Analisis *Data Digital Evidence* pada Layanan *Voice Over Internet Protocol* (*VoIP*)

Muhamad Arsad Adam[#1], Nur Widiyasono[*2], Husni Mubarok[#3]

[#] *Program Studi Teknik Informatika, Fakultas Teknik, Universitas Siliwangi*
Jl. Siliwangi No. 24 Tasikmalaya Kotak Pos 164 Telp. (0265) 323537
[1]muhamad.arsad@student.unsil.ac.id
[3]husni.mubarok@unsil.ac.id
[2]nur.widiyasono@unsil.ac.id

Abstrak— Teknologi VoIP (Voice Over Internet Protocol) merupakan teknologi yang mampu melewatkan panggilan suara, video dan data dalam jaringan IP. Voice over Internet Protocol (VoIP) dalam teknologi komunikasi cukup signifikan sehingga tidak terlepas dari kejahatan cybercrime, Teknologi VoIP dapat disalahgunakan untuk melakukan tindakan kejahatan jarak jauh sehingga diperlukan langkah-langkah investigasi jika terjadi masalah. Menemukan artefact pada Infrastruktur VoIP merupakan tantangan tersendiri. WireSharks salah satu tool yang digunakan dalam investigasi ini. Metode yang digunakan adalah DFIF yang terdiri tahapan adalah Collection, Examination, Analysis, dan Report and Documentation. Investigasi pada layanan VoIP dapat berhasil dilakukan dengan menemukan data digital evidence di layer 5. Tujuan Penelitian ini yaitu Mengetahui Karakteristik Data Digital berupa suara pada layanan Voice Over IP dan Menganalisis Data Digital berupa suara pada layanan Voice Over IP. Hasil dari penelitian ini barang bukti digital yang berupa percakapan yang dapat dipertanggungjawabkan dalam pengadilan..

Kata kunci*— Data, Evidence, Forensik,Network, *VoIP

I. PENDAHULUAN

Kejahatan yang memanfaatkan kemajuan teknologi salah satunya dengan memanfaatkan teknologi *VoIP*. Teknologi *VoIP (Voice Over Internet Protocol)* merupakan teknologi yang mampu melewatkan panggilan suara, video dan data dalam jaringan IP. Bentuk panggilan analog dikonversikan menjadi bentuk digital dan dijalankan sebagai data oleh internet protokol. Jaringan IP sendiri merupakan jaringan komunikasi data yang berbasis packed-switch, sehingga kita bisa menelepon dengan menggunakan jaringan IP atau Internet. Jaringan *VoIP* dapat dibangun dengan menggunakan jaringan nirkabel dan kabel.

Penggunaan teknologi *VoIP* untuk saat ini sangat banyak digunakan, namun dengan banyaknya yang menggunakan teknologi ini banyak juga yang menyalahgunakannya, misalnya untuk kejahatan dalam menipu lewat jaringan *VoIP* ini. Jauh sebelum adanya teknologi *VoIP* kejahatan penipuan dengan menggunakan media telepon konvensional sudah marak dilakukan. Namun dengan seiringnya perubahan jaman maka dengan adanya teknologi *VoIP* yang mempermudah untuk melakukan komunikasi baik itu dari dalam negeri maupun luar negeri.

Kejahatan dalam dunia maya atau internet dikenal dengan sebutan *Cybercrime*. *Cybercrime* adalah kejahatan yang terjadi di Internet / dunia maya yang menjadi alat, sasaran atau tempat terjadinya kejahatan yaitu mengacu pada aktivitas kejahatan dengan komputer atau jaringan komputer.

Kejahatan dalam penggunaan jaringan *VoIP* pada beberapa tahun terakhir ini dilakukan dengan modus penipuan, tercatat pada tahun 2016 terjadi penyalahgunaan jaringan *VoIP* ini yang dilakukan oleh WNA asal Cina, yang memanfaatkan fasilitas yang ada di Indonesia dengan modus berpura – pura sebagai petugas bank yang menginformasikan bahwa masa berlaku kartu kredit telah habis dan jika tidak segera di perpanjang, maka akan ada polisi yang akan mengurusnya.

