Sniffing Sinyal GSM dengan RTL-SDR, GNU Radio dan Wireshark

Yuli Apriyanti[1], Dr. Tutun Juhana, ST, MT[2], Eki Ahmad Zaki Hamidi, MT[3]
[1,3] Teknik Elektro Fakultas Sains dan Teknologi UIN Sunan Gunung Djati Bandung
Jl. A.H. Nasution No. 105, Kota Bandung, Jawa Barat 40614
[2] Teknik Telekomunikasi Institut Teknologi Bandung
Jl. Ganesha No.10, Kota Bandung, Jawa Barat 40132
[1] yuliapriyanti27@gmail.com, [2] tutun.j@gmail.com, [3] ekiahmadzaki@uinsgd.ac.id

Abstrak – *Sebagai Negara yang terus berkembang Indonesia merupakan salah satu Negara dengan tingkat traffic komunikasi yang cukup besar, dengan jaringan sinyal GSM sebagai jaringan utama yang digunakan user untuk berkomunikasi satu user dengan yang lainnya. dalam jaringan GSM terjadi Pertukaran berbagai informasi, baik itu informasi yang bersifat umum hingga yang bersifat personal .Pada penelitian ini dilakukan percobaan sniffing sinyal GSM sehingga koordinat lokasi pengguna dapat diketahui. Sebelum dilakukan proses sniffing, terlebih dahulu melakukan scanning sinyal GSM menggunakan Gqrx untuk melihat range frekuensi sinyal GSM yang ada disekitar area pengamatan. Pada umumnya sinyal GSM berada pada range frekuensi 900 MHz. Proses sniffing pada system dilakukan dengan memanfaatkan RTL-SDR sebagai receiver sinyal GSM dan GNU Radio sebagai decoder sinyal GSM dan diteruskan oleh Wireshark sebagai analisator dari sinyal GSM dengan menggunakan filter GSM_TAP sehingga didapatkan informasi yang berupa Local Area Identification dan Cell Identify yang dapat digunakan untuk menemukan koordinat lokasi pengguna dengan memanfaatkan bantuan dari program phone tracker.*

Kata kunci*: GNU Radio, GSM, Phone Tracker, RTL-SDR dan Wireshark*

1. Pendahuluan

Adanya pengembangan ilmu pengetahuan dan teknologi membuat banyak sekali penemuan terbarukan contohnya dengan ditemukannya teknologi *Global System for Mobile Communication* disingkat GSM, yaitu sebuah teknologi komunikasi selular yang bersifat digital. Teknologi GSM banyak diterapkan pada komunikasi bergerak, khususnya telepon genggam. GSM dijadikan standar global untuk komunikasi selular sekaligus sebagai teknologi selular yang paling banyak digunakan orang di seluruh dunia. Dengan ditemukannya teknologi GSM semakin membuka jalan penemuan-penemuan lain dalam bidang telekomunikasi.

Saat ini teknologi GSM tidak bisa lepas dari kehidupan sehari-hari, Banyaknya pengguan telepon seluler akan terus bertambah setiap tahunnya dan demikian pula dengan pengguna jaringan GSM akan bertambah seiring bertambahnya pengguna telepon genggam. pada tahun 2013 pengguna telepon genggam mencapai 313.226.914 pengguna [1].

Dengan menggunakan RTL-SDR sebagai receiver sinyal GSM maka sinyal dapat di-*Sniffing* menggunakan bantuan GNU Radio dan Wireshark. Sinyal GSM yang ter-*Sniffing* akan menunjukan koordinat lokasi dimana pengguna berada .

Proses *sniffing* sinyal GSM dengan menggunakan RTL-SDR sebagai *Receiver* sinyal, lalu sinyal yang diterima oleh RTL-SDR di*scanning* menggunakan Gqrx untuk menentukan range frekuensi di sekitar area pengamatan. Sinyal GSM yang ter-*sniffing* akan didecoding oleh GNU Radio yang akan menghasilkan kode-kode ASCII lalu kode-kode ASCII tersebut akan dianalisis

oleh wireshark sehingga akan menghasilkan data yang akan digunakan untuk menentukan koordinat lokasi pengguna GSM dan dapat diketahui dengan program phone tracker.

