Implementasi Gr-GSM Untuk Decoding Komunikasi GSM Terenkripsi

Brian Rizky Rivaldy
Telkom University
brianrizkyrivaldy@gmail.com

Henry Rossi Andrian, S.T., M.T.
Telkom University
rossi@tass.telkomuniversity.ac.id

Moch Fahru Rizal, S.T., M.T.
Telkom University
mfrizal@tass.telkomuniversity.ac.id

Abstrak

Dalam penulisan proyek akhir ini membahas mengenai *decoding* komunikasi GSM terenkripsi. Alat yang digunakan adalah RTL-SDR yang dapat menangkap sinyal BTS (*Base Transceiver Station*) dan aplikasi Gr-GSM untuk proses *decoding* data yang ditangkap dari BTS. Tujuan dari penulisan proyek akhir adalah untuk menganalisis keamanan data pada jaringan komunikasi GSM. Dari hasil analisis ini dapat disimpulkan bahwa, dari proses pengujian penangkapan sinyal dan *decoding* mendapatkan informasi operator dari frekuensi berupa GSM Frame Number, IMSI (*International Mobile Subscriber Identity*), TMSI (*Temporary IMSI*), algoritma keamanan yang digunakan pada operator, dan data komunikasi pada keamanan GSM.

Kata Kunci: GSM, RTL-SDR , Gr-GSM, *decoding*, analisis

Abstract

In this final project writing discusses the decoding of encrypted GSM communications. The tool used is RTL-SDR which can capture BTS (Base Transceiver Station) signal and Gr-GSM application for data decoding process captured from BTS. The purpose of writing the final project is to analyze data security on GSM communication networks. From the results of this analysis can be concluded that, from the process of testing the signal capture and decoding obtain operator information from the frequency of GSM Frame Number, IMSI (International Mobile Subscriber Identity), TMSI (Temporary IMSI), security algorithm used on operators, and communication data on GSM security.

Keywords: GSM, RTL-SDR, Gr-GSM, decoding, analyze

Pendahuluan

Pemanfaatan teknologi sudah banyak digunakan dan salah satu jenis teknologi yang digunakan adalah teknologi komunikasi. Dengan berkembangnya teknologi komunikasi sekarang manusia dapat melakukan komunikasi dimana saja, kapan saja dan oleh siapa saja. Teknologi komunikasi dengan layanan bergerak atau yang sering disebut GSM (*Global System for Mobile Communication*) juga mengalami perkembangan yang sangat cepat dimulai dari layanan 1G sampai dengan 4G.

Secara umum di Indonesia jaringan komunikasi yang banyak dipakai adalah GSM. Sebagian besar operator GSM telah meningkatkan layanan keamanan, namun masih ada peluang bagi para penyerang dalam bidang bisnis dengan tujuan untuk mendapatkan data-data jaringan GSM dan menjual ke pihak lain. Kemudian ada juga penyerang yang bertujuan untuk mengacaukan

sinyal GSM yang dapat mengganggu kenyamanan pengguna.

Maka dari itu proyek akhir ini akan melakukan analisis pada keamanan jaringan komunikasi GSM menggunakan alat untuk menangkap frekuensi sinyal dari BTS yaitu perangkat RTL-SDR yang berfungsi untuk diambil dan dibaca data-data nya menggunakan metode dekripsi dengan program Gr-GSM. Perlunya analisis ini adalah untuk masyarakat yang masih menggunakan jaringan komunikasi GSM disarankan untuk pindah ke jaringan komunikasi yang lebih aman.

Adapun perumusan masalah dari paparan latar belakang tersebut adalah sebagai berikut:

1. Bagaimana cara instalasi dan konfigurasi RTL-SDR pada Ubuntu 14.04 LTS?
2. Bagaimana cara instalasi dan konfigurasi Gr-GSM di Linux Ubuntu 14.04 LTS?
3. Bagaimana proses *decoding* data komunikasi GSM terenkripsi?

Adapun tujuan dari jurnal ini adalah sebagai berikut:

1. Mengimplementasikan RTL-SDR pada Ubuntu 14.04 LTS.
2. Mengimplementasikan Gr-GSM pada Ubuntu 14.04 LTS.
3. Mengimplementasikan proses *decoding* data komunikasi GSM.

Adapun batasan masalah dalam pembahasan ini adalah sebagai berikut:

1. Tidak membahas encoding sinyal.
2. Tidak membahas protokol komunikasi.
3. Hanya menangkap sinyal GSM.
4. Hanya membahas keamanan komunikasi pada GSM.
5. Hanya menangkap sinyal *broadcast* dari BTS.

Tinjauan pustaka yang digunakan pada jurnal berikut adalah :

1. Linux Ubuntu 14.04

Ubuntu Versi 14.04 “Trusty Tahr” merupakan distribusi Linux yang paling populer menggunakan user interface Unity yang khas dan disesuaikan. Trusty Tahr merupakan edisi dengan dukungan jangka panjang “Long Term Support” (LTS) selama 5 tahun, berupa dukungan keamanan berikut jalur upgrade yang lebih mudah dibandingkan rilis versi LTS (12.04) sebelumnya.