Merujuk dari beberapa literature dan situs – situs bahwa kejahatan cybercrime ada beberapa jenis kejahatan misalnya penipuan kartu kredit, penipuan bursa efek, penipuan perbankan, pornografi anak, perdagangan narkoba, serta terorisme. Salah satu kejahatan cybercrime yang marak akhir – akhir ini adalah penipuan yang menggunakan jaringan *VoIP* (*Voice Over Internet Protocol*).

Berdasarkan uraian tersebut, maka dilakukan penelitian dengan judul " Analisis Data Digital Evidence pada Layanan Voice Over IP ". Sehingga dapat mengetahui apakah layanan *VoIP* ini aman atau tidak.

Batasan masalah pada penelitian ini yaitu : Simulasi kasus dilakukan dengan menggunakan jaringan *LAN* dengan menggunakan server *Trixbox*, *Tools* yang digunakan dalam penelitian ini adalah *Wireshark* dan *X-Lite* sebagai Softphone, Penelitian tidak membahas proses digital forensik secara keseluruhan dari awal kasus hingga penutupan kasus, hanya membahas mengenai pengolahan barang bukti digital, *Codec* yang dipakai adalah G.711 karena simulasi dilakukan dengan jaringan *LAN*.

Tujuan Penelitian ini yaitu Mengetahui Karakteristik Data Digital berupa suara pada layanan *Voice Over IP* yaitu dilihat dari *Pitch*, *Formant*, dan *Spectogram* dan Menganalisis Data Digital berupa suara pada layanan *Voice Over IP* apakah identik atau tidak antara suara barang bukti dengan suara pembanding.

Manfaat dari penelitian ini adalah dengan menggunakan tools digital forensic setiap kasus yang menggunakan fasilitas teknologi informasi dapat dibuktikan dan diakui keabsahannya. Sehingga bukti data digital pada layanan *Voice Over IP* dapat dijadikan barang bukti yang sah untuk digunakan dalam persidangan.

ISSN 2460-0741

II. DASAR TEORI

A. VoIP (Voice over Internet Protocol)

Pengertian *Voice over Internet Protocol* (*VoIP*) adalah teknologi yang mampu mengirimkan data suara, video dan data yang berbentuk paket secara realtime dengan jaringan yang menggunakan *Internet Protocol* (IP).[1]

B. Network Forensics

Network Forensic adalah cabang dari digital forensic berkaitan dengan monitoring dan analisis lalu lintas jaringan kompuer untuk tujuan pengumpulan informasi, bukti hukum atau deteksi instruksi. [2] *Network Forensics* adalah menangkap, merekam, dan analisis peristiwa jaringan untuk menemukan sumber serangan keamanan atau insiden masalah lainnya.[2]

C. Digital Evidence

Bukti digital (*Digital Evidence*) merupakan salahsatu perangkat vital dalam mengungkap tindak cybercrime. Dengan mendapatkan bukti-bukti yang memadai dalam sebuah tindak kejahatan, sebenarnya telah terungkap separuh kebenaran. Langkah berikutnya adalah menindak-lanjuti bukti-bukti yang ada sesuai dengan tujuan yang ingin dicapai. Bukti Digital yang dimaksud dapat berupa adalah : *E-mail, file-file wordprocessors, spreadsheet, sourcecode* dari perangkat lunak, *Image, web browser, bookmark, cookies*, Kalender.[3]

D. Wireshark

Wireshark merupakan salah satu network analysis tool, atau packet sniffer. *Wireshark* dapat digunakan untuk *troubleshooting* jaringan, analisis, pengembangan *software* dan *protocol* serta untuk keperluan edukasi.[4]

