# Analisis Qos (Quality Of Service) Pada Jaringan Voip Dengan Menggunakan Protokol VPN Sebagai Keamanan Jaringan

## *Qos (Quality Of Service) Analysis On VoIP Network By Using VPN Protocol As Network Security*

**M.Fatkhur Rohman[1)], Triawan Adi Cahyanto[2)]**
[1]Mahasiswa Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jember
email: aefatur@gmail.com
[2] Dosen Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jember
email: triawanac@unmuhjember.ac.id

**Abstrak**

Teknologi internet terus berkembang, sampai sekarang pemanfaatan teknologi tersebut masih sebatas penggunaan untuk hiburan, sebenarnya teknologi ini bisa dimanfaatkan untuk aplikasi yang berguna. Salah satunya pemanfatan teknologi VoIP (Voice over Internet Protocol). Namun kualitas suara pada teknologi VoIP sangat dipengaruhi oleh Quality of Service (QoS) Apabila paket dari voice mengalami proses yang lama (delay) untuk sampai ke tujuan, maka dapat merusak kualitas voice yang terdengar. Selain itu dari segi keaman saat melakukan komunikasi VoIP dibilang masi kurang baik. Maka Pada penelitian ini, membahas Berapa nilai QoS delay, Throughput dan packet loss untuk mengetahui kualitas jaringan dan bagaimana tingkat keamanan jaringan VoIP dengan menggunakan protokol VPN, berikut hasil analisis Nilai QoS dengan 6 kali pengujian rentang waktu 1-6 menit di dapat nilai rata-rata Delay 7,758 ms 7,657 ms, dan 299 bps, 210 bps, dan Packet loss 0%, 0%. Analisis keamanan VoIP dengan menggunakan dua sekenario pengujian di dapat data VoIP antara dua client yang sama-sama terhubung dengan VPN Attacker hanya dapat mensecan IP dan Mac addressnya saja, namun tidak dapat merekam atau mendengarkan percakapan antara client yang saling komunikasi, dan sekenario kedua salah satu client terhubung dengan VPN Attacker dapat mensecan IP dan Mac Addressnya namun tidak hanya dua perangkat itu yang tersecan IP dan Mac addressnya, Dan Attacker dapat merekam atau mendengarkan percakaapan anatara dua client tersebut, namun percakapan yang terekam hannya singkat.

***Kata Kunci :*** *VoIP, VPN (Virtual Private Network), QoS, Delay, Throughput, Packet loss.*

***Abstract***

*Internet technology continues to develop, until now the use of this technology is still limited to use for entertainment, in fact this technology can be used for useful applications. One of them is using VoIP (Voice over Internet Protocol) technology. However, voice quality in VoIP technology is strongly influenced by Quality of Service (QoS). In addition, in terms of security when doing VoIP communication, it's still not good. So in this study, discussing the value of QoS delay, Throughput and packet loss to determine the quality of the network and how the security level of VoIP networks using the VPN protocol, following the results of the analysis of the QoS value with 6 times of testing in a time span of 1-6 minutes, the average value is obtained. average delay is 7,758 ms, 7,657 ms, and 299 bps, 210 bps, and packet loss is 0%, 0%. VoIP security analysis using two test scenarios, VoIP data can be obtained between two clients who are both connected to the VPN Attacker can only scan the IP and Mac addresses, but cannot record or listen to conversations between clients communicating with each other, and in the second scenario one of the the client connected to the VPN Attacker can scan the IP and Mac Address but not only the two devices are scanned for the*

*IP and Mac address, and the Attacker can record or listen to the conversation between the two clients, but the recorded conversation is only short.*

*Keywords: VoIP, VPN (Virtual Private Network), QoS, Delay, Throughput, Packet loss.*

## 1. PENDAHULUAN

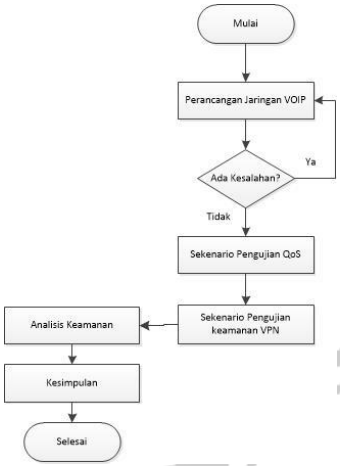
Teknologi internet terus berkembang, sampai sekarang pemanfaatan teknologi tersebut masih sebatas penggunaan untuk hiburan, sebenarnya teknologi ini bisa dimanfaatkan untuk aplikasi yang berguna. Salah satunya pemanfatan teknologi VoIP (Voice over Internet Protocol). VoIP adalah teknologi yang memungkinkan percakapan suara melalui media jaringan komputer (Patih,2012). VoIP menawarkan alternatif komunikasi yang berbeda dengan komunikasi Telpon tradisional, perbedaannya terdapat pada infrastruktur nya, jika VoIP saat berkomunikasi menggunakan jaringan komputer, sedangkan telpon tradisional menggunakan infrastruktur yang dibangun oleh perusahaan telpon konvensional (sugeng, 2008), dan meskipun saat ini komunikasi jarak jauh bisa menggunakan telpon tradisional, tetapi panggilan telpon di indonesia biayanya masih relatif mahal (Sutarti DKK, 2018), apalagi jika terpisah jarak yang cukup jauh maka semakin mahal pula biaya yang di perlukan dalam melakukan komunikasi. Apalagi jika seseorang akan melakukan panggilan kenomor interlokal atau lintas operator biayanyapun tentunya akan semakin mahal. Tetapi dengan berkembangnya internet hal tersebut dapat sedikit diatasi, dengan memanfatkan VoIP (Voice over Internet Protocol). Namun kualitas suara pada teknologi VoIP sangat dipengaruhi oleh Quality of Service (QoS) yaitu delay, Throughput dan packet loss, Apabila paket dari voice mengalami proses yang lama (delay) untuk sampai ke tujuan, maka dapat merusak kualitas voice yang terdengar. Selain itu, besarnya Throughput dan packet loss juga berpengaruh terhadap kualitas dari VoIP itu sendiri (Eko Budi Setiawan,2012)

