Analisis Hasil Implementasi Algoritma RC4 untuk Pengamanan Komunikasi Suara pada Android

Mahazam Afrad[1], L. Budi Handoko, M.Kom[2]
[1,2]Jurusan Teknik Informatika, FASILKOM UDINUS
Jl. Nakula 1 No 5-11 Semarang 50131 INDONESIA
[1]mahazam01@gmail.com, [2] ensignbudi@gmail.com

Abstract (Voice communication through the Internet has the advantage of low cost but of a lower security level and vulnerable to eavesdropping. Safety voice communications can be done in various ways. Securing voice communications will be performed on each bit input by passing a series of safeguards that produces output that is different than the original.

At this research is to implement the RC4 algorithm to secure voice communication via the Internet on the Android platform and know the encryption by using the RC4 algorithm delay does not exceed the predetermined parameter is less than 300 ms.

Results of analysis of different test data using encryption and no encryption obtained delay the packets are encrypted and no encryption states that there is no difference between using encryption with a delay delay without encryption. From these results stating that the android voice communication using RC4 encryption algorithm description in accordance with the recommended delay is less than 300ms so that it can be accepted and the results. With the RC4 algorithm can be used for communication for Voice Over Internet Protocol (VoIP).)

Index Terms— VoIP, Encryption, Android, Technology, Networking, Cryptography

I. PENDAHULUAN

Dewasa ini teknologi informatika bekembang secara pesat, dimana memungkinkan bertukar informasi data melalui jaringan internet. Kemudahan bertukar informasi saat ini dimanfaatkan untuk melakukan komunikasi suara.

Komunikasi suara melalui jaringan internet dapat dibangun dengan mobile. Salah satu perangkat mobile yang dapat digunakan sebagai komunikasi melalui internet yaitu perangkat mobile dengan sistem operasi Android. Android merupakan

sistem operasi berbasis linux yang dapat digunakan pada telepon seluler. Android menyediakan platform terbuka bagi para pengembang buat menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam peranti bergerak.

II. TINJAUAN PUSTAKA

. Tinjauan Pustaka untuk literature dalam penelitian ini dapat dilihat pada tabel 1.

Tabel 1. State of art

No	Nama Peneliti Dan Tahun	Judul	Metode	Hasil
1.	Rinaldi Munir, 2013	Pengamanan Komunikasi Suara Melalui Internet Pada Telepon Seluler denganAlgoritma Tea Pada Platform Android	Metode pengamanan yang diterapkan dengan metode kriptografi modern. Pengamanan dilakukan pada masing masing bit masukan, melewati serangkaian pengamanan, kemudian hasil keluaran yang sama sekali berbeda dengan masukan.	Pada penelitian ini pengamanan komunikasi suara dapat dilakukan pada jaringan internet dengan algoritma TEA dan mobile Android sebagai telepon selulernya Pengamanan yang dilakukan tidak merusak jalannya komunikasi suara dan delay yang dihasilkan dari enkripsi dan deskripsi yakni sebesar 989,686 mili detik.
2.	A. Thoriq Abrowi Bastari, 2010	Analisis Perbandingan Stream Cipher RC4 dan SEAL	Metode pengamanan yang diterapkan dengan metode kriptografi modern. Dengan menganalisa dan membandingkan kedua Algoritma Stream Cipher RC4 dan SEAL	Dari hasil pengujian dan studi yang dilakukan oleh penulis didapatkan bahwa RC4 adalah algoritma enkripsi stream cipher yang sangat cepat dan memiliki tingkat keamanan yang relatif baik.
3.	Mokh. Lugas adi Patra, 2014	Enkripsi Dan Dekripsi Pesan Suara Dengan Metode Algoritm	Menggunakan Metode Algoritma Serpent yaitu memuat cipher block yang	Data suara yang berupa sinyal digital akan dienkripsi terlebih dahulu kemudian

		a Serpent Menggunakan Visual Basic 6.0	berfungsi untuk mengelompokkan bit-bit sinyal digital menjadi block-block dengan ukuran bit tertentu.	dikirim melalui media jaringan dan ketika data suara yang telah dienkripsi sampai ke penerima proses selanjutnya adalah mendekripsi data suara yang telah diterima dengan metode yang sama.

