BAB 4
IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi

Tahap implementasi merupakan tahap penerapan dari analisis yang sudah dilakukan. Penerapan metode yang digunakan pada penelitian, selanjutnya akan diimplementasi pada setiap perangkat yang terlibat untuk menghasilkan sistem yang sesuai dengan tahap perancangan.

4.1.1 Implementasi VoIP *Server*

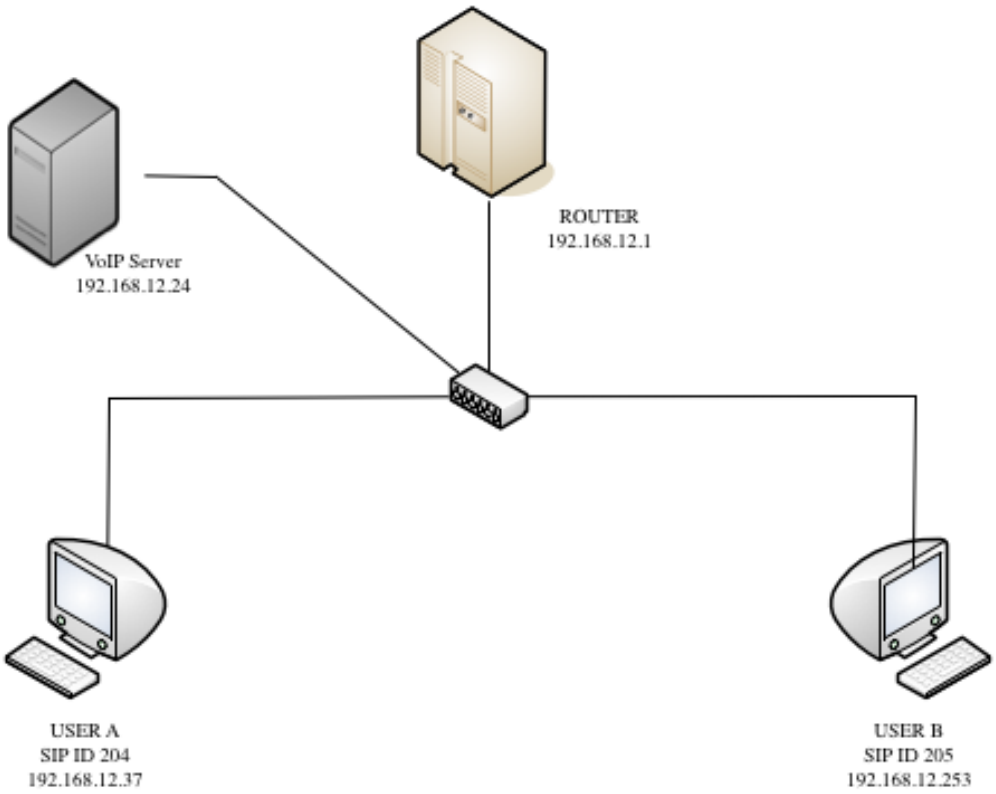
VoIP *server* adalah komputer yang menyediakan layanan VoIP. VoIP server yang digunakan yaitu GNU *Sipwitch* versi 1.5 yang berjalan pada sistem operasi Ubuntu 12.04 . Kebutuhan hardware dari VoIP server adalah sebagai berikut

Tabel 4. 1 Kebutuhan Hardware VoIP *Server*

Perangkat Keras	Spesifikasi
Processor	*Dualcore* 2.4 GHz
Memory	512 MB
Harddisk	10 GB
Sistem Operasi	Ubuntu 12.04
VGA	√
Monitor	√
Keyboard	√
Mouse	√

Perangkat Keras	Spesifikasi
Ethernet	√

VoIP *Server* diimplementasikan menggunakan topologi jaringan pada Gambar 4. 1 Topologi Jaringan VoIP IP address pada VoIP *Server* digunakan sebagai pengalamatan tempat layanan VoIP tersedia. Pada topologi tersebut terdapat 2 user VoIP yang akan saling berkomunikasi.



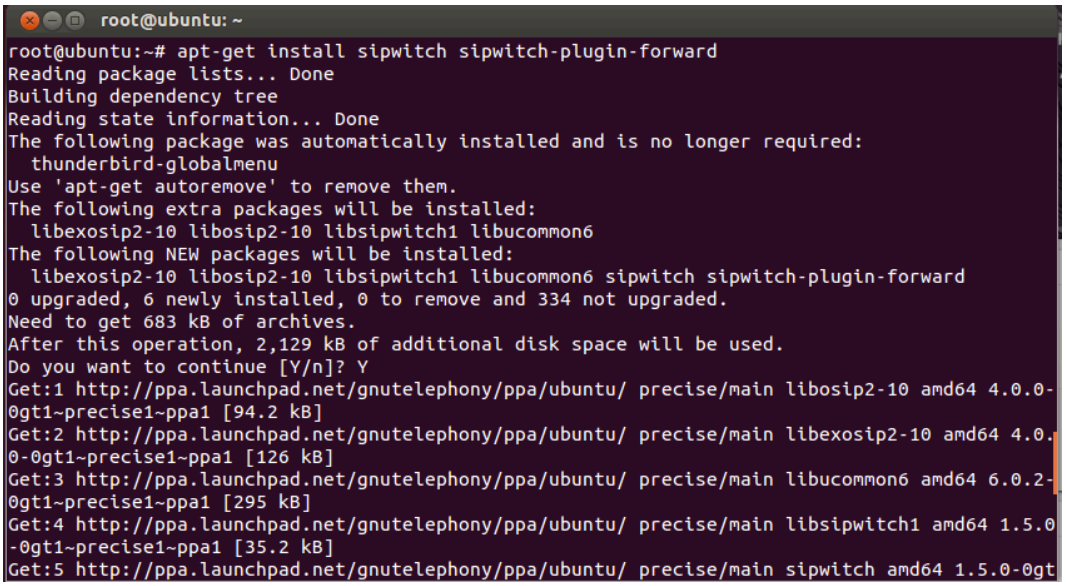
Gambar 4. 1 Topologi Jaringan VoIP

4.1.1.1 Instalasi VoIP *Server*

Instalasi GNU *Sipwitch* dimulai dengan menambahkan repository tempat *source* GNU *Sipwitch* berada. Alamat *Repository* nya adalah "http://ppa.launchpad.net/gnutelephony/ppa/ubuntu" . *Repository* ini ditambahkan

ke dalam sistem operasi sebagai acuan ketika menjalankan perintah ‘apt-get’. Langkah untuk meng-install GNU *Sipwitch* adalah sebagai berikut;

1. Pada terminal, ketik perintah ***sudo add-apt-repository ppa:gnutelephony/ppa***.
2. Setelah *repository* berhasil ditambahkan selanjutnya menginstalasi GNU Sipwitch dengan menggunakan perintah ***sudo apt-get install sipwitch sipwitch-plugin-forward***
3. Untuk menjalankan GNU Sipwitch, gunakan perintah ***/etc/init.d/sipwitch start*** pada terminal.