2. Dasar Teori

2.1. *Global system for Mobile* (GSM)

GSM (*Global system for Mobile*) adalah generasi kedua dari standar sistem selular. Sistem selular yang tengah dikembangkan untuk mengatasi problem fragmentasi yang terjadi pada standar pertama di negara Eropa.Teknologi GSM menggunakan sistem TDMA dengan alokasi kurang lebih sekitar delapan pengguna di dalam satu *channel* frekuensi sebesar 200 kHz per satuan waktu. Awalnya, frekuensi yang digunakan adalah 900 MHz.

Pada perkembangannya frekuensi yang digunakan adalah 1800 MHz dan 1900 MHz. Kelebihan dari GSM adalah *interface* yang lebih bagi para *provider* maupun para penggunanya. Selain itu, kemampuan *roaming* antar sesama *provider* membuat pengguna dapat bebas berkomunikasi [2].

2.2. RTL-SDR

RTL-SDR adalah *Software Defined Radio* yang paling murah dan menggunakan DVD-T TV Tuner Dongle berbasis chipset RTL2832U yang dapat menghasilkan sinyal data I/Q bisa diakses secara langsung, yang memungkinkan DVB-T TV untuk dikonversi ke *Wideband Software Defined Radio* melalui *driver software* baru. RTL-SDR dapat digunakan untuk Scanner radio pita lebar, Mendengarkan percakapan yang tidak terenskripsi yaitu polisi / ambulance / pemadam kebakaran dan Menerima citra satelit cuaca NOAA dan Mendengarkan satelit dan ISS [3].

2.3. GNU Radio

GNU Radio adalah sebuah perangkat lunak gratis dan *open source* yang menyediakan teknik pemprosesan sinyal untuk mengimplementasikan [software radio]. Aplikasi GNU Radio sebagian besar ditulis menggunakan bahasa pemprograman Python, sedangkan bagian pemprosesan sinyal diimplementasikan dalam bahasa pemprograman C++ menggunakan prosesor ekstensi floating-point. GNU Radio mendukung pengembangan algoritma pemrosesan sinyal menggunakan pra-pemprosesan atau pasca-pemprosesan untuk menghindari kebutuhan untuk memiliki perangkat keras radio frekuensi yang sebenarnya. Antarmuka pengguna grafis untuk mengembangkan aplikasi GNU Radio adalah GNU Radio Companion (GRC) [4].

2.4. Wireshark

Wireshark merupakan salah satu tools atau aplikasi "*Network Analyzer*" atau Penganalisa Jaringan. Penganalisaan Kinerja Jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan, sampai pada digunakan pula untuk *Sniffing* (memperoleh informasi penting seperti password email, dan lain-lain). Selain itu wireshark juga digunakan untuk Membaca data secara langsung dari Ethernet, Token-Ring, FDDI, serial (PPP dan SLIP), 802.11 wireless LAN, dan koneksi ATM, Dapat mengetahui IP seseorang melalui typingan room, Menganalisa transmisi paket data dalam jaringan, proses koneksi, dan transmisi data antar computer [5].