2. GSM (*Global System for Mobile Communications*)

Global System for Mobile Communication (GSM mulanya singkatan dari *Groupe Spécial Mobile*) adalah sebuah teknologi komunikasi seluler yang bersifat digital. Teknologi GSM banyak diterapkan pada komunikasi bergerak, khususnya telepon genggam. Teknologi ini memanfaatkan gelombang mikro dan pengiriman sinyal yang dibagi berdasarkan waktu, sehingga sinyal informasi yang dikirim akan sampai pada tujuan. GSM dijadikan standar global untuk komunikasi seluler sekaligus sebagai teknologi seluler yang paling banyak digunakan orang di seluruh dunia.

3. SDR (*Software Defined Radio*)

Software Defined Radio (SDR) ada yang menyebut juga *software radio* (SWR) diperkenalkan pertama kali pada tahun 1991 oleh joseph mitola istilah SDR ini digunakan untuk menujuk sebuah kelas radio yang dapat dikonfigurasikan ulang diprogam ulang, sehingga menghasilkan sebuah jenis perangkat komunikasi nirkabel dengan mode dan bend frekunsi ditentukan oleh fungsi perangkat lunak . SDR memiliki keuntungan karena sifat fleksibelitas (*flexsibeltiy*) ,lengkap dan dapat dikonfigurasikan ulang secara mudah (*complete and easy reconfigurasiability*) dapat disekala, dapat diperogam ulang (*reprogrammability*) secara dapat diperluas (*expandability*) .

4. Decoding

Decoding adalah proses kebalikannya dari encoding, yaitu konversi data yang telah dikirimkan oleh sumber pesan menjadi informasi yang dimengerti oleh penerima.

5. PyBombs

PyBOMBS (*Python Build Overlay Managed Bundle System*) adalah sistem manajemen baru yang digunakan untuk proses installasi GNURadio agar dapat berjalan

dengan baik. GNURadio dasarnya menggunakan bahasa pemrograman python.

Tujuan utama pybombs adalah untuk menggabungkan beberapa aplikasi yang digunakan untuk menyelesaikan suatu projek dengan menggunakan bahasa pemrograman python. Maka pybombs merupakan sistem dasar yang harus ada sebelum menggunakan GNURadio.

6. Kalibrate

Kalibrate adalah program Linux yang dapat memindai BTS GSM pada pita frekuensi yang diberikan dan dapat menggunakan BTS GSM untuk menghitung keseimbangan frekuensi osilator lokal.

7. Enkripsi

Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah.

8. GNU Radio

GNU Radio adalah perangkat lunak untuk membangun dan menyebarkan perangkat lunak sistem radio. Kerangka GNU Radio menyediakan pemrosesan sinyal yang panjang dan pengolahan blok untuk berkomunikasi dengan perangkat keras. GNU Radio telah digunakan array besar aplikasi radio dunia nyata, termasuk pengolahan audio, komunikasi ponsel, pelacakan satelit, sistem radar, jaringan GSM, dll.

9. RTL-SDR

RTL-SDR adalah sebuah usb dvb-t yang digunakan untuk menangkap siaran televisi digital. Alat ini hanya digunakan untuk streaming siaran televisi digital saja, namun bisa digunakan menjadi alat penerima multi-mode dan multi-band atau sebut saja alat yang bisa digunakan sebagai hardware SDR. Chipset DVB-T RTL-SDR adalah Realtek RTL2832U yang mampu menangkap signal radio dan frekuensi tertentu dan paket tersebut dalam bentuk RAW data, tentunya untuk dapat menterjemahkan RAW data ke dalam computer maka diperlukan software yang mampu melakukan proses decoding tersebut seperti GNURadio.

10. Pip

Pip adalah sistem manajemen paket yang digunakan untuk menginstal dan mengelola paket perangkat lunak yang ditulis dengan python.

11. Gr-GSM

Gr-GSM adalah proyek yang berdasarkan penerima GSM yang ditulis oleh Piotr Krysik (juga penulis utama gr-gsm) untuk proyek Airprobe. Tujuannya adalah untuk menyediakan seperangkat alat untuk menerima informasi yang dikirimkan oleh peralatan / perangkat GSM.

12. Airprobe

Airprobe adalah salah satu proyek dari Gr-GSM. Airprobe merupakan aplikasi pendukung alat RTL-SDR untuk *decoding* GSM. Dengan aplikasi ini dengan mudah untuk *decoding* sistem sms GSM.

13. GSM Framecoder

GSM Framecoder adalah aplikasi untuk menghitung *bursts* yang dihasilkan pada paket GSM untuk dapat di *decoding* datanya.

14. Gcc

Gcc adalah kompiler GNU C, namun karena kompilator mendukung beberapa bahasa lain selain C.

15. Osmo Sim Auth

Osmo-sim-auth adalah script kecil yang bisa digunakan dengan *smart card* berbasis PC. Osmo-sim-auth berfungsi sebagai pembaca untuk mendapatkan parameter otentikasi GSM / UMTS dari kartu SIM / USIM.

16. PCSC

PC/SC (singkatan dari "*Personal Computer / Smart Card*") merupakan sebuah spesifikasi antarmuka untuk mengintegrasikan kartu pintar ke dalam aplikasi berbasis komputer.

17. Swig

Simple Wrapper and Interface Generator (SWIG) adalah perangkat lunak sumber terbuka yang digunakan untuk menghubungkan program komputer atau perpustakaan yang ditulis dalam bahasa C atau C++ dengan bahasa *scripting* seperti Lua, Perl, PHP, Python, R, Ruby, Tcl, dan

bahasa lainnya. Seperti C#, Java, JavaScript, Go, Modula-3, OCaml, Octave, Scilab dan Scheme. Output juga bisa dalam bentuk XML atau Lisp S-expression.