III. METODE YANG DIUSULKAN

A. Teknik Analisa Data

Adapun analisis kebutuhan data dan sistem dalam penelitian ini adalah sebagai berikut :

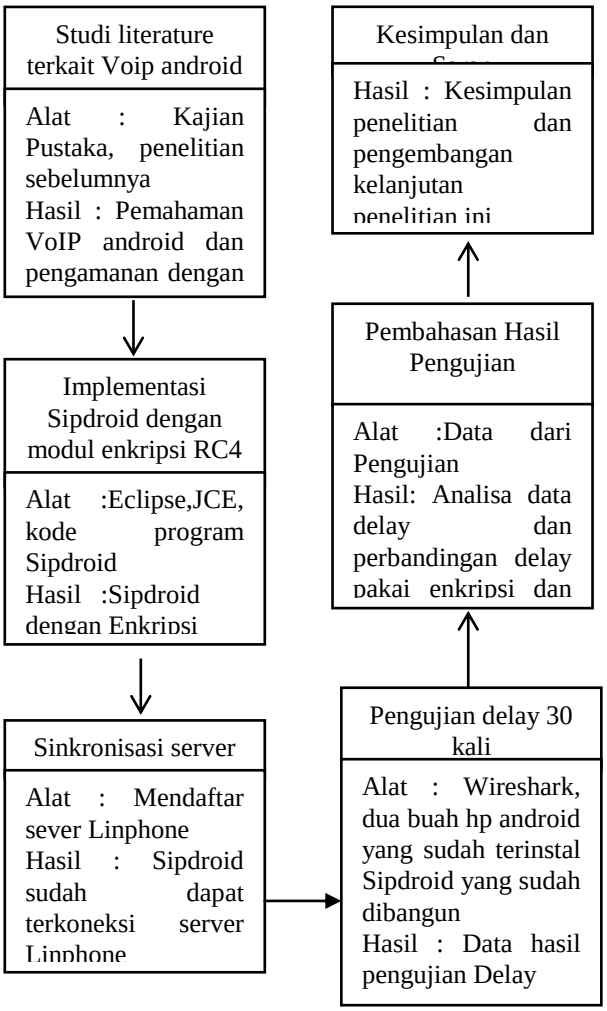
1. Penggunaan API dari Android memberikan kemudahan dalam membangun komunikasi melalui protokol internet. Dalam Tugas Akhir akan dilakukan pengamanan pada bit bit paket suara yang akan dikirim. Tetapi diperlukan pengaksesan pada paket-paket yang akan dikirim. API Android tidak dapat diakses sehingga dapat dipilih aplikasi Sipdroid. Aplikasi ini membangun sendiri komunikasi suara melalui internet. Sehingga penyisipan enkripsi dan dekripsi dapat dilakukan.
2. Penyedia layanan SIP dibagi menjadi berbayar dan tidak berbayar. Untuk mencapai tujuan nilai ekonomis yang rendah, dipilih layanan yang tidak berbayar. Tetapi layanan SIP yang tidak berbayar ini ada berbagai kendala yang bisa terjadi seperti adanya batasan durasi telepon, server yang suka mati, hingga proses pendaftaran yang menyulitkan pengguna. SIP Linphone dipilih karena layanan SIP tidak berbayar ini tidak memiliki kendala yang disebutkan.
3. Pada aplikasi yang akan dibangun menggunakan protocol User Datagram Protocol (UDP) dan algoritma yang digunakan adalah Algoritma RC4.
4. Setelah aplikasi siap selanjutnya melakukan pengujian delay pemanggilan dengan menggunakan enkripsi dan tanpa menggunkan enkripsi. Hasil dari pengujian ini ditangkap menggunakan *tools wirshark.*
5. Pengujian dilanjutkan dengan melakukan pengujian hasil enkripsi untuk mengetahui apakah ciphertext dengan plainteks meru pakan data yang berbeda

dan kunci yang berbada masih dapat saling berkomunikasi atau tidak.