3. Hasil Dan Analisis

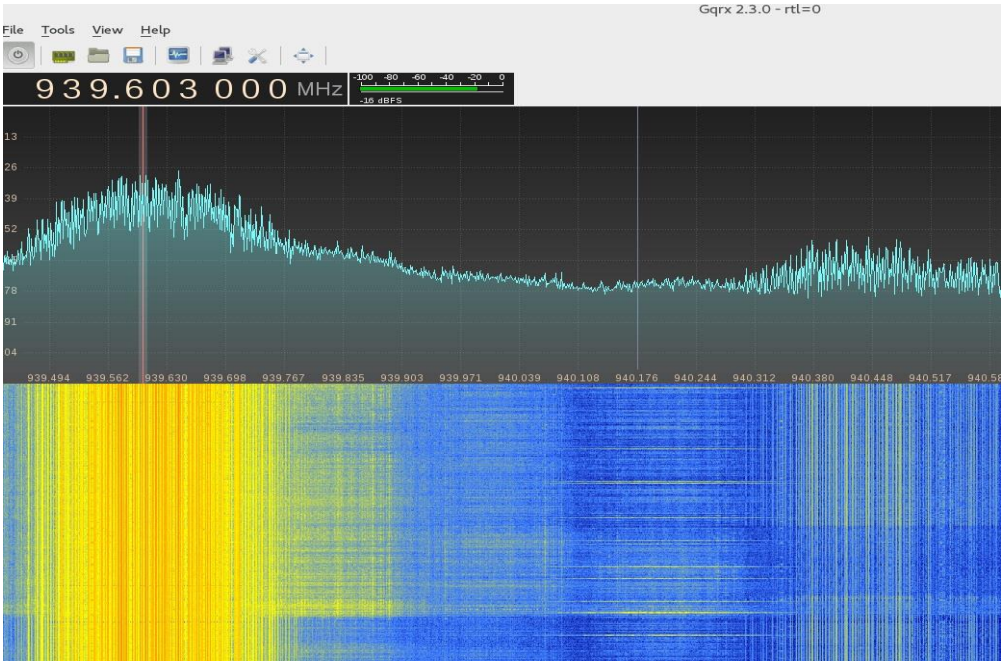
3.1. Proses Scanning Sinyal GSM

Semua percobaan proses *sniffing* sinyal GSM dilakukan pada PC dengan kali linux sebagai operation system. Karena kali linux khusus untuk *penetration testing* dan audit keamanan dengan Lebih dari 300 *tools penetration testing* sehingga untuk melakukan *sniffing* akan lebih mudah.[6]

Sebelum melakukan proses *sniffing*, hal yang harus dilakukan adalah menentukan berapa frekuensi yang digunakan sinyal GSM pada area pengamatan. Pada umumnya frekuensi yang digunakan untuk sinyal GSM adalah 900 MHz dan contohnya pada USA frekuensi sinyal GSM dimulai dari 850 MHz. Namun untuk mengetahui frekuensi sinyal GSM yang berada di sekitar area pengamatan maka dilakukan scanning sinyal GSM menggunakan Gqrx sebagai penerima *Software Defined Radio* (SDR).

ISBN: 978-602-60581-0-2

Tidak hanya menggunakan Gqrx *scanning* sinyal juga dapat dilakukan oleh program-program lain seperti SDRSharp dan Spectrum spy.



Gambar 1. Hasil *Scanning* Sinyal GSM

Berdasarkan gambar 1 yang merupakan hasil dari *scanning* sinyal GSM menggunakan Gqrx menunjukan bahwa sinyal GSM di sekitar area pengamatan terdapat pada range frekuensi 939,6 MHz.

3.2. *Sniffing* Sinyal GSM

Sniffing Sinyal GSM dilakukan dengan cara melakukan decoding sinyal GSM melalui GNU Radio dan analisis jaringan oleh wireshark. Pada GNU Radio untuk melakukan decoder sinyal GSM diperlukan gr-gsm yang khusus meng-decoder sinyal GSM. Dikarenkan gr-gsm tidak terinstall langsung dengan paket GNU Radio maka harus diinstall secara terpisah.

Berikut adalah langkah-langkah menginstall gr-gsm secara manual pada PC namun untuk menginstall gr-gsm perlu juga menginstall program/*libraries* dari *distibution's repository,*untuk installasi dapat dilihat pada tabel 1 [7].

Tabel 1. Installasi *libraries* gr-gsm

No	Project	Packages
1	RTL-SDR	Apt-get install rtl-sdr librtlsdr-dev
2	grosmosdr	Apt-get install osmo-sdr libosmosdr-dev
3	libosmocore	Apt-get install libosmocore libosmocore-dev

Setelah program/*libraries* yang digunakan/berkaitan dengan gr-gsm terinstall maka selanjutnya adalah menginstall gr-gsm.

