אז מה זה בעצם GSM ?

GSM (global system for mobile communication) זוהי טכנולוגיה המשמשת להעברת קול ומידע באופן דיגיטלי. פועלת בערוצים : 850MHz, 900MHz, 1800MHz, 1900MHz.  
GSM עובדת בשיטה של TDMA כלומר חלוקת משאבי התקשורת למשתמשים ע"פ זמן.

מבנה טכנולוגית ה GSM  
GSM זוהי בעצם מערכת גדולה הבנויה מכמה מערכות קטנות :

**Mobile station(MS) –** מכשיר המשמש לתקשורת למשל טלפון פקס וכו

**Base station subsystem(BSS)-**מתחבר ל MS באמצעות תקשורת רדיו .ה BSS מורכב משני חלקים :

BTS(Base tranciver system) .1  
בעצם ה MS מתחבר ל BTS שנמצא בקרבתו הBTS שולח אות ל BSC (יכולים להיות כמה BTS המחוברים לאותו BSC)  
2. BSC(Base station controle)  
ה-BSC מחובר לMSC

**Network and switching subsystem(NSS)-**  
מכיל את ה MSC שהוא עמוד השדרה של המערכת כולה .   
בנוסף מכיל עוד שלושה רכיבים :   
HLR .1 – (Home location register) שומר דאטה בייס של כל המשתמשים שנמצאים באותו אזור גאוגרפי

VLR .2-(Visitor location register) שומר מידע על כל המשתמשים שמבקרים באזור גאוגרפי ספציפי (בעיקר לקוחות נודדים)

AUC .3-(Authentication center ) שולט על הזדהות המשתמשים ע"י בדיקת מספר הסים שלהם ושולח את המידע המבוקש ל MSC.

**Operating subsystem(Oss)-**   
משתמשים בו בעיקר על מנת לשלוט בתעבורה

Diagram

Description automatically generated

RTL -SDR

RTL הוא בעצם קיצור ל RTL2832U אנו נשתמש ב reciver RTL-SDR כסורק של גלי רדיו על מנת לקבל סיגנלים באזורנו.

אופן המתקפה

לכל BTS יש cell identity (Cell ID) ייחודי המאפשר לזהות אותו.

[What is GSM? (tutorialspoint.com)](https://www.tutorialspoint.com/what-is-gsm)

[Mobile Communication 4 - What is GSM ? ( GLOBAL System for MOBILE ) - Bing video](https://www.bing.com/videos/search?q=GSM+WHAT+IS+IT+&&view=detail&mid=FF53D790FDF6F77A95C5FF53D790FDF6F77A95C5&&FORM=VRDGAR&ru=%2Fvideos%2Fsearch%3Fq%3DGSM%2BWHAT%2BIS%2BIT%2B%26FORM%3DHDRSC4) -סרטון על GSM

[What is GSM Technology : Architecture, Circuit Working & Its Applications (elprocus.com)](https://www.elprocus.com/gsm-technology-architecture-its-applications/#:~:text=The%20operation%20support%20subsystem%20%28OSS%29%20is%20a%20part,the%20GSM%20network%20%26%20the%20BSS%20traffic%20load.) -הסבר מפורט על כל המרכיבים

[GSM: Sniffing SMS traffic - The poetry of (in)security (ckn.io)](https://www.ckn.io/blog/2015/11/29/gsm-sniffing-sms-traffic/) – פקודת [**gr-gsm**](https://github.com/ptrkrysik/gr-gsm)  מפורטת .