6. Melakukan perbandingan antara hasil pengujian delay menggunakan enkripsi dengan tanpa menggunakan enkripsi dan hasil delaynya apakah melebihi batas yang direkomendasikan yaitu 300ms.

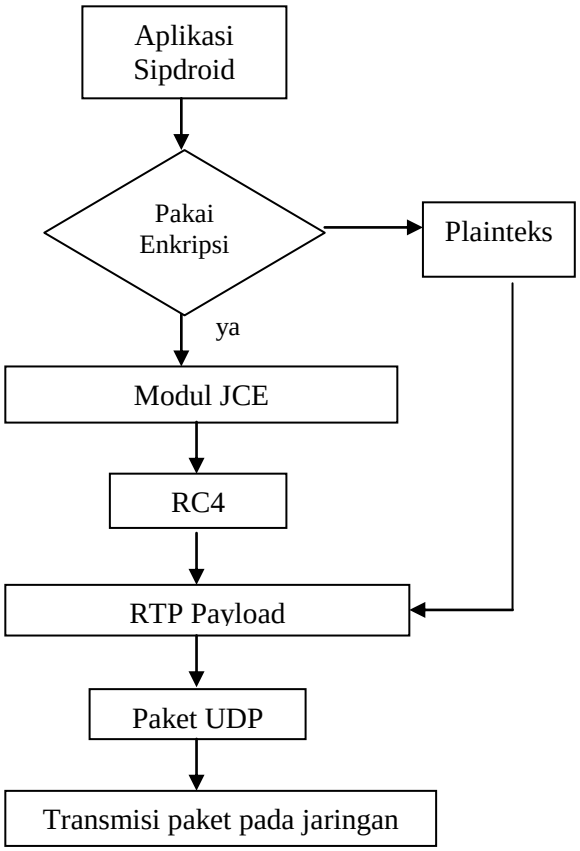
B. Metode Penelitian

Metode penelitian yang akan dilakukan oleh peneliti adalah sebagai berikut:



IV. IMPLEMENTASI

Implementasi algoritma RC4 pada aplikasi Sipdroid menggunakan modul JCE (*Java Cryptography Extension*). Pada aplikasi yang akan dibangun menggunakan protocol User Datagram Protocol (UDP) dan algoritma yang digunakan adalah Algoritma RC4. Proses enkripsi dilakukan pada RTP payload sebelum RTP dibungkus menjadi paket UDP dan dikirim melalui jaringan. Proses penggambaran implementasi modul enkripsi sebagai berikut :