18. Pyscard

Pyscard adalah perangkat lunak bebas, yang dapat mendistribusikan atau memodifikasi berdasarkan ketentuan dari *GNU Lesser General Public License* yang diterbitkan oleh *Free Software Foundation*.

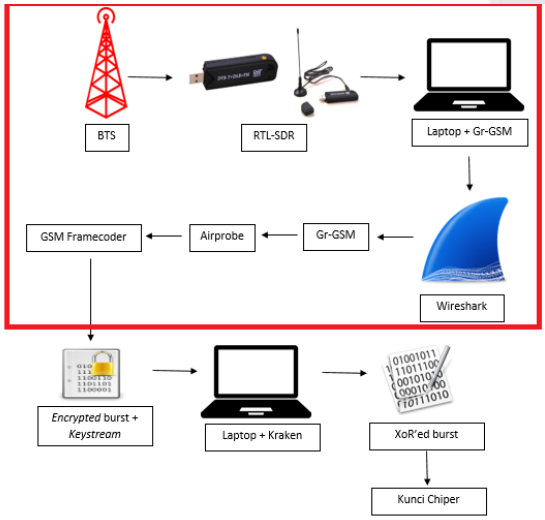
19. Wireshark

Wireshark adalah alat analisis jaringan yang sebelumnya dikenal dengan Ethereal. Wireshark dapat menangkap paket secara *real time* dan menampilkannya dalam format yang mudah dibaca manusia. Pada dasarnya, wireshark adalah penganalisis paket jaringan yang memberikan rincian singkat tentang protokol jaringan, dekripsi, informasi paket, dll. Wireshark adalah sumber terbuka dan dapat digunakan di Linux, Windows, OS X, Solaris, NetBSD, FreeBSD, dan banyak lainnya. Sistem informasi yang diambil melalui alat ini bisa dilihat melalui GUI atau TTY mode TShark Utility.

1. Gambaran Sistem Saat Ini

Berikut ini adalah gambar sistem usulan yang dibuat.

Gambar Sistem Saat Ini



Deskripsi alur kerja

Berikut ini adalah alur kerja sistem yang dibuat :

1. BTS (*Base Transceiver Station*) memancarkan sinyal *broadcast* ditangkap sinyalnya menggunakan perangkat RTL-SDR yang sudah terhubung ke laptop.
2. Laptop yang sudah tersedia aplikasi Gr-GSM mendukung perangkat RTL-SDR saat penangkapan sinyal.
3. Setelah ditemukan sinyal yang berisikan data, akan ditampilkan paket data yang diterima menggunakan aplikasi *wireshark*.
4. Data dari frekuensi yang ditemukan akan disimpan menggunakan aplikasi Gr-GSM dalam format ".cfile".
5. Data yang sudah disimpan, dicari *burst frame* menggunakan aplikasi airprobe dan disimpan dalam format ".txt".
6. Pada file dengan format ".txt" berisikan *burst frame* dicari SDCCH *Trace* berupa bit yang terdapat pada GSM *Frame Number* untuk diproses mencari *key stream* nya menggunakan aplikasi GSM Framecoder.

Kebutuhan Perangkat Keras dan Perangkat Lunak

Berikut adalah spesifikasi sistem perangkat keras dan perangkat lunak yang dibutuhkan :

Perangkat Keras

Berikut ini adalah perangkat keras yang dibutuhkan :

1. RTL-SDR
   Chipset : R2832U
   Interface : USB 2.0 standard
   Recording Format : DVB TV-DVD (MPEG2),FM RADIO, DAB radio, WMA
   Range Frequency : 24 mhs – 1700 mhs.
   Fitur : Menangkap sinyal komunikasi dari BTS terdekat
2. Laptop
   OS : Linux Ubuntu 14.04 LTS
   Processor : Intel(R) Core(TM) i7
   Memory : 4 Gigabyte
   VGA : 2 Gigabyte
   Graphic Card : NVIDIA GeForce 840M
   Harddisk : 1 Terabyte
3. Sim Card Reader

Interface : High Speed USB 2.0
SD-Card Support : Yes (All Type), with SDHC Support
Mini SD Support : Yes (with SD Card Adapter)
Micro SD Support : Yes with No Adapter Required
Sim Card Reader Support : Yes with Free SIM Editor Software (Included)
OS Support : Windows 2000/XP/Vista, Mac OS X (9,0 or Later)

Perangkat Lunak

Berikut ini adalah perangkat lunak yang digunakan :

1. OS : Linux Ubuntu 14.04 LTS
2. RTL-SDR Driver : Driver RTL-SDR 2832U
3. UHD : Driver GNU Radio
4. Aplikasi SDR : GNU Radio, Gr-GSM
5. Aplikasi Decoding : Gr-GSM, Airprobe, GSM Framecoder

Implementasi

Implementasi bertujuan untuk menerapkan analisis dan perancangan yang telah dilakukan sehingga aplikasi dapat diinstalasi dan dikonfigurasi, aplikasi yang digunakan seperti : git, pybombs, gnuradio, uhd, gr-gsm, kalibrate, wireshark, dan library pendukung untuk aplikasi-aplikasi tersebut. Berikut langkah-langkah instalasi aplikasi yang digunakan :

