PROSIDING
SEMINAR NASIONAL INOVASI TEKNOLOGI PENERBANGAN (SNITP) TAHUN 2019
ISSN : 2548-8090

SNIFFING SINYAL GSM MENGGUNAKAN RTL-SDR UNTUK MENENTUKAN KOORDINAT PENGGUNA GSM

Muhammad Hamzah Asy'ari[1], Margono[1], Teguh Imam Suharto[1]
[1)] Program Studi Teknik Navigasi Udara, Politeknik Penerbangan Surabaya
Jl. Jemur Andayani I/73, Surabaya 60236
Email: hamzahg216@gmail.com[1]

Abstrak

Diantara beberapa negara berkembang Indonesia merupakan salah satu Negara dengan tingkat traffic komunikasi yang cukup padat, yang mana jaringan sinyal GSM sebagai jaringan utama yang digunakan oleh pengguna alat komunikasi untuk berkomunikasi satu dengan yang lainnya. dengan ditemukannya teknologi GSM (Global System for Mobile) yaitu teknologi komunikasi seluler yang bersifat digital. Teknologi GSM banyak diterapkan pada komunikasi bergerak, khususnya telepon genggam (handphone). Global System for Mobile Communication GSM adalah sebuah teknologi komunikasi selular yang bersifat digital. GSM menggunakan sistem TDMA dengan alokasi kurang lebih sekitar delapan pengguna di dalam satu channel frekuensi sebesar 200 kHz persatuan waktu. Awalnya, frekuensi yang digunakan adalah 900 MHz. Pada perkembangannya frekuensi yang digunakan adalah 1800 MHz dan 1900 MHz. Pada penelitian ini dilakukan percobaan sniffing sinyal GSM sehingga koordinat lokasi pengguna GSM dapat diketahui. Untuk melaksanaan proses sniffing, dilakukan scanning sinyal GSM terlebih dahulu menggunakan SDRSharp untuk melihat range frekuensi sinyal GSM yang ada disekitar area pengamatan. Proses sniffing sinyal 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 untuk mendapatkan informasi yang berupa Local Area Identification dan Cell Identify yang dapat digunakan untuk menemukan koordinat lokasi pengguna GSM dengan memanfaatkan bantuan dari program phone tracker. Penelitian ini menggunakan metode analisis teknis deskriptif, observasi, dan studi kepustakaan yaitu mendeskripsikan atau menggambarkan kejadian sesungguhnya dan juga merumuskan masalah, mengumpulkan data, menganalisis data untuk menjawab masalah, merumuskan kesimpulan serta menyusun laporan penelitian.

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

Abstract

Among several developing countries Indonesia is one of the countries with a fairly heavy level of communication traffic, which is the GSM signal network as the main network used by users of communication tools to communicate with each other. with the discovery of GSM (Global System for Mobile) technology, namely cellular communication technology that is digital. GSM technology is widely applied to mobile communications, especially mobile phones. Global System for Mobile Communication GSM is a cellular communication technology that is digital. GSM uses a TDMA system with an allocation of approximately eight users in one channel frequency of 200 kHz time unity. Initially, the frequency used was 900 MHz. In its development the frequency used is 1800 MHz and 1900 MHz. In this research an GSM signal sniffing was

ISSN : 2548-8090

conducted so that the location coordinates of GSM users can be known. To carry out the sniffing process, scan the GSM signal first using SDRSharp to see the GSM signal frequency range around the observation are. The signal sniffing process is done by using RTL-SDR as a GSM signal receiver and GNU Radio as a GSM signal decoder and forwarded by Wireshark as an analyst of GSM signals by using the GSM_TAP filter to obtain information in the form of Local Area Identification and Cell Identify that can be used to find coordinates location of GSM users by utilizing the assistance of a phone tracker program. This study uses descriptive analysis, observation, and literature study methods, namely describing or describing actual events and also formulating problems, collecting data, analyzing data to answer problems, form conclusions and compile research reports.