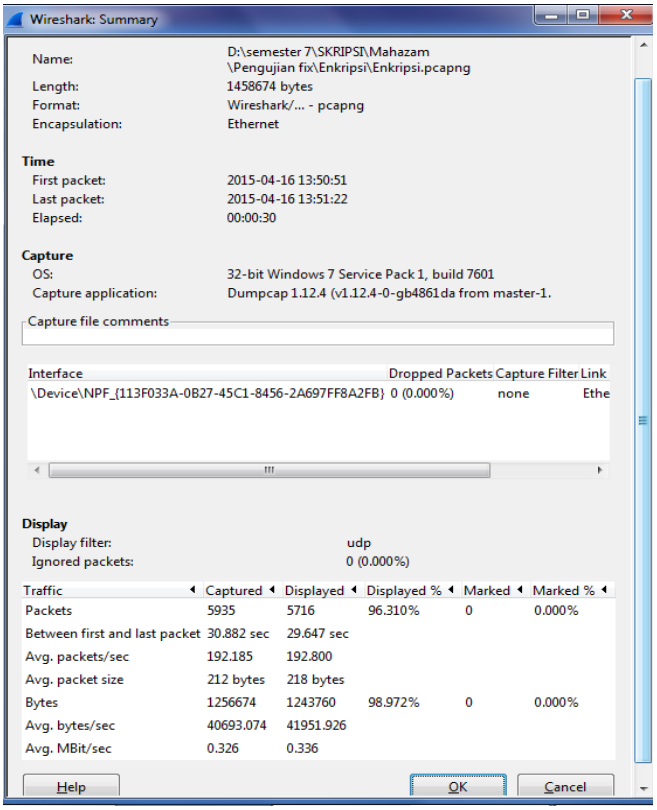


V. ANALISA & PEMBAHASAN

Analisa pengujian sistem bertujuan untuk mengetahui delay dari sistem komunikasi VoIP. Pengujian ini ada tiga tahap yaitu pengujian komunikasi dengan enkripsi, pengujian komunikasi tanpa enkripsi dan pengujian hasil enkripsi. Untuk mendapatkan data yang baik maka pengujian dilakukan sebanyak 30 kali.

A. Analisa Pengujian Delay dengan Enkripsi

Berikut merupakan tangkapan pada menu *summary* di *wireshark* dari sampel pengujian ke satu:



Dengan menggunakan hasil *summary* di atas dapat dihitung *delay* seperti berikut:

$$\text{Delay(sec)Tx} = 1\frac{\textit{Time beween first and last packet(sec)}}{\textit{Jumlah paket}}$$

= 29,647 sec/5716

= 0.005186 sec

Dari hasil perhitungan *delay* pada sampel pertma yang diperoleh yaitu 0,005186sec atau 5,186ms.

Untuk hasil delay dari pengujian sebanyak 30 kali dapat dilihat pada tabel dibawah ini:

Tabel 2 hasil pengujian enkripsi

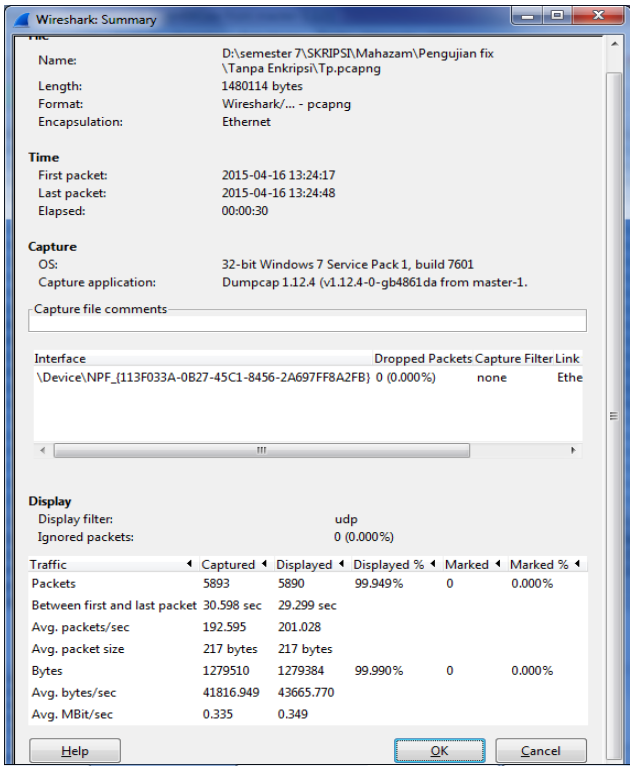
NO	Jumlah Paket	Time beween first and last packet(sec)	Delay (ms)
1	5716	29,647	5,186
2	5980	30,008	5,018
3	5069	30,344	5,986
4	6021	30,432	5,054
5	5887	30,567	5,192
6	5838	30,567	5,236
7	5887	30, 568	5,192
8	5835	30, 455	5,219
9	5838	30,679	5,255
10	5884	30,798	5,234
11	5832	30,488	5,228
12	5854	30,687	5,242
13	5887	30,598	5,198
14	5889	30,768	5,225
15	5878	30,878	5,253
16	5889	30,589	5,194
17	5876	30,489	5,189
18	5840	30,698	5,256
19	5898	30,789	5,220
20	5787	30,482	5,267
21	5885	30,583	5,197
22	5834	30,678	5,258
23	5835	30,776	5,274