Hal ini memungkinkan penulis untuk menerapkan teknologi VoIP Untuk menghadapi tantangan perubahan Teknologi Informasi dan Komunikasi, dengan semakin luasnya jaringan internet di indonesia VoIP bisa dijadikan sebagai alternatif komunikasi yang murah. Maka perlu dibuat suatu perancangan sistem yang menggunakan teknologi VoIP yang dapat berkomunikasi sebagai telpon yang umum digunakan. Teknologi ini diharapkan dapat menjadi langkah awal untuk menerapkan teknologi komunikasi yang dapat diintegrasikan dengan jaringan lokal dan dapat mengelola sendiri sarana prasarana komunikasinya, serta kualitas suara dapat di lihat dengan mengukur parameter QoS yaitu Delay, Throughput, dan packet loss untuk mengetahui tingkat kualitas suara yang di hasilkan saat client melakukan komunikasi.

Dan dikarnakan teknologi VoIP bersifat free atau tidak berbayar sangat menguntungkan bagi penggunanya, Maka penggunaan komunikasi yang murah dari segi keamanan kurang begitu diperhatikan (Laurentinus, 2015). Oleh karena itu keamanan saat melakukan komunikasi suara merupakan suatu hal yang sangat penting. (Amarudin,DKK. 2014) Banyak sekali ancaman serangan yang dapat dengan mudah menyadap, mengalihkan, dan bahkan membajak panggilan VoIP, Salah satunya serangan yang mengancam protokol dan sisitem VoIP adalah serangan MITM (Man in the Middle Attack). MITM merupakan suatu serangan yang dimana attacker berada ditengah bebas mendengarkan percakapan antara dua pihak. maka untuk mengatasi serangan MITM di jaringan VoIP, di perlukan VPN (Virtual Private Network) untuk mengamankan lalu lintas data pada jaringan, VPN merupakan salah satu alternatif untuk mengirimkan packet data voice yang bersifat private atau aman (Domiko F.J.P,DKK.2012).

## 2. METODE PENELITIAN

Metode penelitian adalah suatu proses ilmiah untuk mendapatkan data yang akan digunakan untuk keperluan penelitian, diharapkan metode dalam pengerjaan tugas akhir ini sesui dengan tujuan dan keinginan penulis, berikut diagram alur penelitian tugas akhir ini :



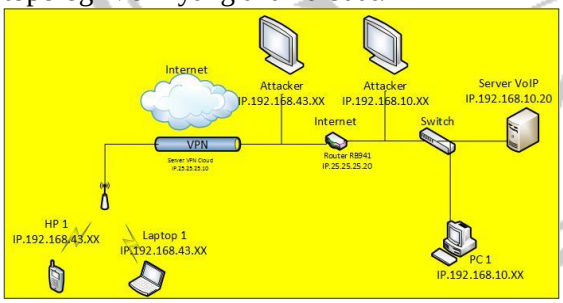

**Gambar 1** Diagram Aliran Penelitian
Sumber: Laurentinus. (2015).

**a. Perancangan Topologi VOIP**

Pada perancangan Topologi VoIP ini ada beberapa komponen yang di gunakan untuk mendukung penelitian ini agar berjalan dengan lancar seperti apayang di inginkan oleh peneliti, yaitu:

1. Komputer Client
2. Server
3. Smartphone
4. Switch
5. Wireless
6. Router RB941
7. Router Cloud

Perancangan arsitektur jaringan akan membahas topologi jaringan yang dibuat dan di konfigurasi yang meliputi device-device yang akan digunakan terkait konektivitas antar server VoIP dengan device lainnya. Berikut rancangan topologi VoIP yang akan dibuat:




**Gambar 2** Topologi Jaringan
Sumber : Topologi Jaringan penelitian

**b. Implementasi VOIP**

Alat dan bahan yang digunakan pada penelitian ini agar berjalan sesui dengan keinginan adalah, Sistem Operasi Windows & Linux sebagai *client*, *software* trixbox sebagai server, *sistem* VPN PPTP sebagai keamanan jaringan, *wireshark* sebagai tool pengukur *performa* kualitas jaringan VoIP dengan menganalisa QoS, Softphone sebagai aplikasi telpon yang di install di client, *cain and abel* sebagai tool penguji kemanan jaringan VoIP.