Untuk download sources gr-gsm :

- git clone https://github.com.ptrkrysik/gr-gsm.git

Kemudian install semua paket libraries yang diperlukan untuk gr-gsm

ISBN: 978-602-60581-0-2

▪ apt-get install cmake libboost-all-dev libcppunit-dev swig \ doxygen liblog4cpp5-dev pyhton-scipy

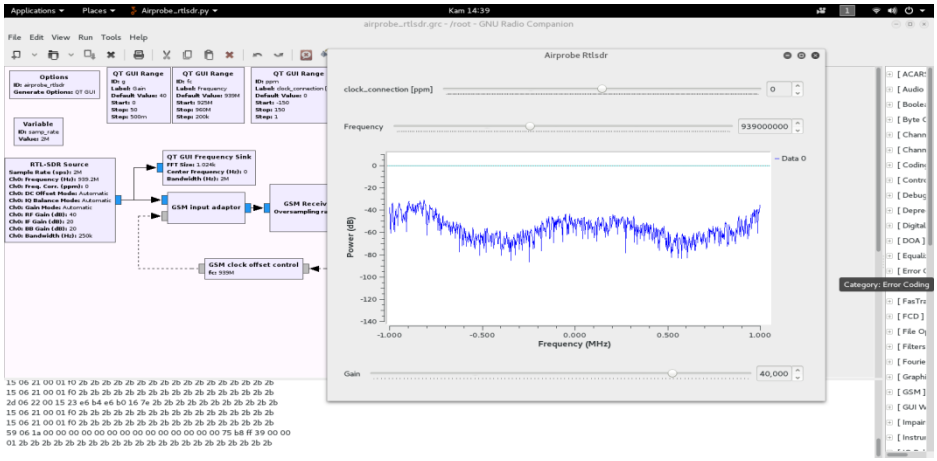
Untuk *Compile* dan Install gr-gsm gunakan perintah

```
cd gr-gsm
mkdir build
cd build
cmake . .
make
make install
```

Gambar 2. Installasi gr-gsm

Dan terakhir buat *config file* ~/.gnuradio/config.conf sehingga gnuradio companion dapat menemukan *custom blocks* untuk gr-gsm [7].

Pengembang gr-gsm yaitu Piotr Krysik, memberikan file untuk pengujian sinyal GSM. Sehingga uji coba *sniffing* sinyal GSM dapat lebih mudah dilakukan yaitu dengan hanya running file airprobe_rtlsdr.grc yang tersimpan pada dokumen gr-gsm. Pada program sudah disetting untuk sinyal GSM yang akan didecoding berada pada frekuensi dengan range mulai dari 939 MHz, sesuai dengan hasil *scanning* yang telah dilakukan menggunakan Gqrx