Wireshark memungkinkan anda pengguna mengamati data dari jaringan yang sedang beroperasi atau dari data yang ada di *disk*, dan langsung melihat dan mensortir data yang tertangkap. Informasi singkat dan datail bagi masing-masing paket, termasuk *full header* dan porsi data, bisa diperoleh. *Wireshark* mempunyai beberapa fitur termasuk *display filter language* yang kaya dan kemampuan untuk merekonstruksi kembali sebuah aliran pada sesi *TCP*.[4]

E. Komponen Suara

a. *Pitch*

Frekwensi getar dari pita suara yang juga disebut dengan istilah frekwensi fundamental (dasar) dengan notasi F0. Masing-masing orang memiliki *Pitch* yang khas (habitual *Pitch*) yang sangat dipengaruhi oleh aspek fisiologis larynx manusia. Pada kondisi pembicaraan normal, level habitual *Pitch* berkisar pada 50 s/d 250 Hz untuk laki-laki dan 120 s/d 500 Hz untuk perempuan. Frekwensi F0 ini berubah secara konstan dan memberikan informasi linguistik seseorang seperti perbedaan intonasi dan emosi[5].

b. *Formant*

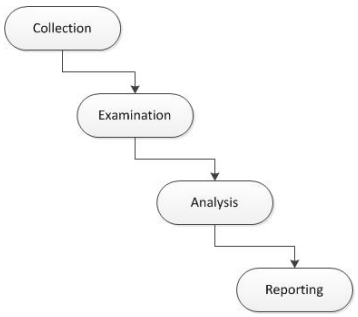
Formant adalah frekwensi-frekwensi resonansi dari *filter*, yaitu *vocal tract (articulator)* yang meneruskan dan memfilter bunyi periodik dari getarnya pita suara (*vocal cord*) menjadi bunyi keluaran (*output*) berupa kata-kata yang memiliki makna. Secara umum, frekwensi-frekwensi *Formant* bersifat tidak terbatas, namun untuk identifikasi suara seseorang, paling tidak ada 3 (tiga) *Formant* yang dianalisa, yaitu *Formant* 1 (F1), *Formant* 2 (F2) dan *Formant* 3 (F3) [5]

c. *Spectogram*

Spectrogram merupakan representasi *spectral* yang bervariasi terhadap waktu yang menunjukkan tingkat *density* (intensitas energi) *spektral*. Dengan kata lain *spectrogram* adalah bentuk *visualisasi* dari masing-masing nilai *Formant* yang dilengkapi dengan level energi yang bervariasi terhadap waktu. *Level* energy ini dikenal dengan istilah *Formant bandwidth*. Nantinya pada kasus-kasus yang bersifat pemalsuan suara dengan teknik *Pitch shift* atau si subyek berusaha untuk menghilangkan karakter suara aslinya, maka *Formant bandiwidth* dapat digunakan untuk memetakan atau mengidentifikasi suara aslinya. Dikarenakan *spectrogram* memuat hal-hal yang bersifat detil, maka *Spectrogram* oleh beberapa ahli juga dikenal dengan istilah sidik jari suara (*voice fingerprint*)[5].

III. METODOLOGI

Metodologi yang digunakan dalam penelitian ini adalah model proses forensik (The Forensic Proces Model) untuk lebih detailnya dapat dilihat pada gambar 1.



Gambar 1 Diagram Alir Metodologi Penelitian [6]

A. Collection

Tahapan ini dilakukan untuk mengumpulkan bukti – bukti digital yang dapat mendukung penyelidikan. Penyelidikan dimulai dari identifikasi dimana bukti itu berada, dimana disimpan dan bagaimana penyimpanannya untuk mempermudah penyelidikan. Barang bukti digital yang akan periksa berupa file suara yang dihasilkan dari monitoring jaringan yang digunakan oleh tersangka dan korban dengan menggunakan aplikasi monitoring yaitu wireshark.