Gambar 4. 2 Proses Instalasi GNU *Sipwitch*

4.1.1.2 Pembuatan SIP ID

SIP ID digunakan sebagai pengalamatan pada VoIP. Pengalamatan SIP ID yang digunakan yaitu sebagai berikut;

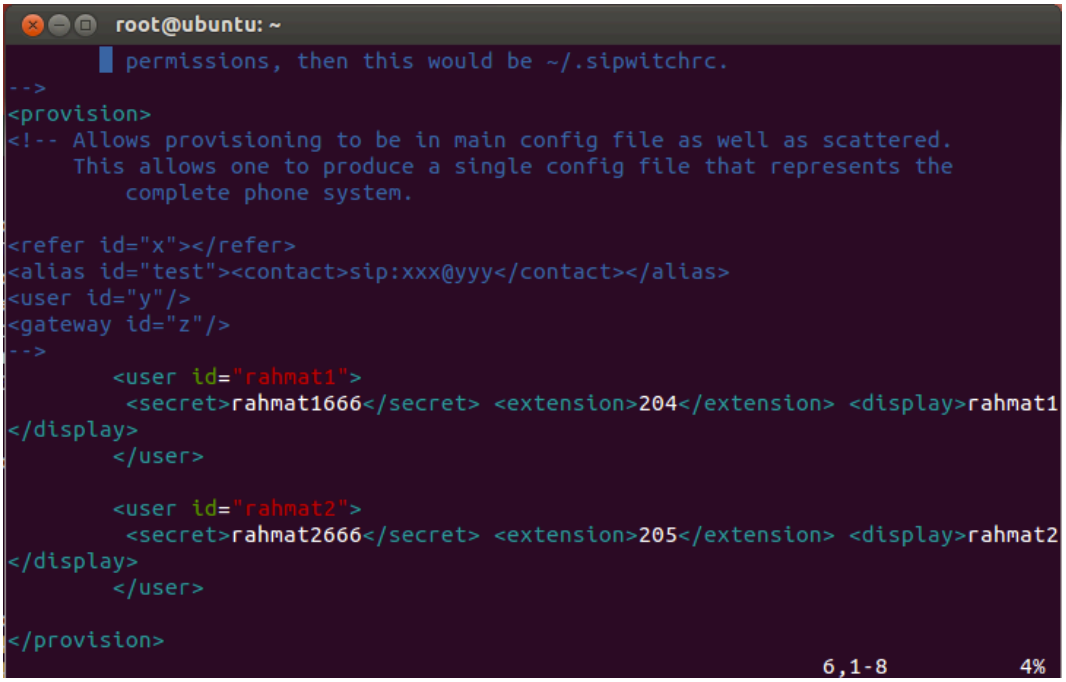
Tabel 4. 2 Pengalamatan SIP ID

IP Address	SIP ID	Keterangan
192.168.12.37	204	*User* A

IP Address	SIP ID	Keterangan
192.168.12.253	205	*User* B

Pembuatan SIP ID pada GNU Sipwitch dilakukan dengan cara meng-edit file "/etc/sipwitch.conf". File sipwitch.conf merupakan file konfigurasi dari GNU *Sipwitch* dan memiliki tipe XML. Berikut ini adalah langkah dalam pembuatan SIP ID

1. Pada terminal, buka file *sipwitch.conf* dengan menggunakan perintah ***vi /etc/sipwitch.conf***
2. Setelah file terbuka, tambahkan konfigurasi dalam tag ***<provision>***
3. Untuk menambahkan SIP ID 204 berikut konfigurasi nya, ***<user id="rahmat1"><secret>rahmat1666</secret><extension>204</extension><display>rahmat1</display></user>***
4. Untuk menambahkan SIP ID 205 berikut konfigurasi nya, ***<user id="rahmat2"><secret>rahmat2666</secret><extension>205</extension><display>rahmat2</display></user>***
5. Simpan file dengan cara menekan tombol *esc*, lalu mengetikkan perintah ***:wq!***



Gambar 4. 3 Konfigurasi file sipwitch.conf

4.1.2 Implementasi VoIP *Client*

Komputer *client* dapat menggunakan layanan VoIP melalui aplikasi VoIP client. Aplikasi VoIP client yang digunakan adalah Jitsi versi 2.4. Jitsi dapat diperoleh dari website jitsi.org. Spesifikasi minimum perangkat keras yang diperlukan yaitu;

Tabel 4. 3 Kebutuhan Perangkat Keras Client

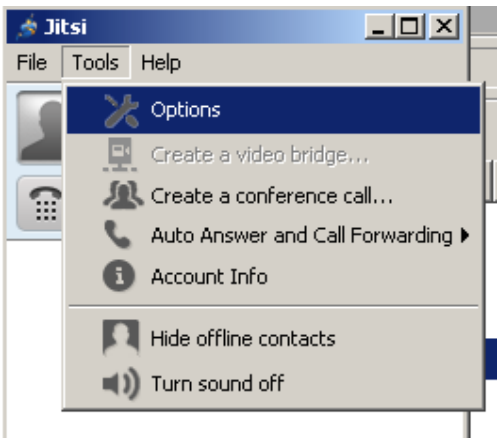
Perangkat Keras	Spesifikasi
Processor	*Dualcore* 2.4 Ghz
Memory	1024 MB
Harddisk	20 GB
Sistem Operasi	Windows 7
VGA	√

Perangkat Keras	Spesifikasi
Monitor	√
Mouse	√
Keyboard	√
Headset with Microphone	√
Ethernet	√

4.1.2.1 Pendaftaran SIP ID

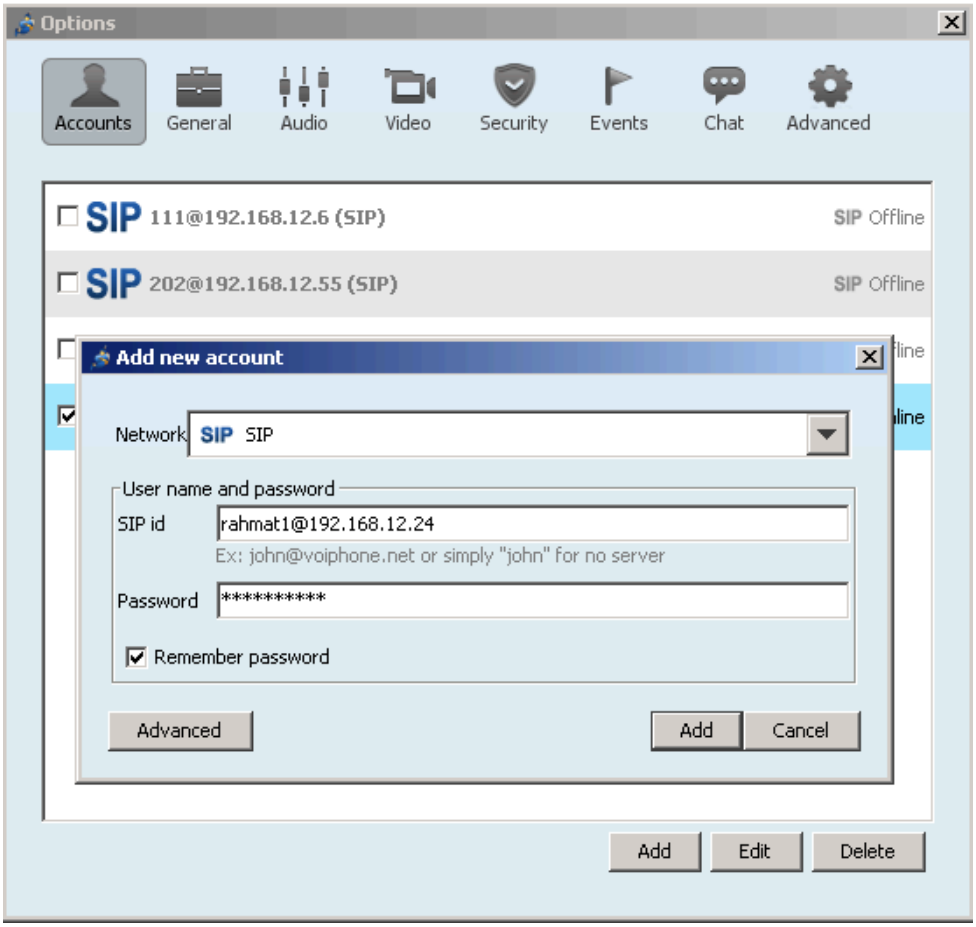
SIP ID yang telah dibuat pada VoIP *Server* lalu diimplementasikan pada VoIP *Client*. Berikut adalah langkah untuk mengimplementasikan SIP ID user A pada VoIP *Client*;

