו מכירים בתור 2G/3G/4G. אותם תקנים מגירים לנו, בין היתר, את תדרי השימוש בארץ אשר מוצגים להלן:

GSM 900, GSM 1800	2G capabilities
UMTS 850, UMTS 2100	3G capabilities
LTE 1800 (Band 3), LTE 2600	4G capabilities

[כלל המספרים מציגים יחידת מידה ב-Mhz]

תפקידו של ה-BTS הוא לנהל איזור גאוגראפי מסויים (שהאנטנה מכסה אותו) על ידי ניהול המנויים הבאים והשבים. לכל תא סלולרי יש מספר מנויים (טלפונים ניידים) שהוא מסוגל לנהל בזמן שיחה ובזמן המתנה.

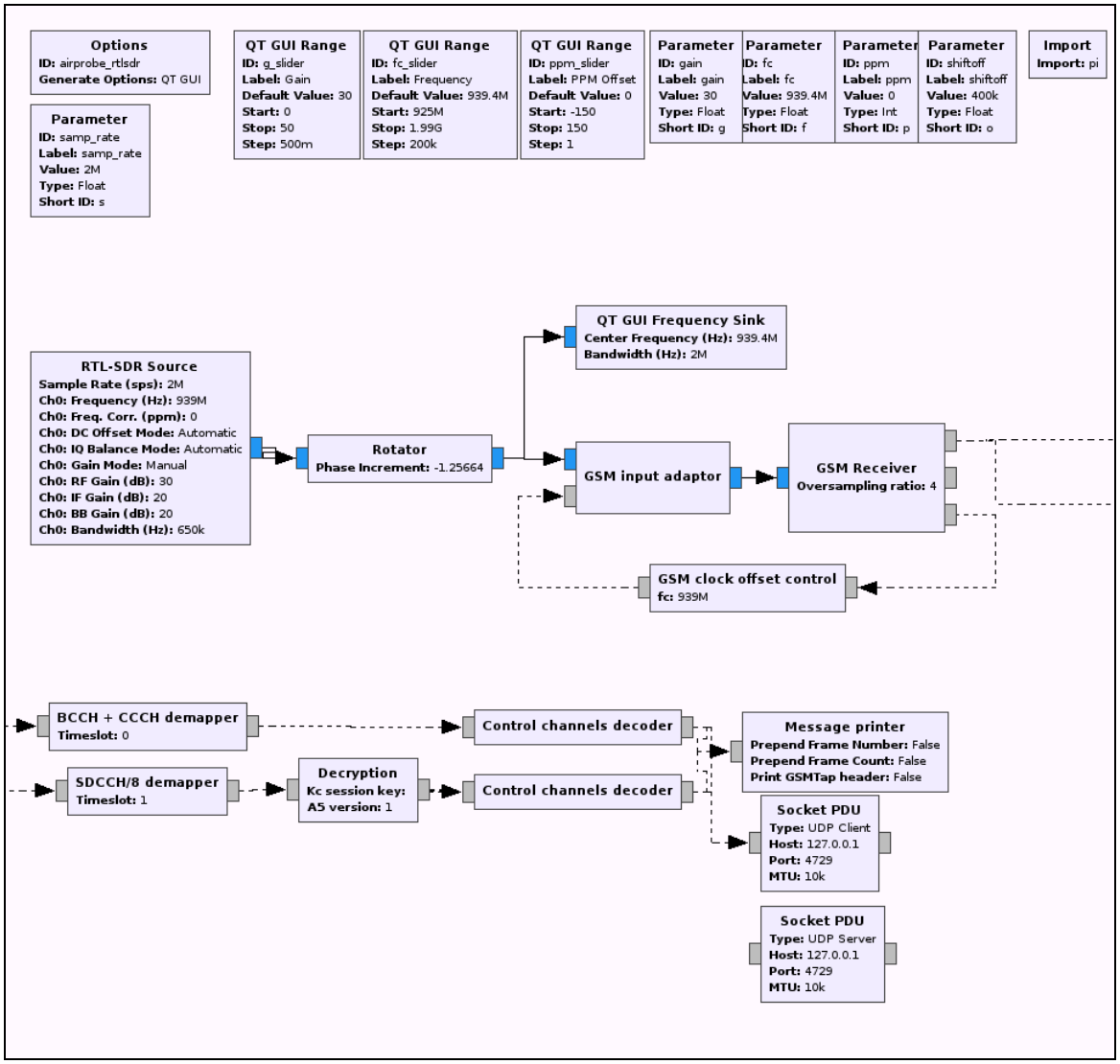
תא סלולרי מנוהל על ידי הרשת הסלולרית ועל ידי המרכזיה הרלוונטית אליו, ומצידו השני נראה אנטנות אשר נראות כך:

[אם תרצו להקים חברת סלולר או סתם תא סלולרי תוכלו להשתמש בפרוייקט הזה אשר מספק תשתית open source להקמה של BTS]

GNURadio הוא אחד התשתיות הטובות ביותר לעבודה עם SDR-ים, הוא מספק דוגמאות רבות למימושים של שרשראות קליטה ומאפשר לנו יכולת גמישות מלאה בכל מה שנרצה לעשות איתו (עוד פרטים יהיו במאמרים הבאים עם דוגמאות).

בדוגמא שאציג לכם התקנתי GNURadio ו-הורדתי את הכלי GR-GSM. יש אומנם סט התקנות שיכול לעשות חיים לא קלים לפעמים, אך בסוף יש שני דברים שצריכים לעניין אותנו: **הראשון** הוא אוסף הכלים והסיפריות שמספקת לנו GNURadio, ובלדיען היה מורכב הרבה יותר לעשות כל דבר - ולו הפשוט ביותר. **השני** הוא סט של סקריפטים שמביאים אותנו ליעד שאנו מעוניינים בו - קליטת תקשורת סלולרית.

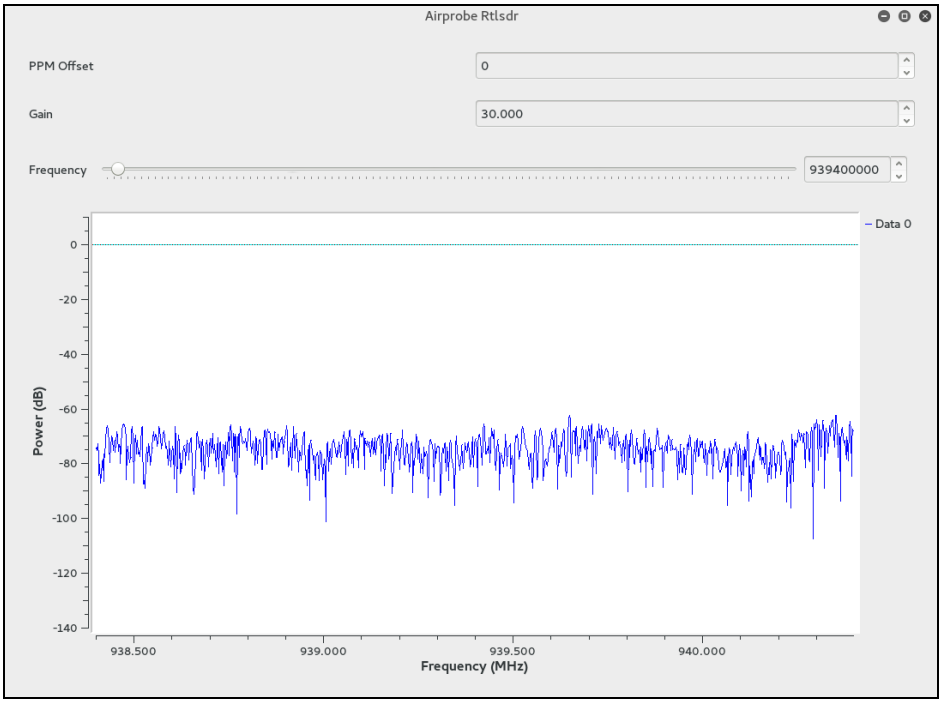
נתחיל בדוגמא של שרשרת קליטה שמומשה בעזרת GNURadio מותאם ל-GSM ועושה שימוש ב-SDR RTL שאנו מכירים מתחילת המאמר:



התמונה שלפניכם מציגה את כל אחד מהשלבים שהאות האלקטרומגנטי עובר עד להפקה של המידע הספרתי, שבסופו של דבר הוא המידע הרלוונטי.