24	5845	30,564	5,229
25	5857	30,445	5,198
26	5821	30,349	5,214
27	5872	30,587	5,209
28	5867	30,689	5,231
29	5834	30,381	5,208
30	5841	30,482	5,219

B. Analisa Pengujian Delay Tanpa Enkripsi

Analisa Pengujian kedua ini untuk megetahui delay yang dihasilkan tanpa adanya proses enkripsi dan deskripsi. Skema analisa pengujian yang digunakan sama seperti pengujian menggunakan enkripsi deskripsi yaitu dengan menggunakan aplikasi *wireshark*. Pengujian komunikasi ini dilakukan selama kurang lebih 30 detik.

Berikut merupakan tangkapan pada menu *summary* di *wireshark:*



Dengan menggunakan hasil *summary* di atas dapat dihitung *delay* seperti berikut:

$$\text{Delay(sec)Tx} = \frac{\textit{Time beween first and last packet(sec)}}{\textit{Jumlah paket}}$$

= 29,299 sec/5890

= 0,004974 sec

Dari hasil perhitungan *delay* pada sampel pertama yang diperoleh yaitu 0,004974 sec sec atau 4,974ms. Perhitungan lengkap pengujian 30 kali delay tanpa enkripsi dapat dilihat pada lampiran 2. Untuk hasil delay dari pengujian sebanyak 30 kali dapat dilihat pada tabel dibawah ini:

Tabel 3 hasil pengujian enkripsi

No	Jumlah Paket	Time beween first and last packet(s)	Delay (ms)
1	5890	29,299	4,974
2	5733	23,923	4,173
3	5878	30,058	5,114
4	5738	23,984	4,118
5	5987	30,883	5,158
6	5938	30,786	5,187
7	5987	30,455	5,087
8	5935	30,568	5,150
9	5938	30,879	5,200
10	5984	30,898	5,163
11	5932	30,888	5,207
12	5899	30,687	5,202
13	5987	30,898	5,161
14	5989	30,568	5,104
15	5978	30,678	5,132
16	5989	30,989	5,174

17	5976	30,789	5,152
18	5897	30,898	5,240
19	5998	30,889	5,150
20	5899	30,882	5,235
21	5985	30,883	5,160
22	5898	30,286	5,135
23	5935	30,876	5,202
24	5945	30,564	5,141
25	5957	30,745	5,161
26	5921	30,549	5,159
27	5972	30,	5,172
28	5967	30,789	5,160
29	5934	30,881	5,204
30	5941	30,882	5,198

Hasil pengujian delay menunjukan bahwa tidak ada delay yang melebihi batas rekomendasi yaitu 300ms.

C. Analisa Uji Beda Statistik

Pada pengujian sebelumnya telah didapat data delay yang menggunakan enkripsi dan tanpa menggunakan enkripsi. Untuk mengetahui apakah ada perbedaan antara delay setelah diberikan enkripsi dan tanpa menggunkan enkrispi ini maka digunakan pengujian perbedaan dua rata rata dari sampel berkorelasi. Untuk menguji siginfikan atau tidaknya perbedaan dua rata rata sampel dapat menggunakan rumus uji t sebagai berikut:

$$t = \frac{\sum D}{\sqrt{\frac{n\sum D^2 - (\sum D)^2}{n-1}}}$$

Keterangan :

t = Koefisien t

X_1 = Delay menggunakan enkripsi

X_2 = Delay tanpa enkripsi

$\overline{X_1}$ = Rata rata pada delay enkripsi

$\overline{X_2}$ = Rata rata pada delay tanpa enkripsi

n = Jumlah data

$\sum D$ = Jumlah perbedaan setiap pasangan (X_1-X_2)