1. Pada aplikasi *Jitsi*, buka menu *Tools* lalu pilih *Options* seperti terlihat pada Gambar 4. 4 Menu *Options* pada *Jitsi*



Gambar 4. 4 Menu *Options* pada *Jitsi*

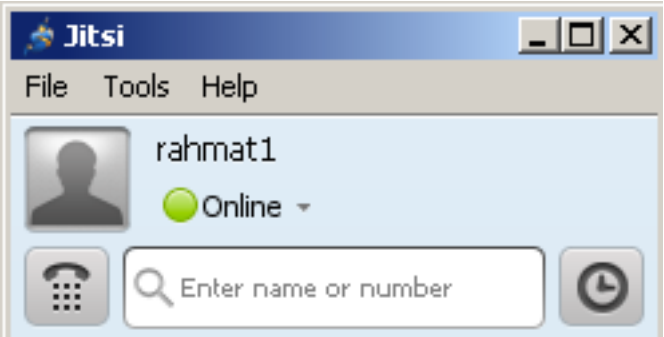
2. Lalu akan muncul jendela *Options*, pada tab menu *Accounts* pilih tombol *Add*
3. Maka akan muncul jendela *Add new Account* seperti pada gambar



Gambar 4. 5 Menu *add new account* pada *Jitsi*

4. Pada baris awal jendela tersebut terdapat list menu *Network* maka pilih *SIP*
5. Pada bagian *field* SIP ID isi dengan user id yang diikuti dengan alamat VoIP *Server* dan digabungkan dengan tanda "@". Maka SIP ID diisi dengan rahmat1@192.168.12.24
6. Bagian *field password* diisi dengan *secret* dari SIP ID, lalu klik *Add*

Setelah SIP ID telah berhasil diimplementasikan akan muncul tanda hijau pada jendela utama seperti pada Gambar 4. 6 Status Koneksi VoIP. Langkah diatas dilakukan juga pada komputer user B.

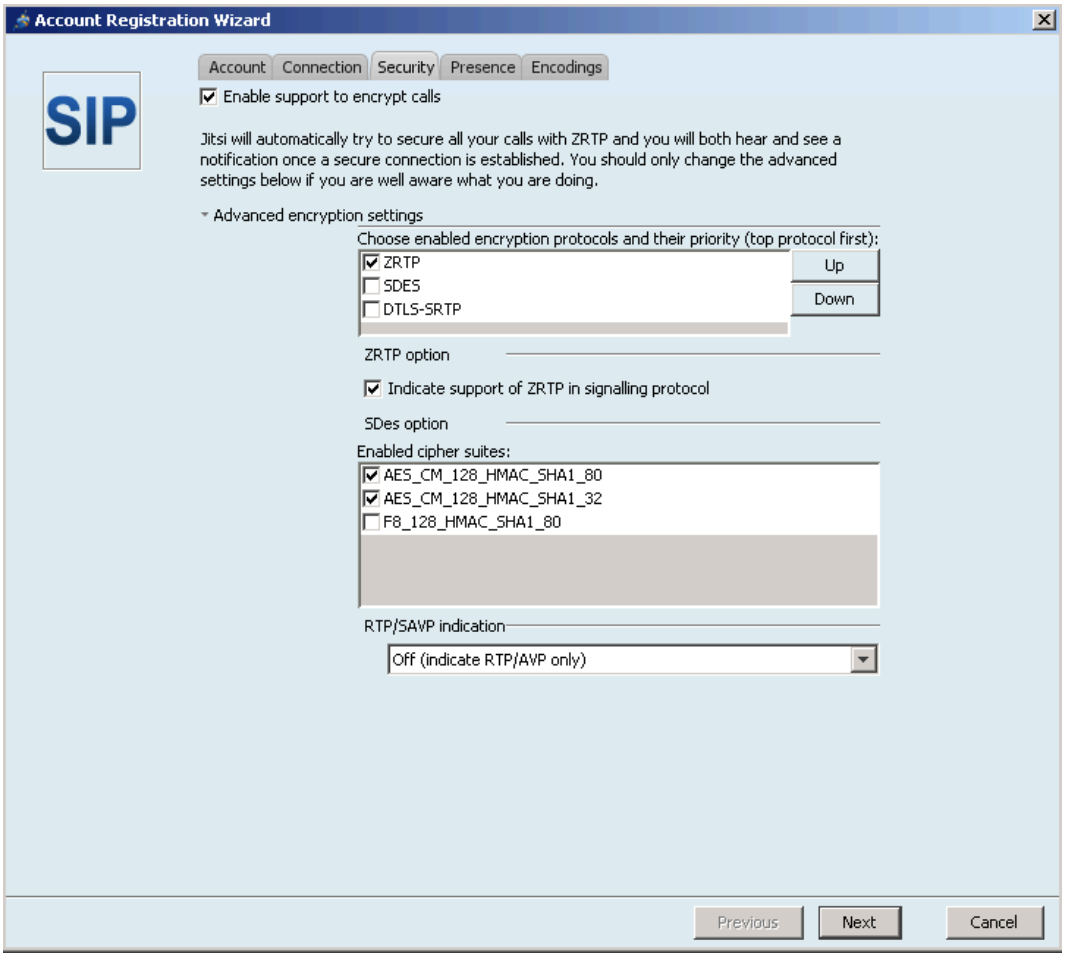


Gambar 4. 6 Status Koneksi VoIP

4.1.2.2 Konfigurasi ZRTP

Komunikasi VoIP dengan ZRTP dapat dilakukan ketika VoIP *server* dan VoIP *client* telah mendukung. Protokol ZRTP sudah didukung oleh GNU Sipwitch tanpa memerlukan konfigurasi tambahan. Pada sisi VoIP Client yang menggunakan *Jitsi*, diperlukan konfigurasi untuk mendukung protokol ZRTP pada komunikasi VoIP dengan langkah sebagai berikut;

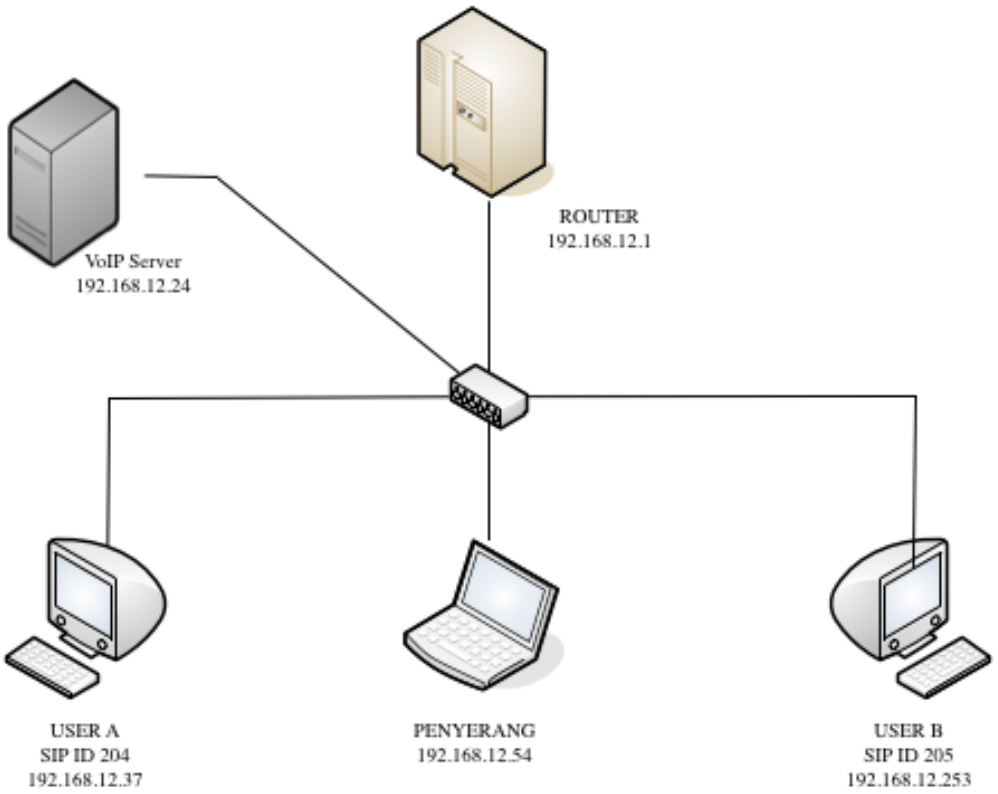
1. Pilih menu *Options* pada *Jitsi*, lalu pilih accout SIP yang digunakan dan pilih *edit*
2. Maka akan muncul jendela *Account Registration Wizard*, pilih tab menu *Security*
3. Lalu *checklist field enable support to encrypt calls*, dan pilih *Advanced encryption settings* untuk menampilkan pilihan yang lebih lengkap
4. Pilihan tersebut menampikan protokol yang akan digunakan dalam mengamankan komunikasi voip dan tipe enkripsi yang akan digunakan. Seperti pada Gambar 4. 7
5. Untuk menyimpan klik *Next* dan klik *Sign In* untuk mengulangi koneksi dengan konfigurasi yang baru ke VoIP *Server*