1. Instalasi Git
```
# apt-get install git
```
2. Instalasi Pip
```
# apt-get install python-pip
```
3. Instalasi PyBOMBS
```
# git clone
https://github.com/pybombs/pybombs
```
4. Instalasi Gr-GSM
```
# pybombs install gr-gsm
```
5. Instalasi Kalibrate
```
# git clone https://github.com/steve-m/kalibrate-rtl
```
6. Instalasi GNU Radio
```
# pybombs install gnuradio
```
7. Instalasi Airprobe
```
# git clone https://github.com/iamckn/airprobe
```
8. Instalasi GSM Framecoder
```
# wget www.ks.uni-freiburg.de/download/misc/gsmframecoder.tar.gz
```
9. Instalasi Wireshark
```
# apt-get install wireshark
```

Pengujian yang dilakukan pada analisis adalah sebagai berikut :

Pengujian Kalibrasi Menggunakan Perangkat Keras RTL-SDR dan Aplikasi Kalibrate

Pada pengujian ini bertujuan untuk memindai pita BTS jaringan GSM terdekat dan untuk menghitung keseimbangan frekuensi osilator lokal. Berikut langkah pengujiannya :

1. Hubungkan perangkat RTL-SDR dengan laptop.
2. Jalankan perintah “kal” untuk memanggil program “-s” untuk stasiun GSM yang digunakan “-g” adalah kekuatan penangkapan sinyal.

```
root@brian-HP-Pavilion-14-Notebook-PC:~# kal -s GSM900 -g 50
Found 1 device(s):
  0:  Generic RTL2832U

Using device 0: Generic RTL2832U
Detached kernel driver
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
[R82XX] PLL not locked!
Setting gain: 50.0 dB
kal: Scanning for GSM-900 base stations.
GSM-900:
        chan: 50 (945.0MHz + 31.666kHz) power: 2474751.69
```

Pada gambar diatas, outputnya berupa alokasi operator telkomsel pada jaringan GSM. Dapat diketahui alokasi frekuensi awal pada operator telkomsel yaitu 945.0MHz

Pengujian Penangkapan Sinyal dan *Decoding* Pada Operator XL Dengan RTL-SDR, Gr-GSM, dan Wireshark

Metode menggunakan perangkat RTL-SDR, aplikasi Gr-GSM, dan aplikasi wireshark yang mengikuti alur *decoding live* aplikasi Gr-GSM yang secara langsung menangkap sinyal dari BTS (*Base Transceiver Station*), menyimpan file yang berformat “.cfile”, dan hingga

decode data komunikasi GSM menggunakan Gr-GSM. Berikut langkah-langkah pengujiannya :

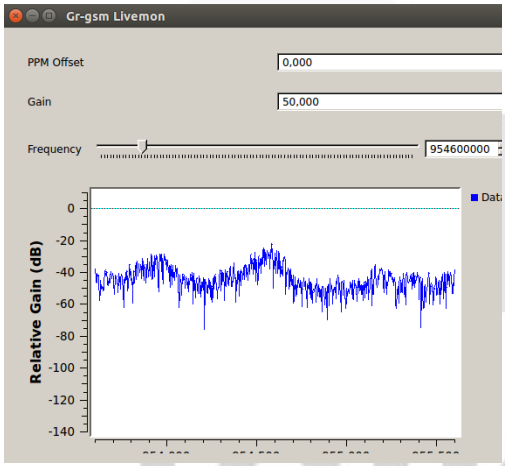
1. Menjalankan aplikasi Gr-GSM, aplikasi tersebut untuk menangkap sinyal GSM dari BTS, dengan mengetikkan perintah berikut pada terminal :

```
# grgsm_livemon
```

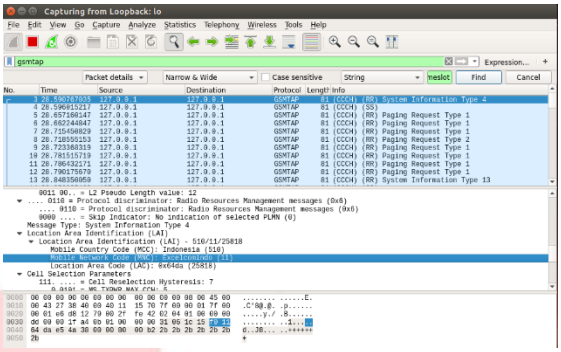
2. Menjalankan aplikasi wireshark karena aplikasi tersebut mendukung untuk analisis paket data yang ditangkap oleh aplikasi Gr-GSM, dengan mengetikkan perintah berikut pada terminal :

```
# wireshark
```

3. Akan muncul kotak dialog grgsm yang dapat mengatur *gain* atau kekuatan penangkapan sinyal di "50,000" dan menetapkan frekuensi "954600000"



4. Jika penangkapan berhasil dilakukan maka wireshark akan menampilkan data berupa paket yang isinya informasi dari frekuensi "954600000".