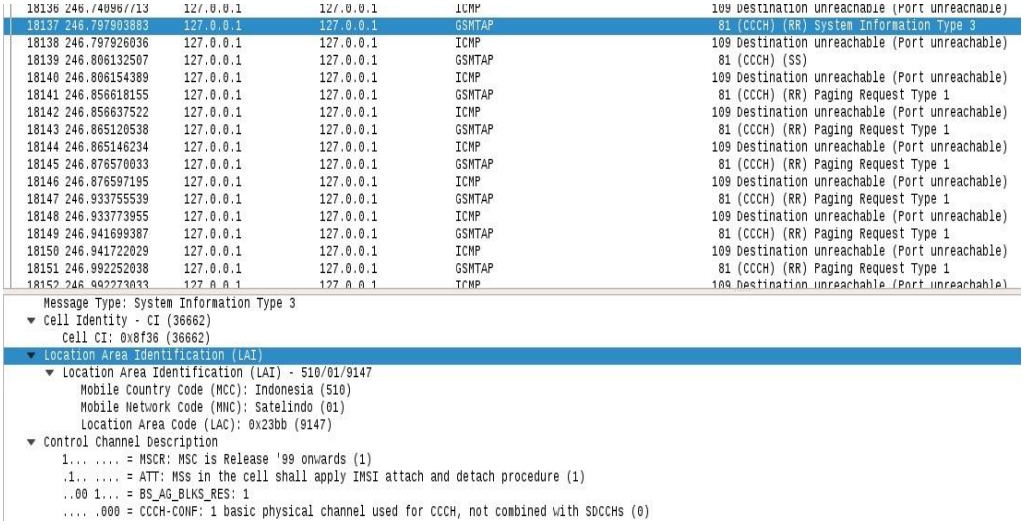
Gambar 3. Decoding sinyal GSM

Pada gambar 3. terlihat grafik sinyal dengan range frekuensi yang telah ditentukan yaitu 939 MHz dan membuktikan bahwa memang ada sinyal GSM pada range frekuensi tersebut dan terlihat bahwa sinyal didecoding sehingga menampilkan kode-kode ASCII yang berisi informasi hasil dari decoding sinyal GSM yang ter-*snifiing*.

Gambar 4. Caputre loopback:lo

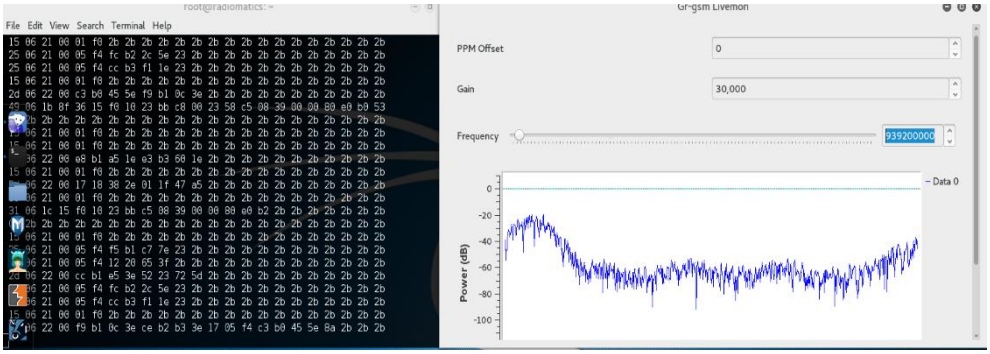
ISBN: 978-602-60581-0-2

Sinyal telah didecoding maka selanjutnya yaitu melakukan analisis sinyal GSM dengan wireshark. Menggunakan capture loopback:lo dan dengan filter gsmtap && !lcmp .



Gambar 5. Data LAI dan Cell Identify

Proses analisis sinyal akan menampilkan data-data dan variable-variabel hasil decoding oleh GNU Radio yang merupakan kode-kode ASCII. Kode-kode ASCII yang didecoding oleh GNU Radio kemudian ditampilkan oleh wireshark dengan berupa bilangan biner, hexa dan glyph sehingga lebih mudah dipahami.



Gambar 6. Sinyal yang didecoding

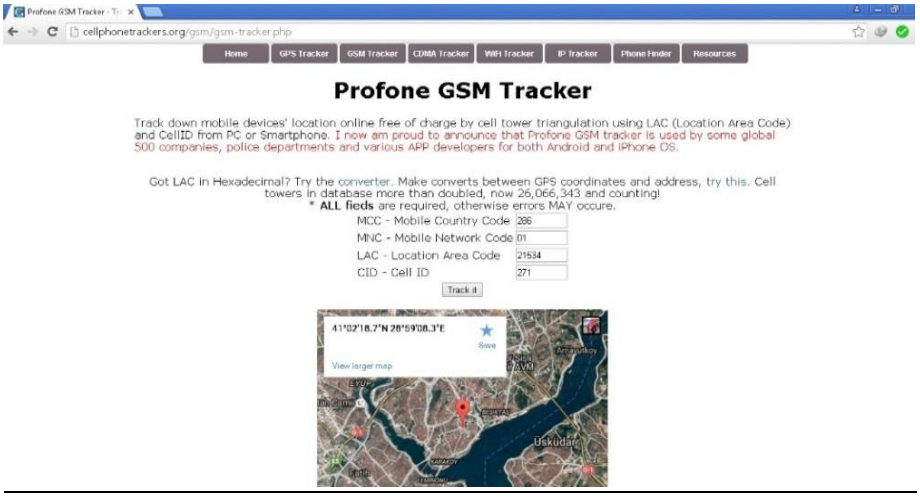
Dari begitu banyaknya data yang ditampilkan oleh wireshark, ada data yang merupakan tujuan dari *sniffing* sinyal GSM ini yaitu lokasi pengguna GSM yang ter-*sniffing*. Data dapat ditemukan di setiap info yang berjudul "*system information type 3*", dikarenakan selama sinyal GSM terus didecoding seperti gambar 3.6 maka semakin banyak data hasil analisis yang ditampilkan oleh wirehsark.