Keyword : *GSM, RTL-SDR, GNU Radio, Wireshark, Phone Tracker*

PENDAHULUAN

1. Latar Belakang

Perkembangan teknologi di dunia khususnya teknologi komunikasi dan informasi sangatlah pesat, salah satu diantaranya yaitu ponsel. Ponsel merupakan salah satu teknologi yang berperan penting di era modern ini, salah satunya untuk membantu komunikasi jarak jauh. Teknologi ponsel terus saja mengalami perkembangan hingga kini mencapai tinggat level smartphone. Dibalik kemunculan teknologi tersebut ternyata sekaligus melahirkan beberapa hal baru yang fungsinya tentu sebagai penunjang fasilitas dari ponsel itu sendiri. Dan hal-hal baru itu diantaranya adalah infrastruktur BTS dan jaringan atau sinyal selular. Tanpa kedua penunjang tersebut, ponsel dapat dinyatakan tidak memiliki fungsi yang berguna.

Kehadiran jaringan pada sebuah ponsel pastinya berfungsi untuk memperlancar segala urusan seperti halnya berkomunikasi, internet, dan lain sebagainya yang termasuk dalam aktivitas mobile. Di Indonesia sendiri, ada jaringan yang umum dipakai pada pada ponsel seperti GSM. Global System for Mobile Communication disingkat GSM, yaitu sebuah teknologi komunikasi selular yang bersifat digital. GSM merupakan teknologi yang memang diciptakan untuk kepentingan jaringan nirkabel menggunakan mobile. GSM sendiri pada awalnya hanya bekerja pada frekuensi jaringan 900 Mhz yang kemudian menjadi sistem komunikasi generasi kedua atau yang biasa disebut 2G. 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 peluang-peluang penemuan dalam bidang teknologi telekomunikasi.

Perlahan, teknologi jaringan GSM terus melakukan perkembangan yang signifikan, bahkan pada saat itu operator GSM telah memasuki masa jaringan 3G atau Third Generation. Jaringan 3G ini memungkinkan penguna untuk

ISSN : 2548-8090

berkomunikasi dengan lebih baik lagi bahkan secara realtime sekali pun. Namun sekarang ini jaringan GSM sudah berkembang meninggalkan generasi 3G dan memasuki generasi 4G, yang mana jaringan tersebut membuat komunikasi menjadi lebih mudah dan lebih baik dibandingkan generasi-generasi sebelumnya. Banyaknya pengguna ponsel yang akan terus bertambah setiap tahunnya dan demikian pula dengan pengguna jaringan GSM yang juga akan bertambah seiring bertambahnya pengguna ponsel.

2. Rumusan Masalah

Berdasarkan latar belakang diatas, maka yang menjadi permasalahan dalam penulisan yaitu:

1. Menguji Sniffing sinyal GSM untuk mengetahui pengguna GSM di sekitar lokasi pelacakan
2. Melacak lokasi pengguna GSM di sekitar lokasi pelacakan.

3. Batasan Masalah

Agar pembahasan masalah dalam penulisan proposal skripsi ini terarah dan tidak keluar dari tujuan penilitian serta penulisan skripsi, maka perlu adanya batasan masalah meliputi:

1. Pengujian ini dibatasi hanya pada pelacakan sinyal pengguna GSM serta posisi pengguna GSM berada saat pelacakan.

4. Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penulisan ini adalah:

1. Sebagai syarat kelulusan Diploma program studi Teknik Navigasi Udara di Politeknik Penerbangan Surabaya.
2. Sebagai media pembelajaran untuk mengetahui konsep dan aplikasi dari teknologi Sniffing.