5. Menyimpan Data Komunikasi Pada Operator XL. Untuk menyimpan data dalam format ".cfile" dapat menggunakan perintah "grgsm_capture.py" pada terminal, perintah "-f 954600000" untuk target frekuensi, perintah "-s 1000000" untuk tingkat sampel penangkapan yang sudah tetap dari program dengan variabel "1000000", perintah "-g 50" untuk kekuatan penangkapan sinyal, perintah "-c sms2XL.cfile" data cfile yang akan disimpan, perintah "-T 60" untuk jarak waktu penangkapan sinyal.

```
root@brian-HP-Pavilion-14-Notebook-PC:~# grgsm_capture.py -f 954600000 -g 50 -s
1000000 -c smsXL.cfile -T 60
gr-osmosdr v0.1.4-98-gc653754d (0.1.5git) gnuradio 3.7.12git-196-g044b6c2b
built-in source types: file osmosdr fcd rtl rtl_tcp uhd hackrf bladerf rfspace a
trspy soapy redpitaya
[INFO] [UHDlinux; GNU C++ version 4.8.4; Boost_105400; UHD_3.11.0.git-233-g25fc3
2af]
Using device #0 Generic RTL2832U SN: 77771111153705700
Detached kernel driver
Found Rafael Micro R820T tuner
[R82XX] PLL not locked!
Exact sample rate is: 1000000.026491 Hz
[R82XX] PLL not locked!
Reattached kernel driver
```

6. Apabila proses penyimpanan sudah selesai, maka data akan tersimpan otomatis di direktori /root/

```
root@brian-HP-Pavilion-14-Notebook-PC:~# ls
airprobe                datacfile.cfile     multi-rtl       sms2XL.cfile
bursts2XL.txt           DATA_KONTRAKAN.cfile notplugged     sms.cfile
burstsDATA_KONTRAKAN.txt downlink.cfile     osmo-sim-auth   smsXL.cfile
burstsINDOSAT.txt       freq_9452.cfile     pcsc-spy        TELKOMSEL1.cfile
burstsTELKOMSEL3.txt    gr-gsm              plugged         TELKOMSEL3.cfile
burstsTELKOMSEL.txt     gsmframecoder       pybombs         tes.grc
bursts.txt              INDOSAT1.cfile      pyscard         top_block.py
-c                      kalibrate-rtl       pysim           usbswitch
```

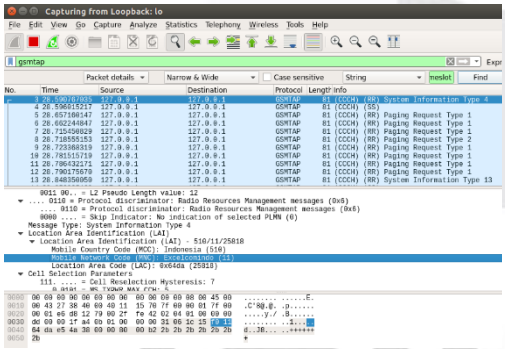
7. Menjalankan perintah "grgsm_decode" pada terminal untuk melakukan *decoding* pada data operator telkomsel yang sudah disimpan, disini melakukan *decoding* pada dua mode BCCH dan SDCCH8, BCCH yaitu mode saluran jaringan logikal yang digunakan BTS dalam GSM untuk mengirim informasi tentang identitas jaringan dimana informasi tersebut

digunakan oleh *mobile station* untuk mendapatkan akses ke jaringan, kemudian SDCCH8 untuk mode jaringan yang melakukan sub aliran jaringan untuk pensinyalan. Kemudian "-a" adalah nomor unik yang diberikan untuk setiap frekuensi GSM tidak berbeda dengan frekuensi sebenarnya, "-s" adalah *samplerate* dimana batas frekuensi yang dapat dikirim perdetiknya, "-t 0" untuk *decoding* pada mode BCCH yang dimaksudkan adalah *timeslot* atau saluran lalulintas.

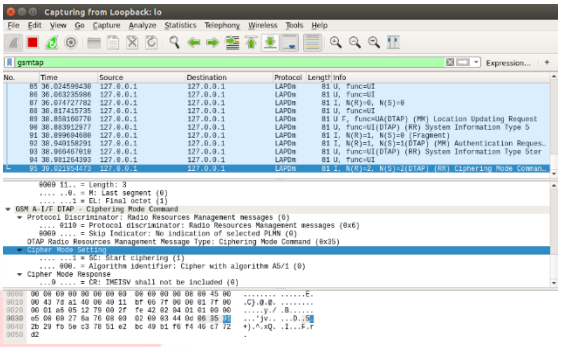
```
root@brian-HP-Pavilion-14-Notebook-PC:~# grgsm_decode -f 954600000 -s 16
 sms2XL.cfile -m BCCH -t 0
```

```
root@brian-HP-Pavilion-14-Notebook-PC:~# grgsm_decode -f 954600000 -s 10
 sms2XL.cfile -m SDCCH8 -t 1
```

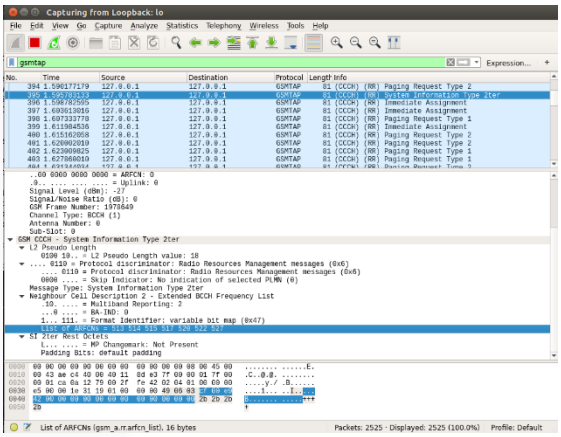
8. Menjalankan aplikasi wireshark untuk membaca informasi yang didapatkan dalam bentuk paket informasi. Salah satu informasi yang didapatkan saat menjalankan mode decoding BCCH adalah identitas yang didapatkan dari data.