Data hasil dari pengujian *sniffing* sinyal GSM dengan RTL-SDR, GNU Radio dan wireshark yang didapat yaitu data *Location Area Identification* (LAI) dan *Cell Identity* pengguna gsm yang ter-*sniffing*. *Local Area Identification* terdiri dari *Mobile Country Code* (MCC), *Mobile Network Code* (MNC) , *Location Area Code* dan *Cell Identity***.**

3.3. Pengujian Data Hasil Analisis Menggunakan Aplikasi Phone Tracker

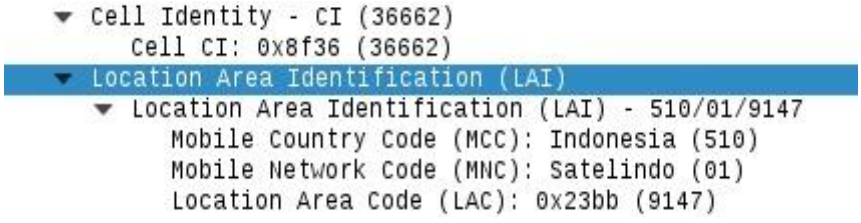
Berdasarkan data *Local Area Identification* dan *Cell Identify* yang didapatkan oleh wireshark maka posisi atau koordinat lokasi pengguna GSM yang sinyalnya ter-*sniffing* dapat ditemukan dengan bantuan program Phone Tracker.

ISBN: 978-602-60581-0-2



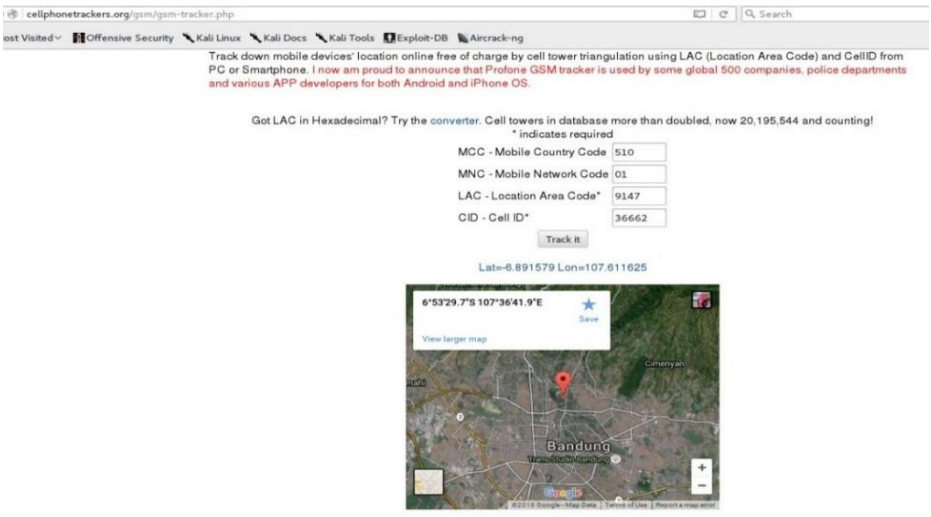
Gambar 7. Tampilan program phone tracker

Program Phone Tracker dapat diakses dari situs http://cellphonetrackers.org/gsm/gsm-tracker.php