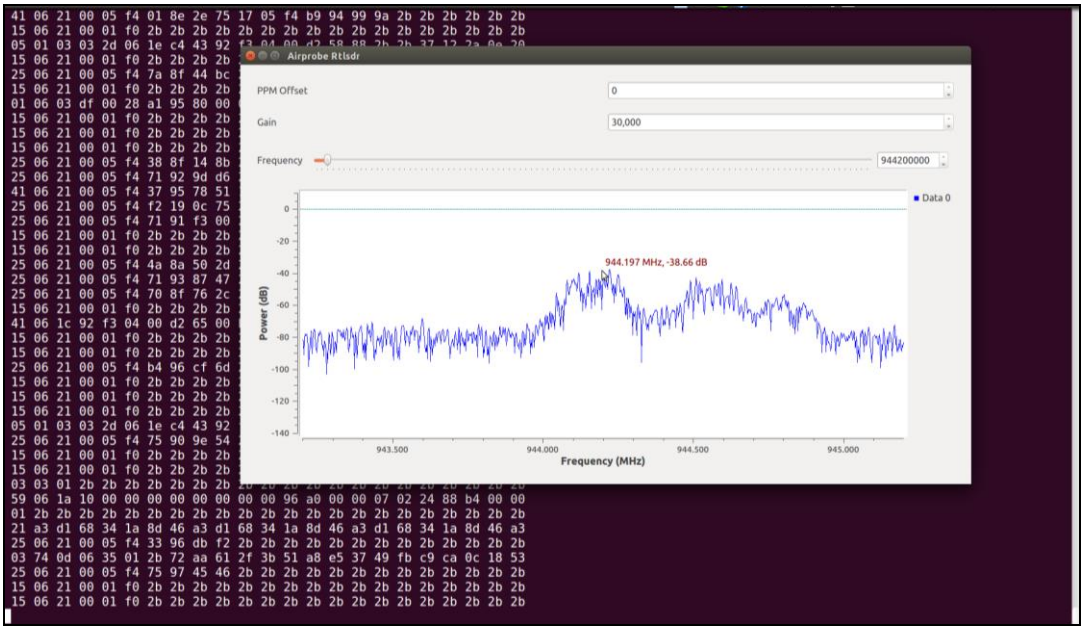
כל אחד ואחד מהשלבים שאנו רואים לפנינו יפורט במאמר הבא בו נעשה שימוש נרחב יותר ביכולות של GNURadio.

כאשר לוחצים על Execute the flow graph, שזהו הכפתור אשר מישם את המימוש שלנו נראה כי יפתח לנו חלון אשר מציג גרף ספקטוגרפי של התדר 939Mhz - שזהו התדר שמוגדר בשלב הראשון של השרשרת מצידו השמאלי (RTL-SDR Source) וזה מה שנראה:



קצת מת כמו שאתם רואים... לא מפתיע במיוחד. כאשר איננו רואים "פיקים" כלפי מעלה והגלים נעים סביב תדר קבוע בד"כ נמצא עצמינו קולטים רעש לבן שאיננו בעל תוכן "קריא" בשביל המקלט שלנו.

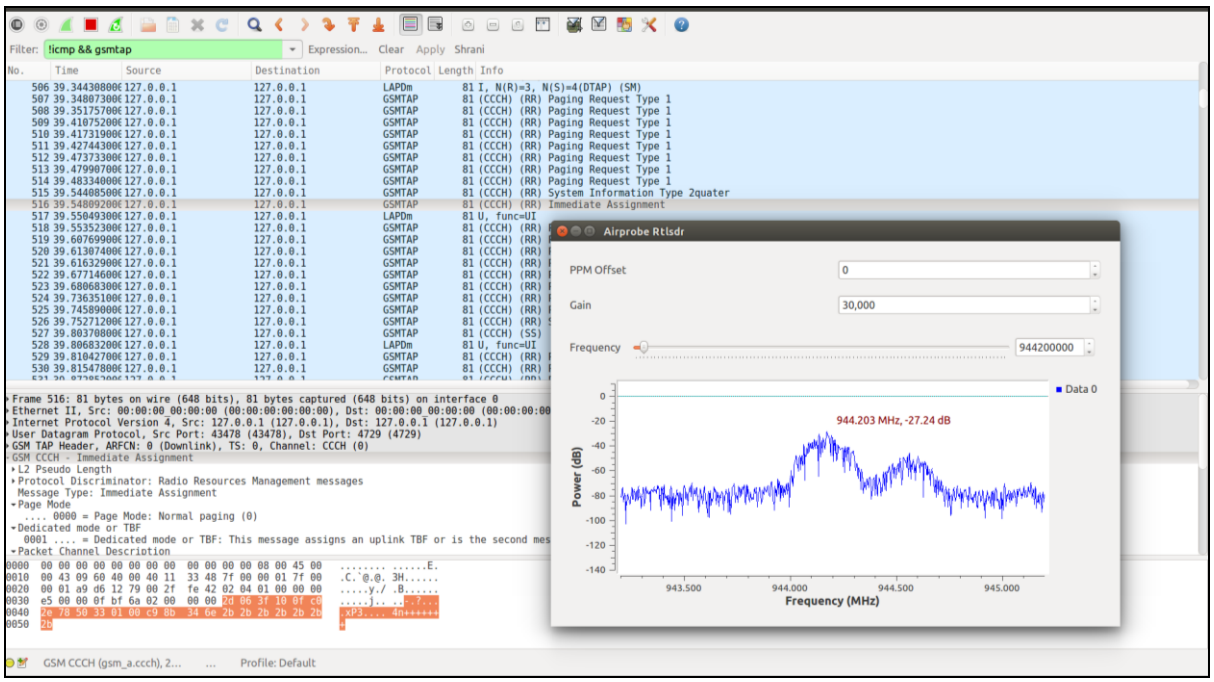
ממשיכים לשחק טיפה עם התדרים עד שמקבלים תנועה שונה של הגל:



וכאן, למען הגילוי הנאות, חשוב לי לציין כי מרגע זה כלל התמונות אשר מצורפות למאמר הן תמונות שלקחתי מאתרי אינטרנט שונים על מנת לא לפרסם מידע של האנשים סביבי.

ברגע שאנו רואים את השורות בטרמינל או ב-GNURadio מתחילות להתמלא אנו יכולים להבין שאנחנו "על הגל" ומכאן אנו בעצם מתחילים לקלוט מידע סלולרי סביבנו.

כמובן שכך לא ניתן להבין כלום. אך מי שפיתח את האפליקציה הזו חשב על הכל עד הסוף, ובעזרת פתיחה של wireshark והאזנה על lo ופילטור של gsmtap נקבל את המצב הבא:



מכאן - הדרך רק נפתחת לדימיון פורה ולאין סוף אפשרויות שנמשיך ונדבר עליהם במאמרים הבאים...

סיכום

לסיכום, עברנו במאמר על שלושה נושאים (פסאדו) אקראיים שנתנו לנו דוגמא קלה ליכולות של ה-SDR, סה"כ הסתכלנו בשלושה תדרים רזים עם SDR פשוט, אותו SDR יכול לשמש אותנו לקליטה של כל התדרים שהוא תומך בהם ובעצם באין ספור מידע שנע סביבנו, החל משידורי רדיו וטלוויזיה ועד לתקשורת דיגיטאלית, האפשרויות אינן מוגבלות וכמות המידע סביבנו הינו חסר הגבלה ומעניין כל תדר מחדש, באופן אישי לאחר החשיפה שלי לתחום גיליתי תחום מדהים שברח מהרדר שלנו שנים רבות.

במאמרים הבאים נדבר לעומק על היכולות של GNUradio ועל פוטנציאלי השידור שמתאפשרים לנו עם SDR מתקדמים יותר, כמובן שאשמח לשמוע מכם אם נושאים מסויימים מעניינים אתכם במיוחד.

נתראה במאמרים הבאים!

מקורות

- http://www.hdradio.ch/en/howdoesitwork/index.html
- http://www.wikipedia.com
- http://4.bp.blogspot.com/-BRBIuvm-EHk/T9IZkLFlyKI/AAAAAAAAAoc/7CWXkqT4nHo/s1600/Block-Diagram-of-FM-Receiver.png
- http://www.esa.int/var/esa/storage/images/esa_multimedia/images/2013/06/proba-v_ads-b_aircraft_detection_europe/12884185-1-eng-GB/Proba-V_ADS-B_aircraft_detection_Europe.jpg
- http://static.commentcamarche.net/en.kioskea.net/pictures/telephonie-mobile-images-reseau-cellulaire.png
- http://www.gsmarena.com/network-bands.php3?sCountry=ISRAEL
- http://www.mbs.ie/antenna3.htm
- https://pravokator.si/wp-content/uploads/2015/10/airprobe_rtlsdr.png
- http://cdn.satellitetoday.com/wp-content/uploads/2015/02/Aireon_GlobalSpaceBasedADSB_Coverage.jpg
- http://adsb-decode-guide.readthedocs.org/en/latest/introduction.html
- https://pravokator.si/wp-content/uploads/2015/10/airprobe_rtlsdr_wireshark.png