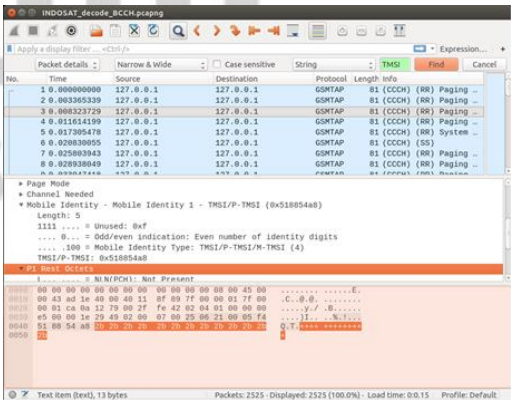
9. Pada saat mendecoding mode SDCCH8 banyak informasi yang didapatkan, seperti mode enkripsi keamanan jaringan GSM yang digunakan operator XL. Disini operator XL menggunakan keamanan jaringan A5/1.



10. Pada decoding mode BCCH juga didapatkan informasi ARFCN (*Absolute Radio Frequency Channel Number*) frekuensi yang digunakan operator XL.

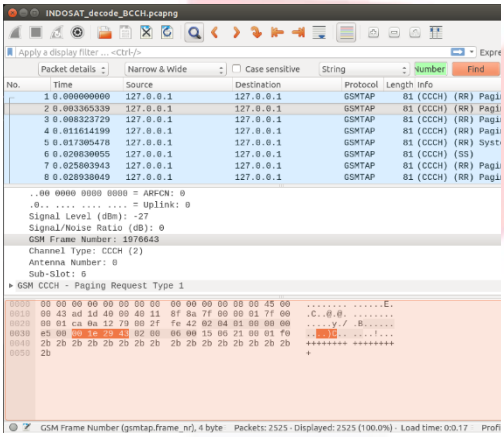


11. Pada mode decoding BCCH didapatkan juga informasi, didapatkan TMSI yang berbeda karena penangkapan yang dilakukan secara *broadcast* atau pengiriman data ke banyak jaringan dan juga digenerate secara periodik setiap sesi, berikut TMSI pada operator jaringan XL



.

12. Dari mode decoding BCCH didapatkan juga informasi, GSM *Frame Number* yang berbeda karena penangkapan yang dilakukan secara *broadcast* atau pengiriman data ke banyak jaringan, berikut GSM Frame number pada operator jaringan XL.



Pengujian Mencari *Bursts Frame* Dari Data Komunikasi Operator Jaringan XL Menggunakan Airprobe

Burst Frame adalah sebuah data berupa sekumpulan bit yang berisikan informasi yang nantinya akan di dekripsi oleh aplikasi kraken, data yang didekripsi adalah KC (*key chipering*).

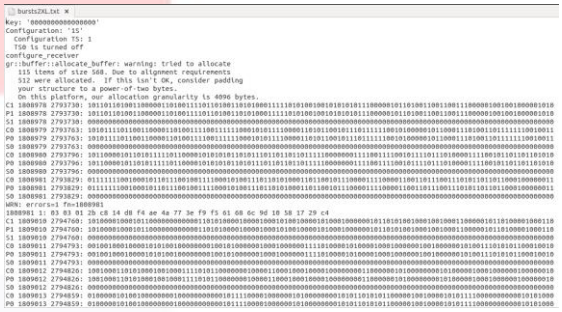
1. Masuk ke direktori "/airprobe/gsm-receiver/src/python" dan jalankan perintah "./go.sh" kemudian tambahkan perintah "/root/sms2XL.cfile 64 1S" yang dimaksud sumber lokasi data telkomsel yang sudah ditangkap, 64 adalah tingkat tujuan GSM dan 1S adalah *timeslot* kemudian ditambah perintah "&>" adalah tujuan penyimpanan lokasi data burst.

```
root@brian-HP-Pavilion-14-Notebook-PC:~/airprobe/gsm-receiver/src/python#
h /root/sms2XL.cfile 64 1S &> /root/bursts2XL.txt
```

2. Selah berhasil maka akan muncul pada direktori root.

```
root@brian-HP-Pavilion-14-Notebook-PC:~# ls
airprobe                datacfile.cfile       multi-rtl       sms2XL.cfile
bursts2XL.txt           DATA_KONTRAKAN.cfile  notplugged      sms.cfile
burstsDATA_KONTRAKAN.txt downlink.cfile       osmo-sim-auth   smsXL.cfile
burstsINDOSAT.txt       freq_9452.cfile       pcsc-spy        TELKOMSEL1.cfile
burstsTELKOMSEL3.txt    gr-gsm                plugged         TELKOMSEL3.cfile
burstsTELKOMSEL.txt     gsmframecoder         pybombs         tes.grc
bursts.txt              INDOSAT1.cfile        pyscard         top_block.py
-c                      kalibrate-rtl         pysim           usbswitch
```

3. Kemudian membuka isi data burst menggunakan perintah "gedit bursts2XL.txt" pada terminal.



Data burst berhasil ditemukan, dan akan dilanjutkan ke proses dekripsi data oleh program kraken untuk mendapatkan KC(*key chipering*) pada data komunikasi GSM.