Gambar 4. 7 Konfigurasi ZRTP

4.2 Pengujian

Pada tahap ini dilakukan pengujian terhadap sistem komunikasi VoIP yang belum diberikan pengamanan dan yang sudah memiliki pengamanan dengan ZRTP. Tujuan dari pengujian ini adalah untuk mengetahui tingkat keamanan dari masing masing sistem VoIP. Arsitektur yang digunakan pada tahap pengujian seperti yang digambarkan pada Gambar 4. 8 Arsitektur Pengujian VoIP



Gambar 4. 8 Arsitektur Pengujian VoIP

4.2.1 Skenario Pengujian

Pada tahap pengujian dilakukan beberapa skenario untuk mengetahui tingkat keamanan sistem VoIP pada beberapa kondisi yang berbeda. Skenario pengujian yang akan dilakukan dijelaskan pada Tabel 4. 4 Skenario Pengujian VoIP.

Tabel 4. 4 Skenario Pengujian VoIP

No	Sistem VoIP	Waktu Penyerangan
1	Tidak menggunakan ZRTP	Sebelum komunikasi VoIP berlangsung
2	Tidak menggunakan ZRTP	Pada saat komunikasi VoIP berlangsung
3	Menggunakan ZRTP	Sebelum komunikasi VoIP berlangsung

No	Sistem VoIP	Waktu Penyerangan
4	Menggunakan ZRTP	Pada saat komunikasi VoIP berlangsung

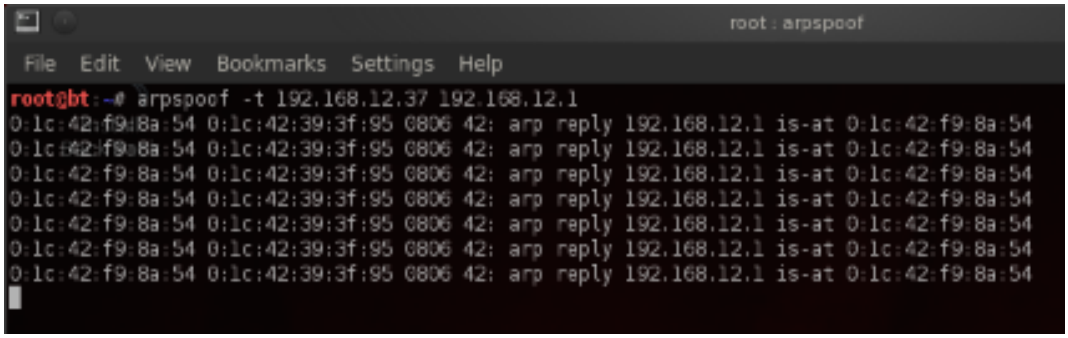
4.2.2 Pengujian VoIP Server tanpa pengamanan

Pada tahap ini pengujian dilakukan berdasarkan topologi dari Gambar 4. 8 Arsitektur Pengujian VoIP. Pengujian dilakukan dengan menggunakan metode *Man In The Middle Attack*. Langkah pertama adalah dengan melakukan *arp spoofing* untuk mengelabui target agar menganggap penyerang adalah *gateway*. Setelah itu dilakukan *packet sniffing* untuk mendapatkan paket rtp milik VoIP. Setelah paket rtp didapatkan langkah selanjutnya adalah mendecode paket rtp tersebut agar dapat diperdengarkan audionya. Pengujian dilakukan dengan sistem operasi *Backtrack* dan menggunakan tools *arpspoof* dan *wireshark*.

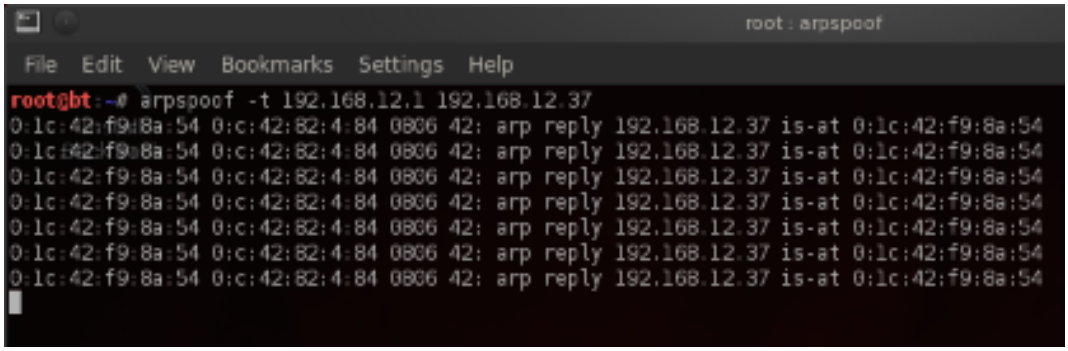
4.2.2.1 Pengujian Sebelum Komunikasi Berlangsung

Pengujian dilakukan sebelum komunikasi antara User A dan User B terjadi. Berikut adalah langkah pengujiannya

1. Pada terminal gunakan perintah ***arpspoof –t 192.168.12.37 192.168.12.1*** dan ***arpspoof –t 192.168.12.1 192.168.12.37*** untuk melakukan spoofing terhadap ip 192.168.12.37