Gambar 8. *Local Area Identification* dan *cell identify*

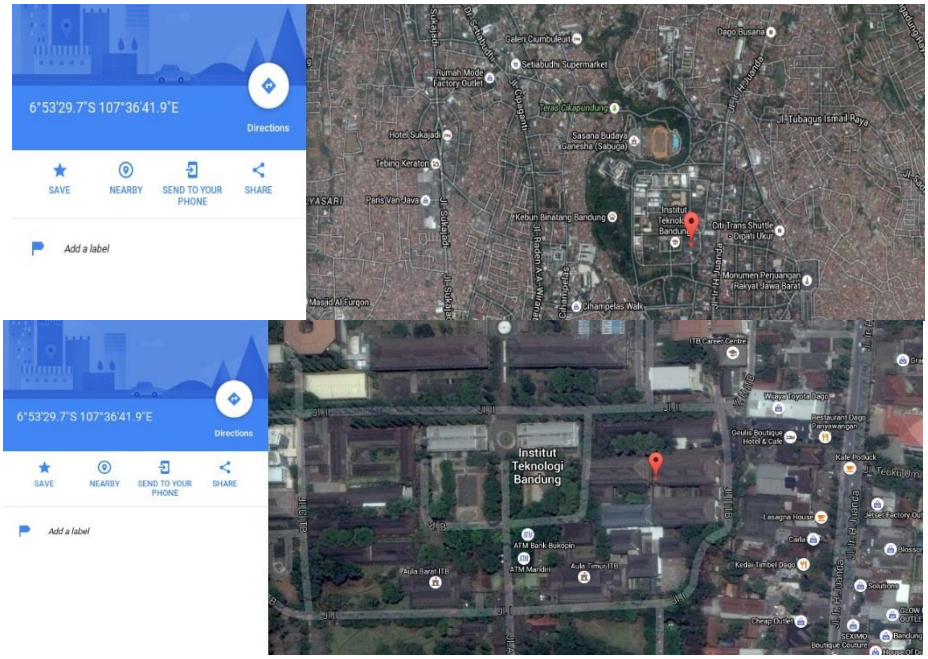
Untuk mendapatkan koordinat lokasi, maka harus mengetahui data yang dibutuhkan yaitu, MCC, MNC, LAC dan CID. Untuk MCC (*Mobile Country Code*) Kode negara untuk operator seluler di Indonesia adalah 510 dan MNC (*Mobile Network Code*) Kode operator telekomunikasi. misalnya Indosat 01, XL 11 dan sebagainya. Untuk MNC dan MCC bisa ditemukan dengan mudah di internet dengan pencarian pada Wikipedia Daftar MNC dan MCC Indonesia.



Gambar 9. Koordinat lokasi pengguna GSM

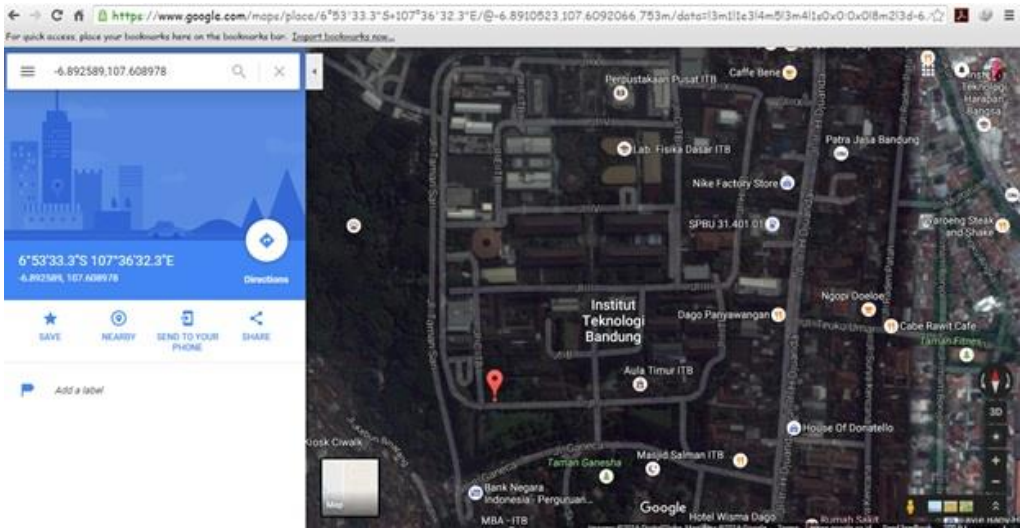
ISBN: 978-602-60581-0-2

Dapat dilihat pada gambar 9 Bahwa koordinat lokasi dari pengguna GSM yang ter-*sniffing* berada di Bandung, Jawa Barat. Dan apabila dilihat dengan *large map* maka lokasinya akan lebih jelas lagi.