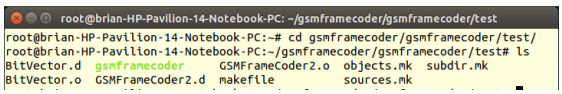
Pengujian Menggunakan GSM Framecoder Pada Bursts File XL

GSM Framecoder digunakan untuk menghitung *bursts* yang dihasilkan pada paket GSM untuk dapat di *decoding* datanya. Pada pengujian ini akan memproses file *bursts* operator XL yang telah didapatkan sebelumnya menggunakan aplikasi Airprobe.

1. Berikut tampilan file yang akan diproses pada direktori root. File tersebut bernama "bursts2XL.txt".

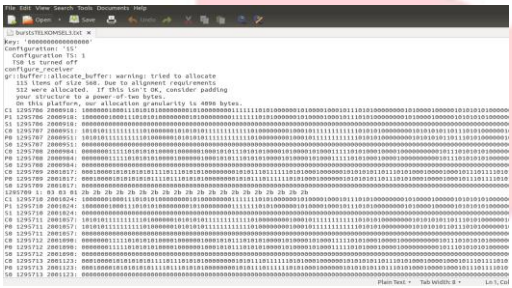
```
root@brian-HP-Pavilion-14-Notebook-PC:~# ls
airprobe                datacfile.cfile       multi-rtl       sms2XL.cfile
bursts2XL.txt           DATA_KONTRAKAN.cfile  notplugged      sms.cfile
burstsDATA_KONTRAKAN.txt downlink.cfile       osmo-sim-auth   smsXL.cfile
burstsINDOSAT.txt       freq_9452.cfile       pcsc-spy        TELKOMSEL1.cfile
burstsTELKOMSEL3.txt    gr-gsm                plugged         TELKOMSEL3.cfile
burstsTELKOMSEL.txt     gsmframecoder         pybombs         tes.grc
bursts.txt              INDOSAT1.cfile        pyscard         top_block.py
-c                      kalibrate-rtl         pysim           usbswitch
```

2. Masuk ke direktori "gsmframecoder/gsmframecoder/test" menggunakan perintah berikut



Pada gambar diatas dapat terlihat perintah "gsmframecoder" berwarna hijau untuk menjalankan proses menghitung *bursts* pada file.

3. Buka file burst dan melihat burst code yang akan diproses



4. Proses kode burst menggunakan perintah berikut

```
root@brian-HP-Pavilion-14-Notebook-PC:~/gsmframecoder/gsmframecoder/test# ./gsmframecoder 03 03 01 2b c0 14 d8 f4 ae 4a 77 3e f9 f5
10 58 17 29 c4
Decoding 03030128bc814d8f4ae4a773ef9f5616886c9d10581729c4
Encoded Frame, Burst1:
10110110011000601101001111011010011010100011111010011010101011100001011101100111000010010010000001010
Encoded Frame, Burst2:
10101111011001100001101001111000111110001010111100001101011001111111101010000001001000111010011011111110010000011
Encoded Frame, Burst3:
10110000101101011111101100001010101011010111011011111000000011110011110111011110100001111100101101101101010
Encoded Frame, Burst4:
01111111001000101011100100111000101001110101000110110101100001111000011001101110011101110110110110100000000011
```

```
root@brian-HP-Pavilion-14-Notebook-PC:~/gsmframecoder/gsmframecoder/test# ./gsmframecoder 05 01 03 03 49 06 06 cf 00 7f ff c0 00 00
00 00 00 00 00
Decoding 05010303490606cf007fffc000000000000000000000
Encoded Frame, Burst1:
10100010001011000000000001101010000100010101001010001000000101101010010010000000100110
Encoded Frame, Burst2:
00101000100001010100100000000100101000001000100000111101000101000010001000000101001110101011000010
Encoded Frame, Burst3:
10010001101010001001000111101011000000100011000100010000000110000001010000010001000000100000010
Encoded Frame, Burst4:
01000001010010000000010000000000101111000010000001010000000101010101100000100100010101111000000000010101000
```

```
root@brian-HP-Pavilion-14-Notebook-PC:~/gsmframecoder/gsmframecoder/test# ./gsmframecoder 05 03 03 03 49 06 1d 00 00 00 00 00 00 00
00 00 00 00 00
Decoding 0503030349061d000000000000002114000000000
Encoded Frame, Burst1:
10100001100110100000011000100101001100000100001011100100000100010000000010000100100101010000100110
Encoded Frame, Burst2:
00000011010000101001110000100110000100000111000000000011001010100001000010110000010000011101001010000110010000
Encoded Frame, Burst3:
00010001001011110010100000010000101000001010101100010100000100000011010000000010000001000001100010
Encoded Frame, Burst4:
00000000100110010100001010000100100100000000001010000000101001010000110001000100011101101000000110000001100
```

Pada gambar diatas telah didapatkan *bursts frame* yang berbeda, dan akan diproses satu per satu menggunakan aplikasi kraken untuk mendapatkan KC (Kunci Chiper) dari file tersebut.