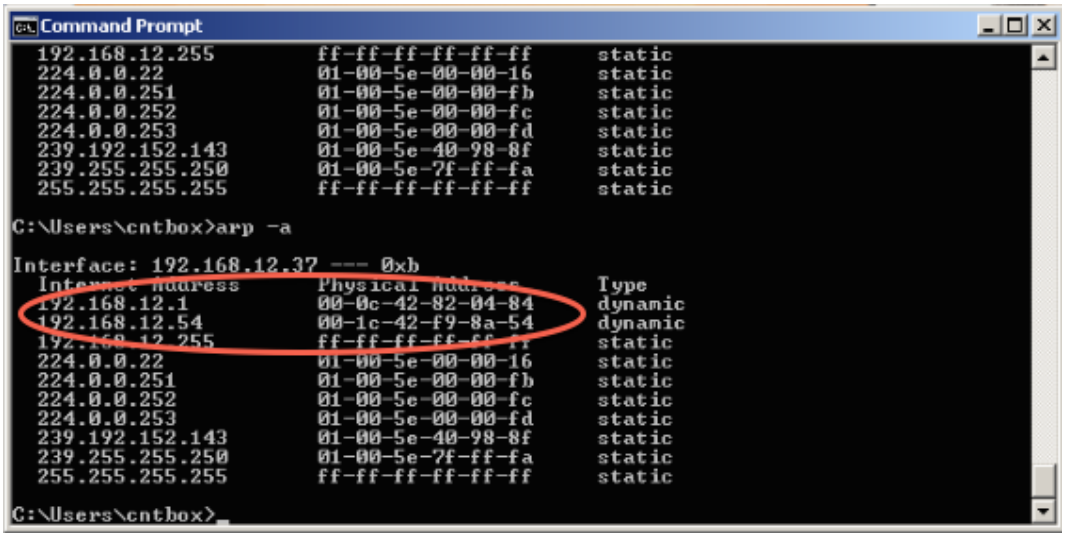


Gambar 4. 9 *Spoofing* terhadap 192.168.12.37

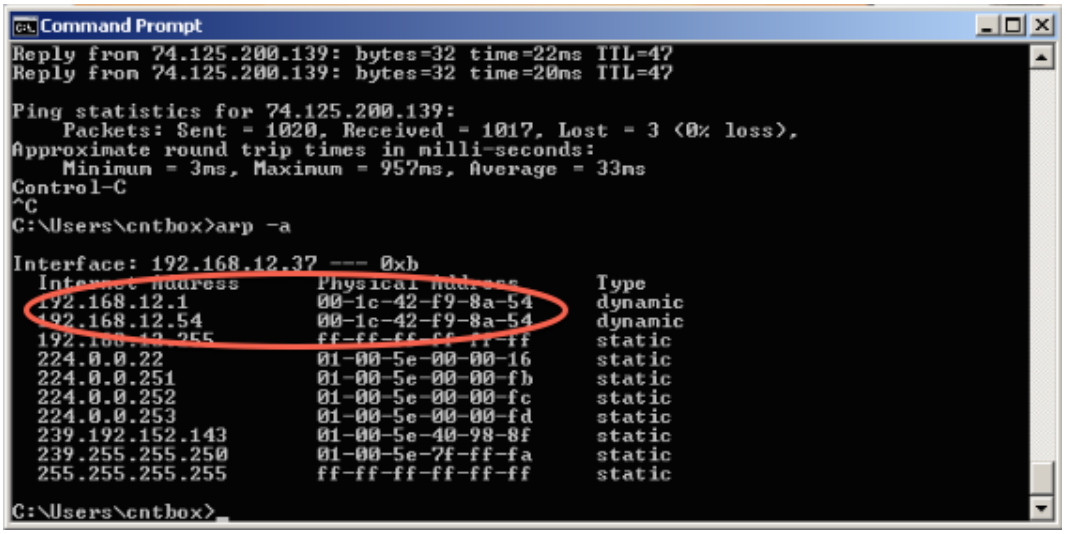


Gambar 4. 10 *Spoofing* terhadap *Gateway*

2. Jika ARP *spoofing* berhasil dilakukan pada sisi target (192.168.12.37), *mac address gateway* (IP Address 192.168.12.1) akan sama dengan mac address penyerang (IP Address 192.168.12.54). Cara mengetahui nya dengan menggunakan perintah ***arp –a*** pada *Command Prompt*

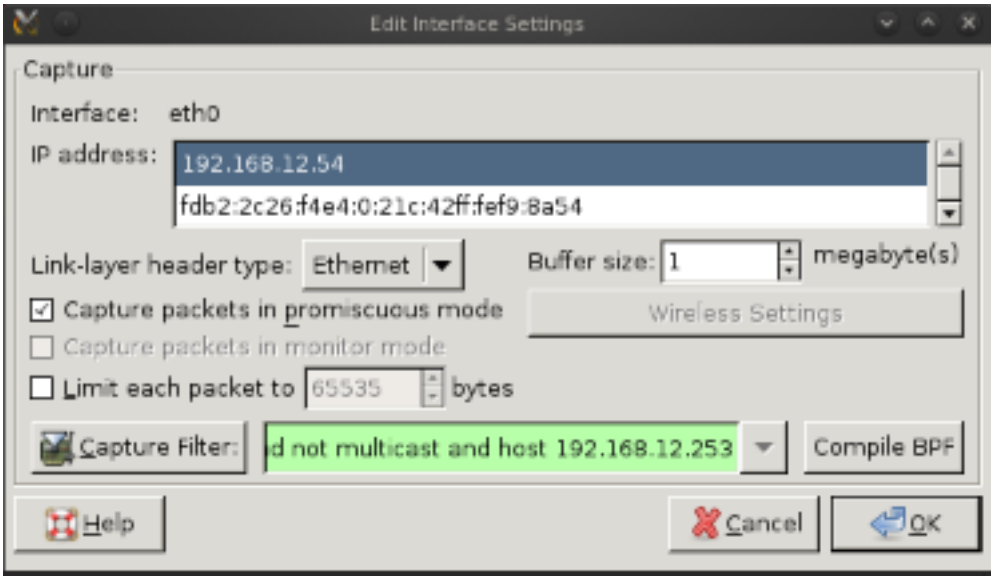


Gambar 4. 11 *Mac Address* sebelum *arp spoofing*



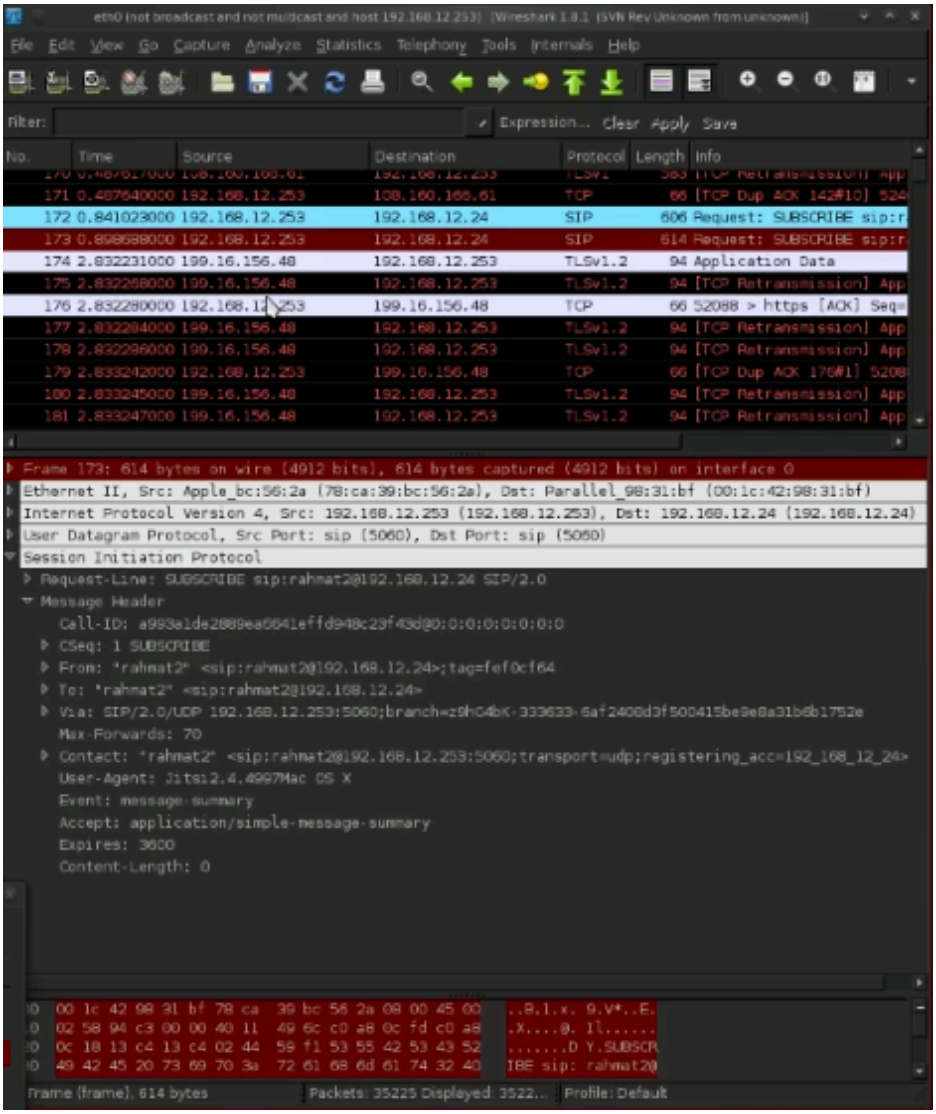
Gambar 4. 12 *Mac Address* setelah *arp spoofing*