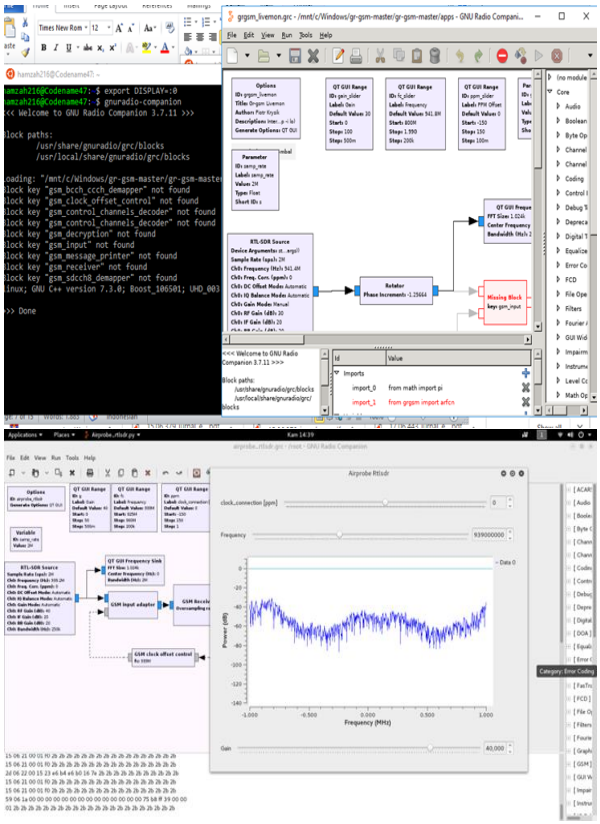
METODE

Dalam melaksannakan penulisan ini, penulis mengadakan penelitian untuk pengumpulan data dengan cara :

1. Metode Kepustakaan atau literature
   Yaitu dengan cara menelaah referensi dari berbagai sumber yang berkaitan dengan masalah yang penulis teliti.
2. Metode Observasi
   Yaitu penulis mengambil data dan melakukan pengamatan di Bandar Udara Sam Ratulangi Manado sebagai bahan analisa serta menganalisa data yang didapat.
3. Metode Analisis
   Yaitu dalam penulisan ini penulis menggunakan analisis teknis dengan menggunakan analisa kuantitatif.

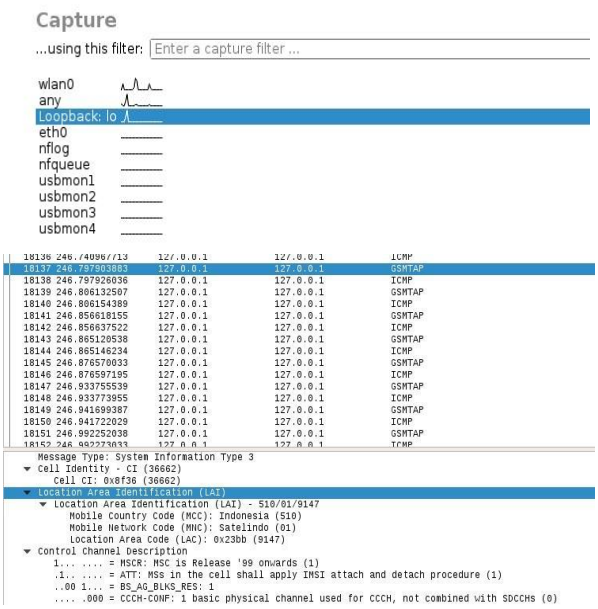
HASIL DAN PEMBAHASAN

ISSN : 2548-8090



Gambar 1 Proses sniffing sinyal GSM

Uji coba sniffing sinyal menggunakan program gr-gsm. Melakukan 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 951 MHz, sesuai dengan hasil scanning yang telah dilakukan menggunakan Sdrsharp. Grafik sinyal dengan range frekuensi yang telah ditentukan yaitu 951 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 2 Analisis sinyal GSM

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. 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". 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 Identify*.

ISSN : 2548-8090

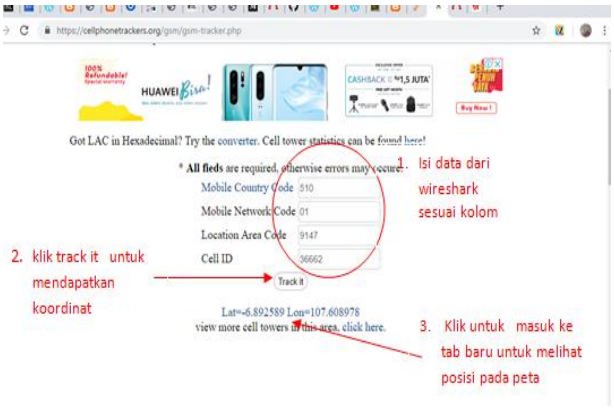
Tabel 1 MCC dan MNC operator seluler

Operator	MCC	MNC
Telkomsel	510	10
XL Axiata	510	11
Indosat Ooredoo	510	01
3 Tri Indonesia	510	89
Smartfren	510	09
Bolt Super 4G	510	88