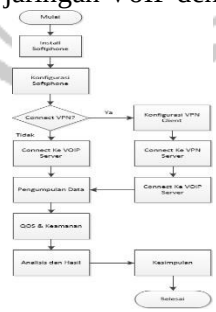
Pada penelitian ini dilakukan pengukuran terhadap parameter QoS yang memengaruhi kualitas suara saat VoIP Melakukan komunikasi yaitu, *Delay*, *Throughput*, *Packet loss* dan pengukuran kaualitas kemanan VPN dari serangan MITM pada jaringan VoIP.

Adapun skema pengujian yang dilakukan pada penelitian ini adalah sebagai berikut:

1. Laptop 1 melakukan panggilan kepada HP 1 selama 6 kali pemanggilan dengan rentang waktu 1 – 6 menit
2. 2. PC 1 melakukan panggilan kepada HP 1 selama 6 kali pemanggilan dengan rentang waktu 1 – 6 menit
3. 3. Mencari Nilai kualitas jaringan VoIP dengan QOS, parameter yang di guanakan Delay, Throuhput, Packet loss, dengan menggunakan tool quality monitoring yaitu Wireshark, selama 6 kali proses pemanggilan dengan rentang waktu 1-6 menit.
4. PC Attacker melakukan attacking bertindak sebagai MITMA (Man In The Middle Attac dengan menjalankan program sniffer atau spoofing, terhadap client yang sedang melakukan komunikasi, Attacing berada di tengah-tengah client yang berkomunukiasi, dengan menggunakan tool cain and abel.

**c. Perancangan Analiss Nilai QoS dan Keamanan VoIP**

Perancangan ini di butuhkan untuk mengatahui kualitas Nilai QoS dan kemanan jaringan VoIP dengan menggunakan VPN



**Gambar 3** Flowchart perancangan Konfigurasi Client dan Analisis Penelitian
Sumber: Laurentinus. (2015).

**d. Pengujian dan Analisis**

Dalam penelitian ini diuji pula koneksi antar client yang saling terhubung. Pengujian di lakukan sebanyak 6 kali, Untuk meningkatkan akurasi, pengamatan dan pengambilan data. Pada tahap ini akan melakukan analisis jaringan VoIP, Analisa pengujian dilakukan dengan cara melakukan pengukuran parameter *delay, Throughput dan packet loss* dengan menggunakan *Wireshark* sebagai network analizer.

**1. *Delay***

Pengujian parameter *Delay* dilakukan untuk mengetahui kualitas nilai QoS, semakin rendah nilai *Delay* yang di dapat dikatakan sangat Baik, begitu juga sebaliknya semakin tinggi nilai *Delay* yang di dapat maka kualitas sangat Buruk. Proses pengujian ini di lakukan dengan 6 kali percobaan panggilan, dengan rentang waktu 1 – 6 menit. Percobaan pertama Laptop1 melakukan panggilan pada HP1 selama 1 -6 menit, percobaan ke dua PC1 Melakukan panggilan pada HP1 selama 1 – 6 menit, kemudian ditahap akhir di carai nilai rata-rata darai 6 kali percobaan tersebut.

***2. Throughput***

Pengujian parameter *Throughput* dilakukan untuk mengetahui Nilai kecepatan rata-rata dari sebuah paket yang dikirim, semakin rendah nilai *Throughput* yang di dapat dikatakan Buruk, begitu juga sebaliknya semakin tinggi nilai *Throughput* yang di dapat maka kualitas sangat Baik. Proses pengujian ini di lakukan dengan 6 kali percobaan panggilan, dengan rentang waktu 1 – 6 menit. Percobaan pertama Laptop1 melakukan panggilan pada HP1 selama 1 - 6 menit, percobaan ke dua PC1 Melakukan panggilan pada HP1 selama 1 – 6 menit, kemudian ditahap akhir di carai nilai rata-rata darai 6 kali percobaan tersebut.

***3. Packet Loss***

Pengujian parameter *Packet loss* dilakukan untuk mengetahui Nilai QoS, semakin rendah nilai *Packet loss* yang di dapat dikatakan Sangat Baik, begitu juga sebaliknya semakin tinggi nilai *Packet Loss* yang di dapat maka kualitas sangat Buruk. Proses pengujian ini di lakukan dengan 6 kali percobaan panggilan, dengan rentang waktu 1 – 6 menit. Percobaan pertama Laptop1 melakukan panggilan pada HP1 selama 1 -6 menit, percobaan ke dua PC1 Melakukan panggilan pada HP1 selama 1 – 6 menit, kemudian ditahap akhir di carai nilai rata-rata darai 6 kali percobaan tersebut.