3. Setelah ARP *Spoofing* berhasil dilakukan, maka selanjutnya melakukan packet sniffing untuk mengetahui paket apa saja yang dikirim atau diterima oleh target. Buka *wireshark* lalu pilih menu *Capture* lalu *Options*, lalu akan muncul daftar interface. Klik 2 kali pada *interface* eth0 yang memiliki IP *Address* 192.168.12.54 maka akan muncul jendela *Interface Settings*
4. Pada jendela *Interface Settings*, agar paket yang dipantau hanya yang memiliki tujuan ke komputer User B (IP Address 192.168.12.253), maka pada bagian *Capture Filter* diisi dengan aturan ***not broadcast and not multicast and host 192.168.12.253***. Klik Ok



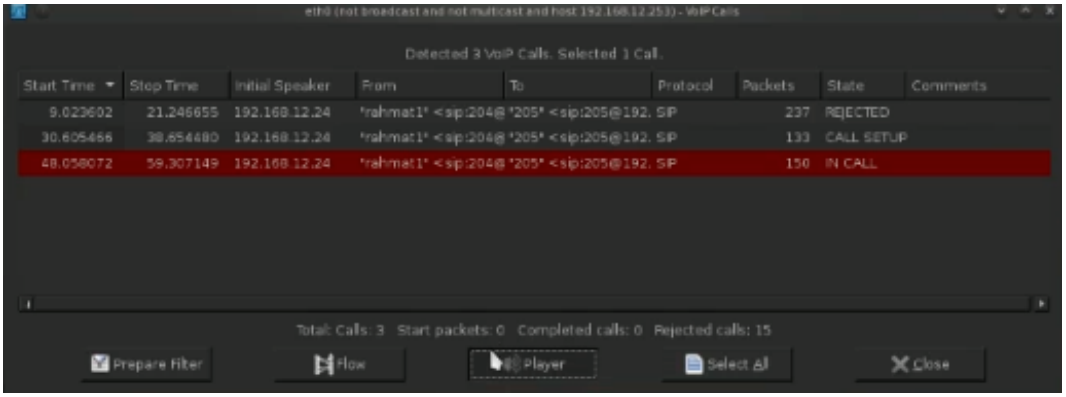
Gambar 4. 13 *Interface Settings*

5. Pilih menu *Capture* lalu *Start* untuk memulai proses *packet sniffing*. Proses ini dilakukan ketika proses komunikasi VoIP berlangsung sampai dengan selesai. Saat komunikasi VoIP berlangsung akan terlihat paket SIP dan RTP pada jendela *wireshark* seperti pada Gambar 4. 14 Proses *Packet Sniffing*



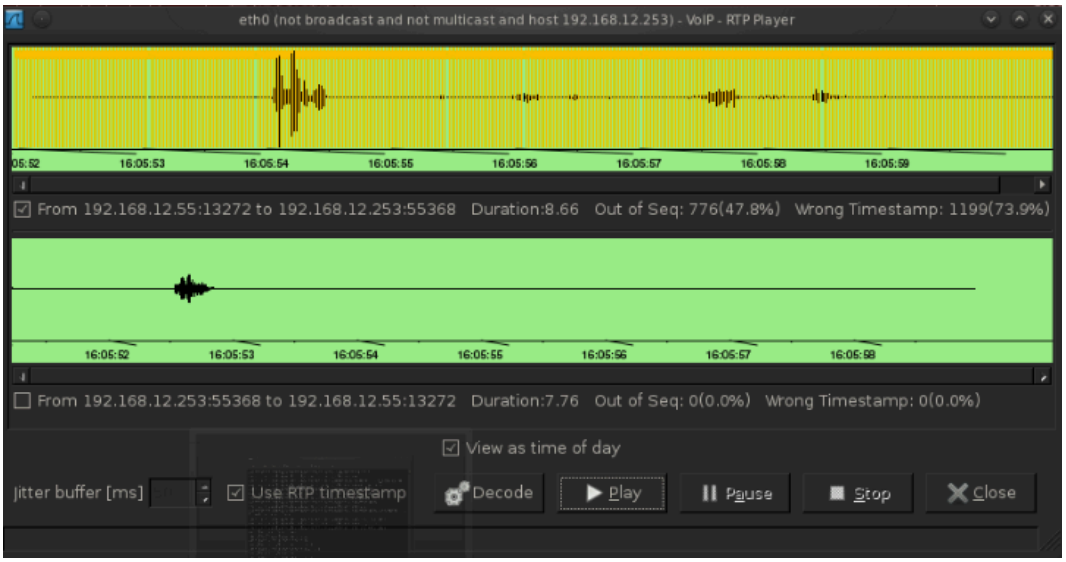
Gambar 4. 14 Proses *Packet Sniffing*

6. Ketika pada jendela wireshark tidak menampilkan lagi paket RTP atau SIP, dapat disimpulkan komunikasi VoIP telah selesai. Selanjutnya adalah mendecode paket RTP dengan memilih menu *Telephony* lalu *Voip Calls* . *Wireshark* akan menampilkan komunikasi VoIP yang terdeteksi seperti pada Gambar 4. 15



Gambar 4. 15 Daftar Komunikasi VoIP

7. Pilih komunikasi VoIP, lalu klik tombol "Player" untuk mendengarkan audio dari komunikasi yang berlangsung maka akan muncul jendela RTP *Player* seperti pada Gambar 4. 16 RTP Player



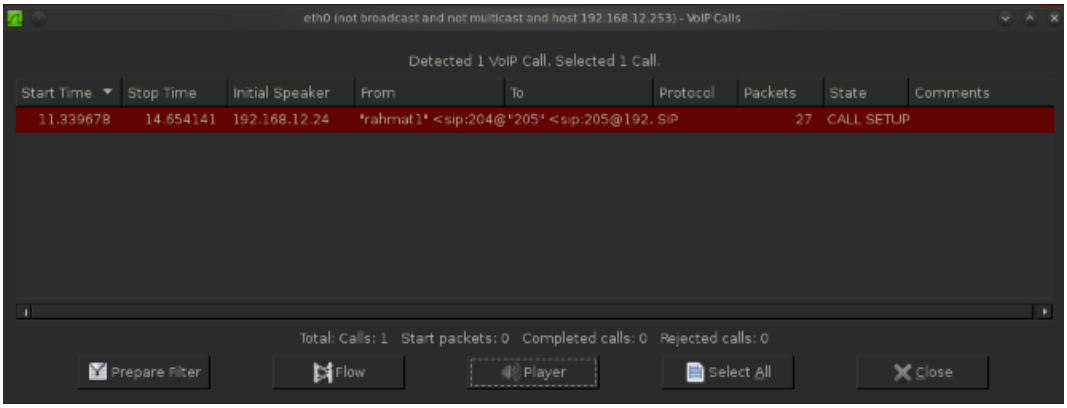
Gambar 4. 16 RTP Player

8. Pada jendela RTP *Player*, klik play untuk mendengarkan audio.

4.2.2.2 Pengujian Pada Saat Komunikasi Berlangsung

Pengujian pada skenario ini memiliki langkah yang sama dengan pengujian pada sistem VoIP tanpa pengamanan ZRTP. Perbedaan terdapat pada waktu pengujian menggunakan *arp spoofing* dan *packet sniffing*. Hasil yang

diperoleh, komunikasi dapat terdeteksi oleh penyerang seperti terlihat pada Gambar 4. 17 Pendeteksian Komunikasi VoIP



Gambar 4. 17 Pendeteksian Komunikasi VoIP

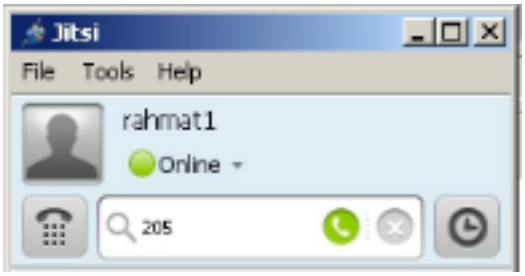
4.2.3 Pengujian VoIP *Server* dengan pengamanan ZRTP

Pengujian VoIP *server* yang sudah diamankan dengan ZRTP menggunakan metode dan tools yang serupa dengan pengujian VoIP *Server* tanpa pengamanan pada sub bab 4.2.2. Langkah yang dilakukan juga sama yang membedakan pada bagian ini adalah waktu mulai proses *packet sniffing*.