Gambar 10. Lokasi pengguna GSM ter-*sniffing*

Gambar 3.10 lokasi pengguna yang ter-*sniffing* jika dilihat dari Google Maps berada pada gedung Labtek VIII Sekolah Tinggi Elektro dan Informatika Institut Teknologi Bandung, Jawa Barat.



Gambar 11. Lokasi terbaru pengguna GSM ter-*sniffing*

Namun saat dilakukan pelacakan koordinat pengguna GSM tersebut pada tanggal 12 agustus 2016 pada jam 16.30 wib , dengan memasukan data MCC, MNC , LAC dan Cell identify yang sama dengan data hasil analisis wireshrak, lokasi pengguna berpindah namun

ISBN: 978-602-60581-0-2

masih di sekitar lokasi yang sama dengan lokasi sebelumnya.

4. Kesimpulan dan Saran

4.1. Kesimpulan

Berdasarkan dari hasil percobaan dan analisis sinyal GSM ter-*sniffing*, maka dapat ditarik kesimpulan bahwa :

- Data yang dihasilkan dalam proses *sniffing* sinyal GSM yaitu berupa *Local Area Identification*. Data-data tersebut yang dapat menunjukan koordinat lokasi pengguna GSM yang ter-*sniffing* dengan bantuan program Phone Tracker.
- Percobaan *sniffing* sinyal GSM yang dilakukan berberapa kali hanya mendapatkan satu pengguna GSM yang ter-*sniffing* dan dengan koordinat lokasi yang sama.
- Pada pelacakan ulang koordinat lokasi pengguna GSM ter-*sniffing* dengan menggunakan *Local Area Identification* yang didapatkan dalam proses *sniffing* dilaboratorium, pengguna GSM ter-*sniffing* berpindah tempat namun masih disekitar lokasi sebelumnya yaitu masih di sekitar kampus ITB.

4.2. Saran

Berdasarkan percobaan yang telah dilakukan, tentunya masih ada beberapa hal yang perlu ditingkatkan dan dijadikan acuan pengembangan dan penyempurnaan dari proses *sniffing* sinyal GSM ini agar lebih baik lagi, seperti :

- *Sniffing* pengguna GSM diarea yang lebih luas, tidak hanya didalam satu ruangan, agar mendapatkan lebih banyak pengguna GSM yang ter-*sniffing*.
- Analisis jaringan yang lebih kompleks, sehingga tidak hanya lokasi pengguna GSM yang ter-*sniffing* yang diketahui namun bisa dilakukan *sniffing* percakapan terenskripsi.

Daftar Pustaka

[1] Badan Pusat Statistik.(2015). Jumlah Pelanggan Telepon Menurut Jenis Penyelenggaraan Jaringan 2010-2013. https://www.bps.go.id/linkTabelStatis/view/id/1844
[2] T, Fahkrudin. (2011). *GSM (GLOBAL SYSTEM FOR MOBILE)*. Medan : Universitas Sumatera Utara.
[3] _____. RTL-SDR. http://www.rtl-sdr.com/about-rtl-sdr/.
[4] _____. GNU Radio. http://gnuradio.org/about/.
[5] Orebaugh, Angela, Gilbert Ramirez, Jay Beale. (2007). *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Canada: Syngress publishing, inc.
[6] Oktavian, Fachrizal. 2015. *Kali Linux: 300% Attack*. Jakarta : Jasakom.
[7] Krysik, Piotr. Manual compilation and installation. https://github.com/ptrkrysik/gr-gsm/wiki/Manual-compilation-and-installation.

ISBN: 978-602-60581-0-2