Berdasarkan implementasi dan pengujian yang dilakukan dapat disimpulkan :

1. Penangkapan sinyal GSM dari BTS (*Base Transceiver Station*) dapat dilakukan menggunakan perangkat keras RTL-SDR.
2. Aplikasi Gr-GSM memiliki fitur yang dapat membantu proses penangkapan sinyal GSM.
3. *Decoding* data komunikasi GSM yang dilakukan dengan aplikasi Gr-GSM, Airprobe, dan GSM Frame Coder hanya mendapatkan data keamanan pada jaringan GSM.

Jaringan komunikasi GSM memiliki sistem keamanan yang cukup rumit karena harus melakukan 4 tahapan *decoding* hingga mendapatkan data keamanan pada jaringan tersebut. Dalam proyek akhir ini hanya dapat menganalisis sistem keamanan jaringan GSM tidak sampai proses *decoding* sms dan telepon karena pada sistem keamanannya memiliki frekuensi ARFCN (*Absolute Radio Frequency Channel Number*) yang tiap periode berubah jadi analisis tidak bisa fokus pada satu data *subscriber*. Mungkin untuk kedepannya dapat berhasil melakukan *decoding* komunikasi GSM hingga mendapatkan sms dan telepon secara *live* yang dilakukan antara telepon pengguna.

[1] G. L. Indonesia, "Ubuntu 14.04 LTS," Gudang Linux Indonesia, 2013. [Online]. Available: http://gudanglinux.com/produk/ubuntu-14-04-lts/. [Accessed 2 March 2017].

[2] Wikipedia, "GSM (Global System for Mobile Communication)," Wikipedia, 30 Oktober 2016. [Online]. Available: https://id.wikipedia.org/wiki/Global_System_for_Mobile_Communications. [Accessed 20 Januari 2017].

[3] J. Stender, Aplikasi Platform Komputasi Software-Defined Radio (SDR) untuk Digital Spectrum Analizer, Malang, 2014.

[4] L. H. N. E. Lilik Hardianti, "ENCODING DAN DECODING KODE HAMMING SEBAGAI KODE TAK SIKLIK DAN SEBAGAI KODE SIKLIK," pp. 1-12, 2015.

[5] GNURadio, "PyBOMBS," Redmine, 2013. [Online]. Available: http://gnuradio.org/redmine/projects/pybombs/wiki. [Accessed 02 March 2017].

[6] RTL-SDR, "HOW TO CALIBRATE RTL-SDR USING KALIBRATE-RTL ON LINUX," RTL-SDR, 5 June 2013. [Online]. Available: http://www.rtl-sdr.com/how-to-calibrate-rtl-sdr-using-kalibrate-rtl-on-linux/. [Accessed 5 March 2017].

[7] R. Primartha, "Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption (DES)," *Jurnal Sistem Informasi,* vol. III, p. Okrober, 2011.

[8] G. Radio, "Introduction to GNU Radio and Software Radio," gnuradio, 2006-2013. [Online]. Available: http://gnuradio.org/redmine/projects/gnuradio/wiki/Guided_Tutorial_Introduction. [Accessed 13 Maret 2017].

[9] M. F. R. D. R. S. Diki Nugraha, "IMPLEMENTASI GNURADIO GSM (gr-gsm) untuk decoding sinyal GSM".

[10] Wikipedia, "pip (package manager)," Wikipedia, 11 July 2017. [Online]. Available: https://en.wikipedia.org/wiki/Pip_(package_manager). [Accessed 16 July 2017].

[11] P. Krysik, "Gr-GSM," Github, 18 August 2015. [Online]. Available: https://github.com/ptrkrysik/gr-gsm/wiki. [Accessed 19 July 2017].

[12] RTL-SDR, "SNIFFING AND ANALYZING GSM SIGNALS WITH GR-GSM," RTL-SDR, 1 December 2014. [Online]. Available: http://www.rtl-sdr.com/tag/airprobe/. [Accessed 23 July 2017].

[13] K. Meier, "[A51] gsmframecoder to calculate bursts," Srlabs.de, 23 February 2011. [Online]. Available: https://lists.srlabs.de/pipermail/a51/2011-February/001067.html. [Accessed 23 July 2017].

[14] GNU and G. , "GCC 6 Release," Wikipedia, 4 July 2017. [Online]. Available: https://gcc.gnu.org/gcc-6/. [Accessed 27 07 2017].

[15] Osmocom, "osmo-sim-auth," Osmocom, 2 February 2016. [Online]. Available: https://osmocom.org/projects/osmo-sim-auth/wiki. [Accessed 27 July 2017].

[16] Wikipedia, "PCSC," Wikipedia, 22 January 2017. [Online]. Available: https://id.wikipedia.org/wiki/PCSC. [Accessed 27 July 2017].

[17] Wikipedia, "SWIG," SWIG Developer, 9 June 2017. [Online]. Available: https://en.wikipedia.org/wiki/SWIG. [Accessed 27 July 2017].

[18] J.-D. Aussel, "pyscard user guide," pyscard, 2001-2009. [Online]. Available: https://pyscard.sourceforge.io/user-guide.html. [Accessed 27 July 2017].

[19] A. Parmar and K. M. Pattani, "Sniffing GSM Traffic Using RTL-SDR And Kali Linux OS," *Sniffing GSM Traffic Using RTL-SDR And Kali Linux OS,* vol. IV, no. 01, pp. 1637-1642, 2017.

Telkom
University