4.2.3.1 Pengujian sebelum komunikasi VoIP

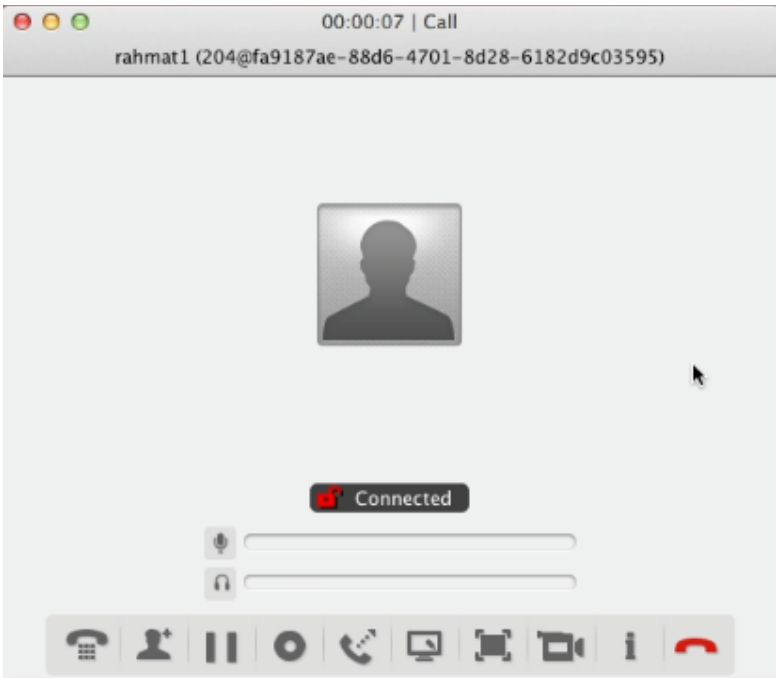
Pada skenario ini pengujian dilakukan sebelum komunikasi VoIP berlangsung. Langkah melakukan *arp spoofing* dan *packet sniffing* sama seperti yang dijelaskan pada sub bab 4.2.2 hanya waktu pelaksanaan *packet sniffing* yang berbeda, berikut langkahnya

1. Pada jendela *wireshark*, klik *Capture* lalu *Start* untuk memulai *packet sniffing*
2. Pada komputer User A, lakukan panggilan ke user B dengan mengisi SIP ID user B pada field *Enter Name or Number* di aplikasi *Jitsi* dan klik tombol *Call* seperti pada Gambar 4. 18 Panggilan pada *Jitsi*

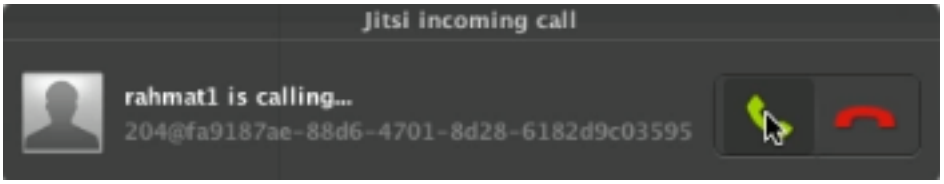


Gambar 4. 18 Panggilan pada *Jitsi*

3. Pada komputer *User* B akan muncul panggilan dari User A, terima panggilan dengan mengklik icon telephone yang berwarna hijau seperti pada Gambar 4. 20 Menerima Panggilan dan mulai perbincangan. Pada tahap ini, tidak muncul SAS terlihat dari tanda ikon gembok yang berwarna merah menandakan pengamanan ZRTP tidak terjadi seperti pada Gambar 4. 19 Panggilan tidak aman.

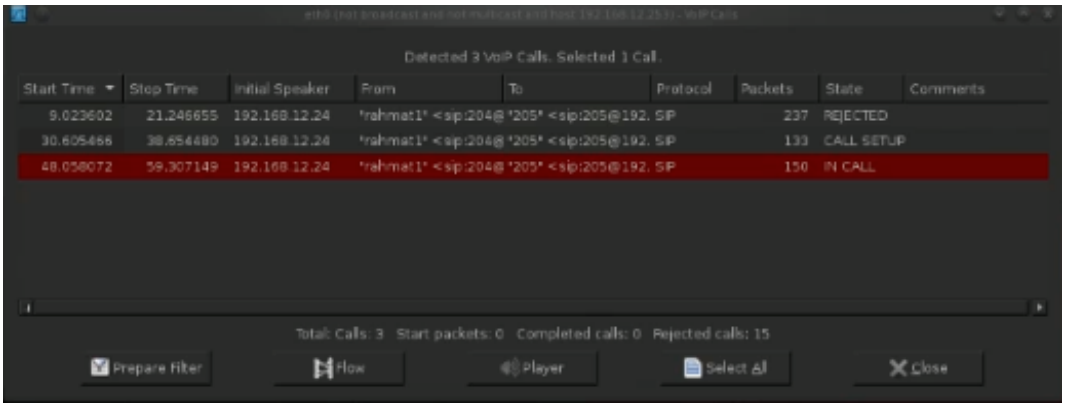


Gambar 4. 19 Panggilan tidak aman

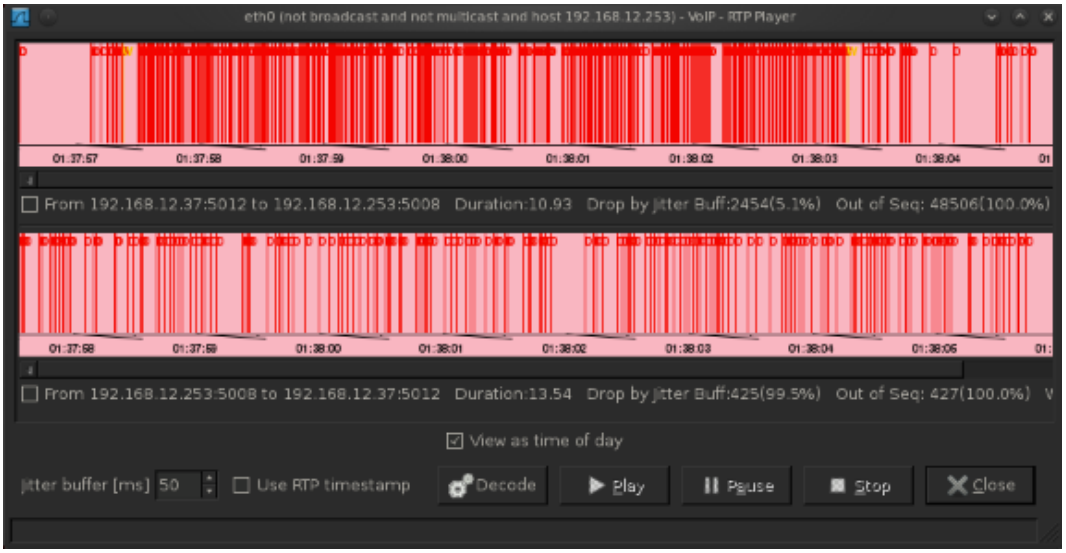


Gambar 4. 20 Menerima Panggilan

4. Akhiri panggilan dengan mengklik icon *telephone* yang berwarna merah.
5. Lalu kembali ke jendela *wireshark* untuk menghentikan proses *packet sniffing* dengan mengklik menu *Capture* lalu *Stop*.
6. Selanjutnya klik menu *Telephony* lalu pilih VoIP *Calls* untuk melihat komunikasi voip yang terdeteksi oleh *wireshark* seperti ditampilkan pada Gambar 4. 21. Komunikasi voip berhasil terdeteksi karena pengamanan ZRTP tidak berjalan. Hasil decode dari komunikasi VoIP terlihat pada Gambar 4. 22 Hasil decode VoIP