**4. Mekanisme Pengujian Keamanan**

Mekanisme pengujian keamanan VPN pada jaringan VoIP dengan serangan MITM pada saat client melakukan komunikasi menggunakan dua kondisi, yaitu: pengujian keamanan pangilan kedua client terhubung dengan VPN dan pengujian keamanan panggilan salah satu client yang terhubung dengan VPN, berikut mekanismenya:

**a) Pengujian Panggilan kedua client terhubung dengan VPN**

Pengujian ini di lakukan dengan cara client saling komunikasi dengan rentang waktu 2-4 menit, yaitu Laptop 1 menghubungi HP1, kemudian komputer *Attacker* melakukan *sniffing* atau melakukan serangan terhadap *client* yang sedang komunikasi, serangat tersebut ingin mengatahui tingkat kemanan VPN pada jaringan VoIP apakah *Attacker* dapat mendengarkan percakapan antara *client* tersebut apa tidak, serangan MITM ini menggunakan *software Cain and abel.*

**b) Pengujian Panggilan salah satu client terhubung dengan VPN**

Pengujian ke dua ini tidak jauh beda dengan pengujian pertama, perbedaan hanya pada client yang melakukan komunikasi, yaitu PC1 menghubungi HP1 dengan rentang waktu 2-4 menit, kemudian komputer *Attacker* melakukan *sniffing* atau melakukan serangan terhadap *client* yang sedang komunikasi, serangat tersebut ingin mengatahui tingkat kemanan VPN pada

jaringan VoIP apakah *Attacker* dapat mendengarkan percakapan antara *client* tersebut apa tidak, serangan MITM ini menggunakan *software Cain and abel.*

## 3. PEMBAHASAN

Pengujian kualitas menggunakan tiga pengukuran *QOS (Quality of Service),* sedangkan keamanannya di uji dengan menggunakan serangan MITM. Aplikasi pendukung yang di gunakan yaitu aplikasi *Wireshark dan cain and abel,* hasil pengujian sebagai berikut:

### a. Mencari Nilai QoS pada Jaringan VoIP

Pengujian analisisi Voip ini menggunakan tiga pengukuran *Quality of service (QoS)* yaitu, *Delay, Throughput* dan *Packet loss,* aplikasi yang di gunakan unutk mencari nilai QoS tersebut adalah *Wireshark.* Berikut ini langkah-langkah mencari nilai QoSnya:

1. Menjalnak sistem VoIP Server yang sudah di seting pada Pc Server
2. Menjalankan Aplikasi Wireshark
3. Client melakukan komunikasi sesui dengan rencana pengujian.

Pada aplikasi *Wireshark* akan terlihat protocol yang sedang bekerja selama proses komunikasi berlangsung, dan untuk mendapatkan nilai *Delay, Throughput, packet loss,* proses captur pada aplikasi *Wireshark* harus di stop terlebih dahulu, berikut hasil kapcer dan perhitungan masing-masing Parameter QoS dengan menggunakan aplikasi *Wireshark*:

#### 1. *Delay*

**Statistics**

| Measurement | Captured | Displayed | Marked |
|---|---|---|---|
| Packets | 9338 | 9338 (100.0%) | – |
| Time span, s | 70.453 | 70.453 | – |
| Average pps | 132.5 | 132.5 | – |
| Average packet size, B | 203 | 203 | – |
| Bytes | 1893750 | 1893750 (100.0%) | 0 |
| Average bytes/s | 26k | 26k | – |
| Average bits/s | 215k | 215k | – |

**Gambar 4.** Halis Capture wireshark
Sumber : Tangkap Layar Wireshark

Dari data yang di dapat dari *Wireshark* maka di dapat Nilai *delay* dengan cara perhitungan sebagai berikut:

*Delay = Total Delay / Paket yang dikirim*
= 70,453 / 9338
= 0,0075s
= 7.5447 ms

#### 2. *Throughput*

Dari data yang di dapat dari *Wireshark* maka di dapat Nilai *Throughput* dengan cara perhitungan sebagai berikut:

*Throughput* = Jumlah data yang dikirim / Waktu pengiriman data
*= 1893750/70,453*
*= 26,879 x 8*
*= 215bps*

#### 3. *Packet Loss*

Dari data yang di dapat dari *Wireshark* maka di dapat Nilai *Packet loss* dengan cara perhitungan sebagai berikut:

*Packet loss* = Paket yang dikirim – paket yang ditrima x 100 % / Paket yang dikirim
= 9338-9338 x 100% / 9338
= 0,0 %

### b. Analisis Nilai QoS pada jaringan VoIP

Analisis nilai QoS pada jaringan VoIP dengan 6 kali pengujian rentang waktu 1 – 6 menit pada pangilan Laptop1 ke HP1 dan PC1 ke HP1, yaitu *Delay, Throughput dan Packet loss,* berkit analisisnya:

#### 1. *Delay*

**Tabel 1** Nilai *Delay* pada panggilan Laptop1 ke HP1

| Percobaan | Waktu | Status | *Delay* (ms) | Keterangan |
|---|---|---|---|---|
| Percobaan 1 | Panggilan selama 1 Menit | Laptop1 menghubungi HP1 | 8,059 ms | Baik |
| Percobaan 2 | Panggilan selama 2 Menit | | 7,511 ms | Baik |
| Percobaan 3 | Panggilan selama 3 Menit | | 7,515 ms | Baik |
| Percobaan 4 | Panggilan selama 4 Menit | | 10,679 ms | Baik |
| Percobaan 5 | Panggilan selama 5 Menit | | 7,085 ms | Baik |
| Percobaan 6 | Panggilan selama 6 Menit | | 5,699 ms | Baik |
| Rata-rata | | | 7,758 ms | Baik |

Sumber : Hasil Perhitungan

Pengertian Tabel diatas, dapat dilihat nilai *Delay* Pada panggilan Laptop1 ke HP1 percobaan ke 1 selama 1 menit didapat nilai 8,059 ms, percobaan ke 2 selama 2 menit didapat nilai 7,511 ms, percobaan ke 3 selama 3 menit didapat nilai 7,515 ms, percobaan ke 4 selama 4 menit didapat nilai 10,679 ms, percobaan ke 5 selama 5 menit didapat nilai 7,085 ms, percobaan ke 6 selama 6 menit didapat nilai 5,699 ms, dari hasil pengujian

selama rentang waktu 1-6 menit di dapatkan nilai rata-rata 7,758 ms dan di katakan Baik.

**Tabel 2** Nilai *Delay* pada panggilan PC1 ke HP1

| Percobaan | Waktu | Status | *Delay* (ms) | Keterangan |
|---|---|---|---|---|
| Percobaan 1 | Panggilan selama 1 Menit | PC1 menghubungi HP1 | 7,545 ms | Baik |
| Percobaan 2 | Panggilan selama 2 Menit | | 7,816 ms | Baik |
| Percobaan 3 | Panggilan selama 3 Menit | | 7,632 ms | Baik |
| Percobaan 4 | Panggilan selama 4 Menit | | 7,600 ms | Baik |
| Percobaan 5 | Panggilan selama 5 Menit | | 7,562 ms | Baik |
| Percobaan 6 | Panggilan selama 6 Menit | | 7,787 ms | Baik |
| Rata-rata | | | 7,657 ms | Baik |

Sumber : Hasil Perhitungan

Pengertian Tabel diatas, dapat dilihat nilai *Delay* Pada panggilan PC1 ke HP1 percobaan ke 1 selama 1 menit didapat nilai 7,545 ms, percobaan ke 2 selama 2 menit didapat nilai 7,816 ms, percobaan ke 3 selama 3 menit didapat nilai 7,636 ms, percobaan ke 4 selama 4 menit didapat nilai 7,600 ms, percobaan ke 5 selama 5 menit didapat nilai 7,562 ms, percobaan ke 6 selama 6 menit didapat nilai 7,787 ms, dari hasil pengujian selama rentang waktu 1-6 menit di dapatkan nilai rata-rata 7,657 ms dan di katakan Baik.

**2. *Throughput***

**Tabel 3** Nilai *Throughput* Pada panggilan Laptop1 ke HP1

| Percobaan | Waktu | Status | *Throughput*(bps) |
|---|---|---|---|
| Percobaan 1 | Panggilan selama 1 Menit | Laptop1 menghubungi HP1 | 239 bps |
| Percobaan 2 | Panggilan selama 2 Menit | | 258 bps |
| Percobaan 3 | Panggilan selama 3 Menit | | 256 bps |
| Percobaan 4 | Panggilan selama 4 Menit | | 178 bps |
| Percobaan 5 | Panggilan selama 5 Menit | | 297 bps |
| Percobaan 6 | Panggilan selama 6 Menit | | 566 bps |
| Rata-rata | | | 299 bps |

Sumber : Hasil Perhitungan

Pengertian Tabel diatas, dapat dilihat nilai *Throughput* Pada panggilan Laptop1 ke HP1 percobaan ke 1 selama 1 menit didapat nilai 239 bps, percobaan ke 2 selama 2 menit didapat nilai 258 bps, percobaan ke 3 selama 3 menit didapat nilai 256 bps, percobaan ke 4 selama 4 menit didapat nilai 178 bps, percobaan ke 5 selama 5 menit didapat nilai 297 bps, percobaan ke 6 selama 6 menit didapat nilai 566 bps, dari hasil pengujian selama rentang waktu 1-6 menit di dapatkan nilai rata-rata 299 bps.