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. Untuk program Phone Tracker itu sendiri berupa web dengan akses secara bebas. Untuk program Phone Tracker itu sendiri dapat diakses di internet dengan menuju link http://cellphonetrackers.org/gsm/gsmtracker.php

Gambar 3 LAI dan CID yang terdeteksi

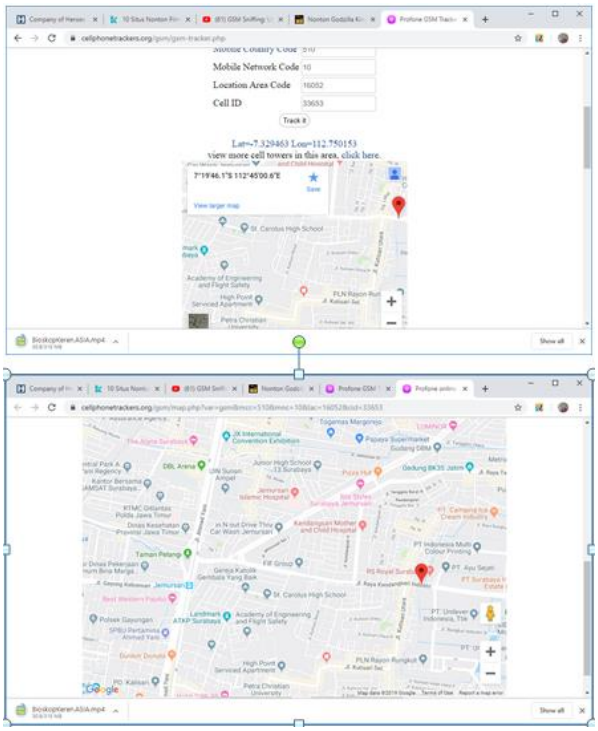
Untuk mendapatkan koordinat lokasi, maka harus mengetahui data yang dibutuhkan yaitu, MCC, MNC, LAC dan CID. Untuk MCC (*Mobile Country Code*) Kode negara untuk operator seluler di Indonesia adalah 510 dan MNC (*Mobile Network Code*) Kode operator telekomunikasi. misalnya Indosat 01, XL dan sebagainya.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



Gambar 4 Halaman utama pada Phone Tracker

Data-data seperti LAI, MCC, MNC, LAC dibutuhkan untuk mengisi data Phone Tracker. Setelah mengisi data yang dibutuhkan untuk tracking, maka setelah itu menekan “track” sehingga kita akan mendapatkan koordinat berupa *Latitude* dan *Longitude* serta dengan menekan tulisan longitude dan latitude, maka kita akan masuk ke tab baru.

ISSN : 2548-8090



Gambar 5 Peta lokasi dan posisi yang dilacak

Setelah didapatkan Latitude dan Longitude maka hasil yang didapat berupa koordinat berupa peta posisi sipengguna GSM. Posisi yang didapat adalah posisi yang bersifat sementara, apabila melakukan track sekali lagi pada Phone Tracker maka ada kemungkinan posisi si pengguna akan berubah.