Sebelum menghitung nilai t hitung dibuat hipotesa untuk penelitian ini yaitu:

1. Hipotesis Penelitian:

H_0 = Tidak terdapat perbedaan antara delay yang telah menggunakan enkrispi dengan delay tanpa menggunakan enkripsi.

H_1 = Terdapat perbedaan antara delay yang telah menggunakan enkrispi dengan delay tanpa menggunakan enkripsi.

2. Hipotesa statistik:

$H_0 : \mu_1 = \mu_2$

$H_1 : \mu_1 \neq \mu_2$

3. Mencari besarnya nilai t hitung

$$t = \frac{\sum D}{\sqrt{\frac{n\sum D^2 - (\sum D)^2}{n-1}}}$$

$$t = \frac{4{,}308}{\sqrt{\frac{30.18{,}558864 - (4{,}308)^2}{30-1}}}$$

$$t = \frac{4{,}308}{\sqrt{\frac{556{,}766 - 18{,}559}{29}}}$$

$$t = \frac{4{,}308}{4{,}307}$$

$$t = 1{,}00023$$

Pengujian hipotesis dilakukan pada taraf sihnifikan α = 0,05 dan derajat kebebasan dk =(n_1+n_2)=58, maka dari daftar distribusi t dengan peluang 1- α= 0,95 dan dk = 58 diperoleh $t_{0,95}$ (58) =1,672.

Berdasarkan perhitungan penelitaian diperoleh t=$1,00023$, jadi t_{hitung}<t_{tabel} yaitu $1,00023$ < 1,672. Sehingga dapat disimpulkan H_1 ditolak dengan H_0 diterima dengan taraf sihnifikan α = 0,05, maka dapat disimpulkan bahwa tidak terdapat perbedaan antara delay dengan menggunakan enkripsi dan tanpa menggunakan enkripsi.

D. Pembahasan

Hasil analisa data uji beda dengan menggunakan enkripsi dan tanpa menggunakan enkripsi diperoleh delay dengan paket yang dienkripsi dan tanpa menggunakan enkripsi menyatakan bahwa tidak ada perbedaan antara delay menggunakan enkripsi dengan delay tanpa enkripsi. Dari hasil ini menyatakan komunikasi suara yang pada android dengan menggunakan enkripsi deskripsi algoritma RC4 sesuai dengan delay yang direkomendasikan yaitu kurang dari 300ms sehingga dapat diterima dan hasil tersebut. Hasil ini juga membuktikan bahwa algoritma RC4 merupakan algoritma yang ringan dan sesuai untuk pengamanan komunikasi suara secara realtime.

VI. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan dari penelitian yang telah dilakukan maka dapat diambil kesimpulan seperti berikut:

1 Pengamanan pada komunikasi suara yang dibangun pada platform android dengan mengenkripsi RTP payload yang akan ditransmikan pada jaringan VoIP menggunakan algoritma RC4 dapat berjalan dengan baik.

2 Dengan menggunakan algoritma RC4, pengamanan yang dilakukan tidak merusak jalannya komunikasi suara.

3 Berdasarkan uji beda rata rata stitistik delay yang dihasilkan dari komunikasi suara menggunakan enkripsi tidak berbeda dengan delay tanpa enkripsi.

4 Delay menggunakan enkripsi dan tanpa menggunakan enkripsi tidak melebihi batas yang direkomendasikan yaitu 300 ms. Dengan ini algoritma RC4 dapat untuk digunakan untuk komunikasi suara melalui internet(VoIP).