**Tabel 4** Nilai *Throughput* Pada panggilan PC1 ke HP1

| Percobaan | Waktu | Status | *Throughput*(bps) |
|---|---|---|---|
| Percobaan 1 | Panggilan selama 1 Menit | PC1 menghubungi HP1 | 215 bps |
| Percobaan 2 | Panggilan selama 2 Menit | | 206 bps |
| Percobaan 3 | Panggilan selama 3 Menit | | 210 bps |
| Percobaan 4 | Panggilan selama 4 Menit | | 212 bps |
| Percobaan 5 | Panggilan selama 5 Menit | | 212 bps |
| Percobaan 6 | Panggilan selama 6 Menit | | 206 bps |
| Rata-rata | | | 210 bps |

Sumber : Hasil Perhitungan

Pengertian Tabel diatas, dapat dilihat nilai *Throughput* Pada panggilan PC1 ke HP1 percobaan ke 1 selama 1 menit didapat nilai 215 bps, percobaan ke 2 selama 2 menit didapat nilai 206 bps, percobaan ke 3 selama 3 menit didapat nilai 210 bps, percobaan ke 4 selama 4 menit didapat nilai 212 bps, percobaan ke 5 selama 5 menit didapat nilai 212 bps, percobaan ke 6 selama 6 menit didapat nilai 206 bps, dari hasil pengujian selama rentang waktu 1-6 menit di dapatkan nilai rata-rata 210 bps.

**3. *Packet Loss***

**Tabel 5** Nilai *Packet loss* Pada panggilan Laptop1 ke HP1

| Percobaan | Waktu | Status | *Packet loss* (%) | Keterangan |
|---|---|---|---|---|
| Percobaan 1 | Panggilan selama 1 Menit | Laptop1 menghubungi HP1 | 0 % | Sangat Baik |
| Percobaan 2 | Panggilan selama 2 Menit | | 0 % | Sangat Baik |
| Percobaan 3 | Panggilan selama 3 Menit | | 0 % | Sangat Baik |
| Percobaan 4 | Panggilan selama 4 Menit | | 0 % | Sangat Baik |
| Percobaan 5 | Panggilan selama 5 Menit | | 0 % | Sangat Baik |
| Percobaan 6 | Panggilan selama 6 Menit | | 0 % | Sangat Baik |
| Rata-rata | | | 0 % | Sangat Baik |

Sumber : Hasil Perhitungan

Pengertian Tabel diatas, dapat dilihat nilai *Packet loss* Pada panggilan Laptop1 ke HP1 percobaan ke 1 selama 1 menit didapat nilai 0%, percobaan ke 2 selama 2 menit didapat nilai 0%, percobaan ke 3 selama 3 menit didapat nilai 0%, percobaan ke 4 selama 4 menit didapat nilai 0%,

percobaan ke 5 selama 5 menit didapat nilai 0%, percobaan ke 6 selama 6 menit didapat nilai 0%, dari hasil pengujian selama rentang waktu 1-6 menit di dapatkan nilai rata-rata 0%, dan di katakan sangat Baik.

**Tabel 6** Nilai *Packet loss* Pada panggilan PC1 ke HP1

| Percobaan | Waktu | Status | *Packet loss* (%) | Keterangan |
|---|---|---|---|---|
| Percobaan 1 | Panggilan selama 1 Menit | PC1 menghubungi HP1 | 0 % | Sangat Baik |
| Percobaan 2 | Panggilan selama 2 Menit | | 0 % | Sangat Baik |
| Percobaan 3 | Panggilan selama 3 Menit | | 0 % | Sangat Baik |
| Percobaan 4 | Panggilan selama 4 Menit | | 0 % | Sangat Baik |
| Percobaan 5 | Panggilan selama 5 Menit | | 0 % | Sangat Baik |
| Percobaan 6 | Panggilan selama 6 Menit | | 0 % | Sangat Baik |
| Rata-rata | | | 0 % | Sangat Baik |

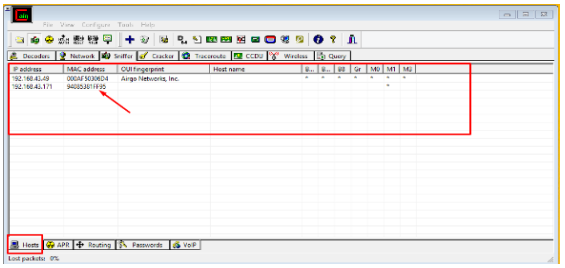
Sumber : Hasil Perhitungan

Pengertian Tabel diatas, dapat dilihat nilai *Packet loss* Pada panggilan PC1 ke HP1 percobaan ke 1 selama 1 menit didapat nilai 0%, percobaan ke 2 selama 2 menit didapat nilai 0%, percobaan ke 3 selama 3 menit didapat nilai 0%, percobaan ke 4 selama 4 menit didapat nilai 0%, percobaan ke 5 selama 5 menit didapat nilai 0%, percobaan ke 6 selama 6 menit didapat nilai 0%, dari hasil pengujian selama rentang waktu 1-6 menit di dapatkan nilai rata-rata 0%, dan di katakan sangat Baik.