Gambar 4. 21 Mendeteksi VoIP

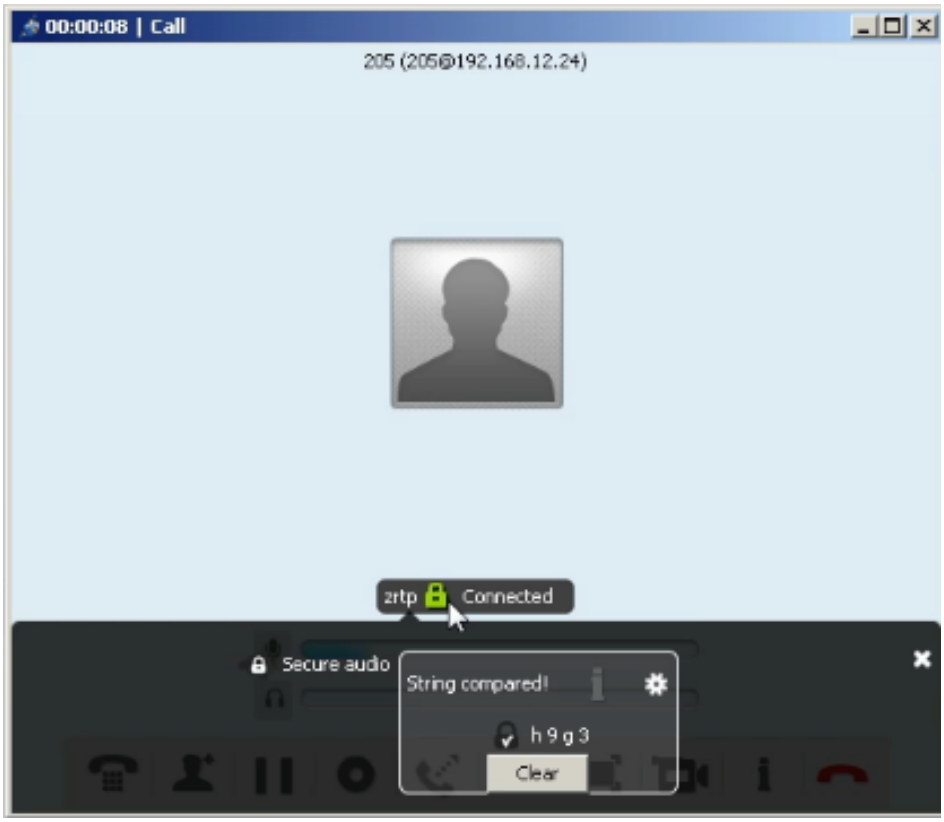


Gambar 4. 22 Hasil decode VoIP

4.2.3.2 Pengujian pada saat komunikasi VoIP berlangsung

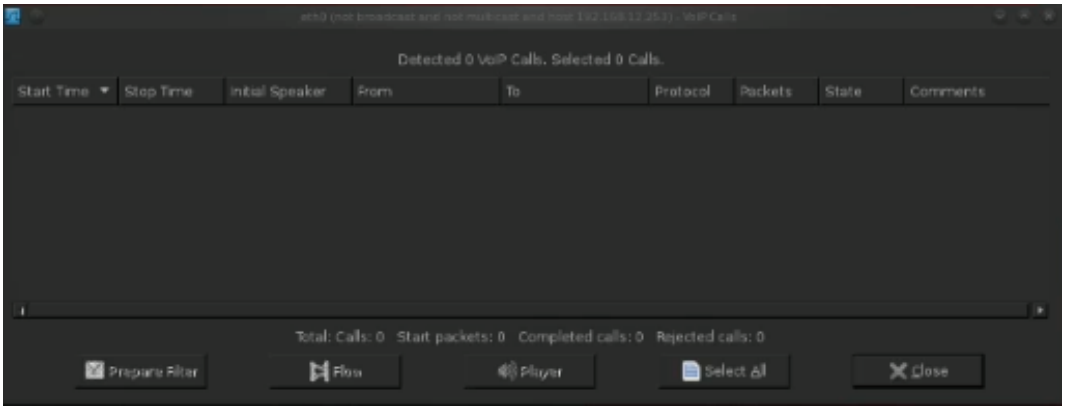
Pengujian pada skenario dilakukan dengan menggunakan metode dan tools yang sama pada sub bab 4.2.2. Pada skenario ini, proses packet sniffing dilakukan saat komunikasi VoIP berlangsung. Berikut langkahnya

1. Pada komputer *User* A, lakukan panggilan ke *user* B dengan mengisi SIP ID *user* B pada *field Enter Name or Number* di aplikasi *Jitsi* dan klik tombol *Call* seperti pada Gambar 4. 18
2. Pada komputer *User* B akan muncul panggilan dari *User* A, terima panggilan dengan mengklik icon telephone yang berwarna hijau seperti pada Gambar 4. 20 dan mulai perbincangan. Pada tahap ini, muncul SAS yang menandakan pengamanan ZRTP terjadi.
3. Nilai SAS antara *User* A dan *User* B akan dibandingkan, ketika sesuai maka akan tampil status *ZRTP Connected* seperti pada Gambar 4. 23



Gambar 4. 23 Tampilan SAS

4. Pada jendela *wireshark*, klik *Capture* lalu pilih *Start* untuk memulai *packet sniffing*
5. Akhiri panggilan dengan mengklik icon telephone yang berwarna merah.
6. Lalu kembali ke jendela *wireshark* untuk menghentikan proses *packet sniffing* dengan mengklik menu *Capture* pilih *Stop*.
7. Selanjutnya klik menu *Telephony* lalu pilih VoIP *Calls* untuk melihat komunikasi voip yang terdeteksi oleh *wireshark* seperti ditampilkan pada Gambar 4. 24.



Gambar 4. 24 Komunikasi VoIP tidak terdeteksi

4.2.4 Hasil Pengujian

Hasil pengujian pada penelitian ini diperoleh berdasarkan pengujian yang telah dilakukan berdasarkan skenario pada Tabel 4. 4 Skenario Pengujian VoIP. Hasil pengujian terdiri dari pengujian komunikasi voip, penyadapan dan pengamanan ZRTP yang ditampilkan pada Tabel 4. 5 Hasil Pengujian.

Tabel 4. 5 Hasil Pengujian

No	Skenario Pengujian	Komunikasi VoIP	Percobaan Penyadapan	Pengamanan ZRTP
1	Sistem VoIP tanpa Pengamanan	Berhasil	Berhasil	-
2	Sistem VoIP tanpa Pengamanan	Berhasil	Berhasil	-
3	Sistem VoIP dengan ZRTP sebelum percakapan	Berhasil	Berhasil	Tidak Berfungsi
4	Sistem VoIP dengan ZRTP pada saat percakapan	Berhasil	Tidak Berhasil	Berfungsi