5 Suara yang dienkripsi aman, karena telah diuji coba jika antara perangkat satu dengan yang lain memiliki kunci yang berbeda atau yang satu dengan enkripsi dan yang lain fungsi enkripsi nya dimatikan maka akan hasil suara menjadi bising.

B. Saran

Sedangkan saran yang dapat diberikan pada penelitian ini adalah sebagai berikut:

1 Penelitian ini dapat dilanjutkan dengan memperbaiki kualitas suara pada komunikasi menggunakaan enkripsi. Meski komunikasi berjalan lancer masih ada sedikit *noise*

2 Penelitian ini dapat dilanjutkan dengan menambahkan algoritma enkripsi yang lain agar lebih aman.

3 Penelitian ini dapat dilanjutkan dengan memperbaiki sistem dari sipdroid yang telah dienkripsi, yakni jika kunci enkripsi pada penerima berbeda maka komunikasi langsung terputus.

VII. REVERENSI

[1] Denver, & Munir, R. (2013). Pengamanan Komunikasi Suara Melalui Internet Pada. *Prosiding Konferensi Nasional Informatika*, (pp. 96-101). Bandung.

[2] Lestari, D., & Riyanto, M. Z. (2012). SUATU ALGORITMA KRIPTOGRAFI STREAM CIPHER. *Kontribusi Pendidikan Matematika dan Matematika dalam Membangun* (pp. 33-40). Yogyakarta: FMIPA UNY.

[3] Bastari, A. T. (2010). *Analisis Perbandingan Stream Cipher RC4 dan* SEAL. Bandung: Institut Teknologi Bandung.

[4] Patra, M. L. (2014). *ENKRIPSI DAN DEKRIPSI PESAN SUARA* DENGAN *METODE ALGORITMA* Serpent Menggunakan Visual Basic 6.0 . Semarang: Universitas Dian Nuswantoro Semarang.

[5] Rakhmat, B., & Fairuzabadi, M. (2010, september). STEGANOGRAFI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DENGAN *KOMBINASI* ALGORITMA KRIPTOGRAFI VIGENÈRE DAN RC4. *Jurnal Dinamika Informatika, 5*(2), 1-17.

[6] BIBLIOGRAPHY \l 1033 Andi. (2003). *Memahami model enkripsi & security data.* Semarang: Wahana Komputer Semarang.

[7] Setiadi, W., Irawan, B., & Halomoan, J. (2012). *SISTEM PENJUALAN ONLINE DENGAN MENGGUNAKAN APLIKASI JAVA BERBASIS SISTEM* ANDROID *2.1*. Bandung: Institut Teknologi Telkom .

[8] TONG, H. A. (2005). SIP-based VoIP service – Architecture and Comparison. INFOTECH *Seminar Advanced Communication Services (ACS)* (pp. 1-10). Institute of Communication Networks and Computer Engineering Universityof Stuttgart.

[9] Carlson, I., & Avila, C. (2004). Voice over IP (VoIP)/SIP Infrastructure Considerations for the Interaction Center Platform. *Interactive Intelligence*, 2-19.

[10] H, M. (2003). *Dasar-Dasar Jaringan VOIP*. Retrieved from IlmuKomputer.Com: IlmuKomputer.Com

[11] Bahaweres, R. B., Alaydrus, M., & Wahab, A. (2012). Analisis Kinerja VoIP Client SIPDROID dengan Modul Enkripsi Terintegrasi. *SNATI 2012*.

[12] Kurniawan, A. (2012). *Network Forensics Panduan Analisis & Investigasi* Paket *Data* Jaringan *Menggunakan Wireshark.* ANDI OFFSET.

[13] Suprianto, D., & Agustina, R. (2012). *Pemrograman Aplikasi Android* Step *by Step Membuat Aplikasi Android untuk Smatphone dan* Tablet. Jakarta: PT. Buku Seru.

[14] *CISCO*. (n.d.). Retrieved Desember 10, 2014, from CISCO: http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/5125-delay-details.html