**4. Analisis *Keamanan* VOIP**

Analisis keamanan VoIP ini dilakukan dengan dua cara pengujian agar di dapat perbedaan kualitas keamanan VPN dari serangan MITM, yaitu kedua client terhubung dengan VPN dan salah satu client terhubung dengan VPN, kemudian di uji keamanan dengan melakukan serangan MITM menggunakan software *cain and abel*. Skema pengujiannya clien 1 menghubungi client 2 dan Attacker berada di tengah-tengah antara clien1 dan clien 2, Adapun analisis keamanannya menggunkan software *cain and abel* sebagai berikut:

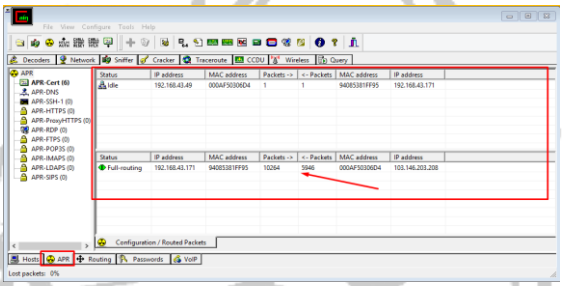
**a) Pengujian Panggilan kedua client terhubung dengan VPN**



**Gambar. 5** Proses *scanning Mac address client* Laptop1 ke HP1

Sumber : Tangkap layar hasil penelitian

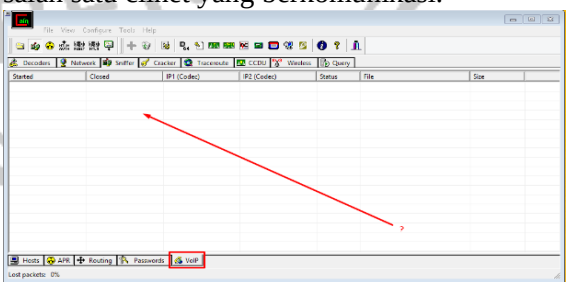
Pengertian Gambar diatas, menunjukkan bahwa *Attacker* dapat melakukan scanning terhadap *client* yang sedang melakukan komunikasi, di tunjukkan dengan *Attacker* dapat melihat IP dan *MAC address client* tersebut.



**Gambar 6** Proses *Arpspoofing* Laptop1 ke HP1

Sumber : Tangkap layar hasil penelitian

Pengertian Gambar diatas menunjukkan bahwa *attacker* berhasil melakukan *Arpspoofing* terhadap *client* yang sedang melakukan komunikasi. Pada tahap ini *attacker* akan bertindak sebagai MITM. Namun pada pengujian dengan menggunakan VPN *Attacker hanya dapat* melihat jumlah packet data yang di kirim, tidak dapat melakukan serangan dengan mengirimkan *mac address* miliknya kepada salah satu clinet yang berkomunikasi.



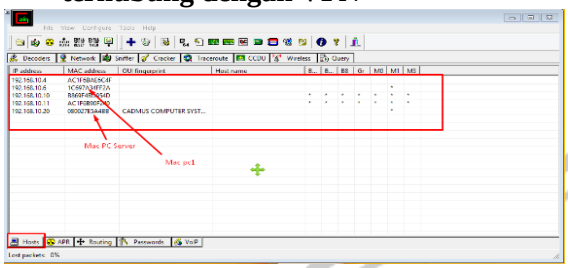
**Gambar 7** VoIP *Recording* Laptop1 ke HP1

Sumber : Tangkap layar hasil penelitian

Pengertian Gambar diatas menunjukkan bahwa *Attacker* tidak dapat merekam atau

mendengarkan percakapan client yang sedang melakukan komunikasi.

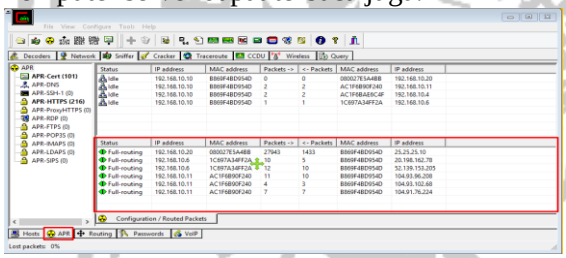
**b) Pengujian pangilan salah satu client terhubung dengan VPN**




**Gambar 8** Proses *scanning Mac address client* PC1 ke HP1

Sumber : Tangkap layar hasil penelitian

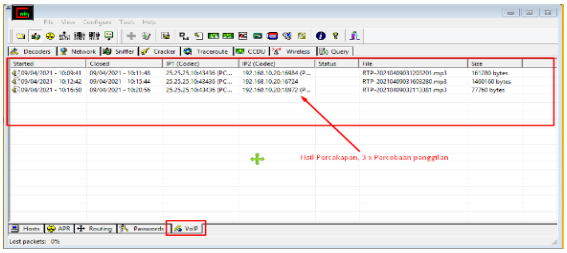
Pengujian keamanan hanya menggunakan satu client saja yang terhubung dengan VPN dan client satunya tidak terhubung dengan VPN. pada proses *scanning mac address attacker* dapat melihat IP dan *Mac address* lebih banyak dari pada proses yang pertama. Di karnakan *Software Cain and abel* dapat membaca perangkat-perangkat local yang saling terhubung, salah satunya IP dan *Mac address* komputer server dapat terbaca juga.