PENUTUP

1. Kesimpulan

Data yang dihasilkan dalam proses sniffing sinyal GSM yang berupa Local Area Identification dan Cell identification. Data-data tersebut yang dapat menunjukan koordinat pengguna sinyal GSM yang ter-sniffing dengan bantuan program aplikasi phone tracker. Percobaan sniffing sinyal GSM yang dilakukan dua kali untuk mendapatkan satu pengguna GSM secara acak yang ter-sniffing dan dengan koordint yang sama. Berdasarkan uraian pada pembahasan penelitian dengan judul "Sniffing Sinyal GSM Menggunakan RTL-SDR Untuk Menentukan Koordinat Pengguna GSM" yang telah tertera pada BAB IV maka dapat diambil kesimpulan :

a) Sesuai dengan hasil penelitian data yang diambil dari proses sniffing sinyal GSM Diketahui bahwa hasil dari analisa data menggunakan wireshark, maka yang didapat berupa data Local Area Identiication, Cell Identiication, MCC, dan MNC. Data tersebut digunakan untuk menentukan koordinat menggunakan aplikasi phone tracker.
b) Sniffing dilakukan sebanyak dua kali dengan target yang sama untuk melihat pergerakan si pengguna. Target yang dipantau pergerakannya tidak berubah posisi dan masih di sekitar lokasi area pengamatan.

2. Saran

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

a) Snffing pengguna GSM diarea yang lebih luas, tidak hanya didalam satu ruangan atau tempat, agar mendapatkan lebih banyak pengguna GSM yang dapat ter-sniffing.
b) Analisa jaringan yang lebih kompleks, sehingga tidak hanya lokasi pengguna GSM yang ter-sniffing yang diketahui namun bisa

ISSN : 2548-8090

dilakukan snifing percakapan yang terenskripsi..

c) Penelitian ini hanya digunakan untuk sebagai pembelajaran taruna, karena pada dasarnya Sniffing adalah sebuah teknik memonitoring atau melakukan analisis terhadap paket data yang ditransmisikan sehingga tidak boleh digunakan untuk kejahatan Cyber.

DAFTAR PUSTAKA

[1] Krysik, Piotr. Manual compilation and installation. https://github.com/ptrkrysik/gr-gsm/wiki/Manual-compilation-and-installation

[2] Getting the RTL-SDR to work in Windows 10. https://www.rtl-sdr.com/getting-the-rtl-sdr-to-work-on-windows-10/

[3] Gunawan Wibisono, Uke Kurniawan Usman, Gunadi Dwi Hantoro. **Konsep Teknologi Seluler.** Balikpapan : Informatika

[4] Orebaugh, Angela, Gilbert Ramirez, Jay Beale. (2007). *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Canada: Syngress publishing, inc.

[5] RTL-SDR. http://www.rtl-sdr.com/about-rtl-sdr/

[6] GNU Radio. http://gnuradio.org/about/

[7] Budiono, Adhima Arisandi. Installasi GNURadio pada Linux Ubuntu. https://adhimaab.wordpress.com/2018/03/20/installasi-gnuradio-pada-linux-ubuntu/

[8] Purba, Onno Widodo. GNURadio: Progamming Untuk pemula. https://lms.onnocenter.or.id/wiki/index.php/GNURadio:_Programming_Untuk_Pemula

[9] Braun, Martin. PyBOMBS-The What. The How and the Why. https://www.gnuradio.org/blog/2016-06-19-pybombs-the-what-the-how-and-the-why/

[10] Profone GSM Tracker. https://cellphonetrackers.org/gsm/gsm-tracker.php

[11] gr-gsm. Manual compilation and installation. https://osmocom.org/projects/gr-gsm/wiki/Installation Krysik, Piotr. Manual compilation and installation. https://github.com/ptrkrysik/gr-gsm/wiki/Manual-compilation-and-installation

[12] Getting the RTL-SDR to work in Windows 10. https://www.rtl-sdr.com/getting-the-rtl-sdr-to-work-on-windows-10/

[13] Gunawan Wibisono, Uke Kurniawan Usman, Gunadi Dwi Hantoro. **Konsep Teknologi Seluler.** Balikpapan : Informatika

[14] Orebaugh, Angela, Gilbert Ramirez, Jay Beale. (2007). *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Canada: Syngress publishing, inc.

[15] RTL-SDR. http://www.rtl-sdr.com/about-rtl-sdr/

[16] GNU Radio. http://gnuradio.org/about/

[17] Budiono, Adhima Arisandi. Installasi GNURadio pada Linux Ubuntu. https://adhimaab.wordpress.com/2018/03/20/installasi-gnuradio-pada-linux-ubuntu/