**Gambar 8** Proses *Arpspoofing* PC1 ke HP1

Sumber : Tangkap layar hasil penelitian

Pengertian Gambar diatas menunjukkan bahwa *attacker* berhasil melakukan *Arpspoofing* terhadap *client* yang sedang melakukan komunikasi, pada tahap ini *attacker* akan bertindak sebagai MITM yang akan mengirimkan *mac address* miliknya kepa salah satu *client* yang berkomunikasi dan akan menyebabkan *client* tersebut dibanjiri *spoofing mac address. Client* pun akan beranggapan bahwa *mac address* dari *attacker* tersebut sah. Hal ini membuktikan nahwa sistem VoIP standar tidak memiliki perlindungan terhadap aspek kerahasiaan dan kepercayaan data dari serangan *Main in The Middle* (MITM)




**Gambar 9** VoIP *Recording* PC1 ke HP1

Sumber : Tangkap layar hasil penelitian

Pengertian Gambar diatas pada percobaan panggilan 3 kali *Attacker* dapat merekam dan mendengarkan percakapan client yang melakukan komunikasi, namun hasil rekaman yang di dapat tidak sama dengan waktu panggilan client tersebut yang berarti hasil trekaman yang di dapat tidak utuh 100%. menunjukkan bahwa *Attacker* berhasil mendapatkan percakapan client yang sedang melakukan komunikasi.

## 4. KESIMPULAN

Dari skenario pengujian QoS dan mengetahui tingkat keamanan jaringan VoIP dengan Menggunakan Protocol VPN dapat disimpulan sebagi berikut:

a. Nilai QoS dengan 6 kali pengujian rentang waktu 1-6 menit di dapat nilai rata-rata *Delay* 7,758 ms 7,657 ms, dan 299 bps, 210 bps, dan *Packet loss* 0%, 0%.

b. Analisis keamanan VoIP dengan menggunakan dua sekenario pengujian di dapat data VoIP antara dua *client* yang sama-sama terhubung dengan VPN *Attacker* hanya dapat mensecan IP dan Mac addressnya saja, namun tidak dapat merekam atau mendengarkan percakapan antara client yang saling komunikasi, dan sekenario kedua salah satu client terhubung dengan VPN *Attacker* dapat mensecan IP dan Mac Addressnya namun tidak hanya dua perangkat itu yang tersecan IP dan Mac addressnya, Dan *Attacker* dapat merekam atau mendengarkan percakaapan anatara dua client tersebut, namun percakapan yang terekam hannya singkat.

## 5. REFERENSI


Ahmad, F. (2011). *Uji Kemanan Sistem Komunikasi VoIP dengan Pemanfaatan Fasilitas Enkripsi Pada Open VPN*, Universitas Syarif Hidaytullah Jakarta.

Abdoe R.S,(2017). *Analisis Kinerja VoIP Open Source FreePBX Asterisk Menggunakan Metode MOS- E-Model (ITU-T.G.107).*Universitas Muhammadiyah Jember

Anjar, S. (2013). *Analisis Simulasi Mobile VoIP (Voice Over Internet Protocol) Berbasis SIP(Session Initiaton Protocol) Pada jaringan Wireless digedung FTI UKSW,* Universitas Kristen Satya Wacana Salatiga.

Amarudin, DKK (2014). *Analisis keamanan jaringan single sign on (sso) Dengan lightweight directory access protocol (ldap) Menggunakan metode MITMA*.Universitas Gadjah Mada Yogyakarta.

Ari, P.W. (2017). *Optimasi Jaringan Local Are Network Menggunakan VLAN dan VOIP*,Universitas Widyatama.

DomikoF.J.P, DKK. (2012), *Analisa perancangan server voip (voice internet protocol) Dengan opensource asterisk dan vpn (virtual privatenetwork) Sebagai pengaman jaringan antar client,* Universitas Lampung.

Eko, B.S. (2012), *Analisa quality of services (QOS) voice over interneProtocol (VoIP) dengan protokol h.323 dan session Initial protocol (sip),* Program Studi Teknik Informatika UNIKOM Bandung.

Hari R, Bowo N, (2012). *Analisis implementasi keamanan jaringan virtual Private network (VPN) pada Pt. Layar sentosa shipping corporation*, Universitas Dian Nuswantoro

Harun sujadi, Aqis Mutaqin. (2017), *Rancang Bangun Arsitektur Jaringan Komputer Teknologi Metropolitan Area Network (Man) Dengan Menggunakan Metode Network Development Life Cycle (Ndlc).*Universitas Majalengka

Junaedi A.P,DKK (2017). *Investigasi Performa VoIP Pada jaringan Wireless dengan menggunakan server Elastix*. Politeknik Negri Banyuwangi

Laurentinus (2015), *Rancang bangun server voisce over internet Protocol (VOIP) dengan pengamanan virtual Private network (VPN) studi kasus Stmik Atma Luhur*, Teknik Informatika Stmik Atma Luhur Pangkalpinang.