Bukti digital berupa suara tersebut didapat dari hasil filterisasi paket data – paket data hasil dari monitoring. Proses Filterisasi merupakan salah satu proses untuk mempermudah dalam menemukan paket data yang dibutuhkan dalam proses penyelidikan.

B. Examination

Paket data hasil monitoring jaringan yang telah disimpan sebelumnya kemudian akan diperiksa secara komprehensif

ISSN 2460-0741

dengan maksud untuk mendapatkan data – data digital yang sesuai dengan investigasi, jadi analis forensik harus mendapatkan gambaran fakta kasus yang lengkap dari investigator, sehingga apa yang dicari dan akhirnya ditemukan oleh analis forensik sama seperti yang diharapkan oleh investigator untuk pengembangan investigasinya, setelah mendapatkan gambaran dari kasus tersebut, maka analis forensik melakukan pencarian (searching) terhadap paket data untuk mendapatkan file atau data yang diperlukan dalam proses penyelidikan.

Proses searching bisa memakan waktu yang cukup lama, tergantung seberapa besar jumlah paket data yang didapat dari hasil monitoring, untuk mempersingkat waktu dalam proses searching dapat digunakan teknik manual searching atau automated searching. Kemampuan dasar melakukan manual searching tentunya harus dimiliki oleh siapapun yang akan melakukan aktivitas analisis forensik.

C. *Analysis*

Tahapan ini dilaksanakan dengan melakukan analisa secara mendalam terhadap bukti – bukti yang ada. Bukti yang telah didapatkan perlu di explore kembali kedalam sejumlah scenario yang berhubungan dengan kasus tersebut. selama proses analisis berlangsung, analis forensik harus selalu berdiskusi dengan investigator mengenai data – data digital yang nantinya menjadi barang bukti digital dalam rangka mengonfirmasi data – data tersebut sesuai dengan fakta kasus dari kasus kejahatan yang sedang diinvestigasi. Sehingga yang dihasilkan pada proses ini matching (sama) seperti yang diharapkan oleh tim investigator.

D. *Reporting*

Data yang diperoleh dari barang bukti digital dari mulai proses pemeriksaan sampai dengan proses analisis diatas, selanjutnya data – data mengenai barang bukti digital tersebut dimasukkan ke dalam laporan teknis.

Laporan ini secara umum dibagi menjadi beberapa bab penjelasan, sebagai berikut :

1. Judul : memuat judul pemeriksaan yang dilengkapi dengan nomor pemeriksaan laboratorium.
2. Pendahuluan : memuat nama – nama analis forensik yang melakukan pemeriksaan dan analisis secara digital forensik terhadap barang bukti elektronik, disamping itu bab ini juga memuat tanggal/waktu pemeriksaan.
3. Barang Bukti : memuat jumlah dan jenis barang bukti elektronik yang diterima untuk dilakukan pemeriksaan dan analisis.
4. Maksud Pemeriksaan : memuat uraian tentang maksud dari pemeriksaan yang dilakukan oleh analis forensik.
5. Prosedur Pemeriksaan : memuat tahapan – tahapan yang akan dilakukan dalam pemeriksaan agar sesuai dengan maksud yang diinginkan. Tahapan - tahapan sebaiknya ditulis dengan sesuai SOP (Standard Operating Procedure) yang baku dan lengkap.
6. Hasil Pemeriksaan : memuat penjelasan tentang hasil dari pemeriksaan yang dilakukan pada barang bukti.
7. Kesimpulan : memuat simpulan – simpulan yang merupakan rangkuman dari hasil analisis pemeriksaan terhadap barang bukti.
8. Penutup : menjelaskan bahwa proses pemeriksaan dan analisis dilakukan dengan sebenar – benarnya tanpa ada rekayasa dan dapat dipertanggungjawabkan secara ilmiah. Bab ini dilengkapi dengan tanda tangan analis forensik yang melakukan pemeriksaan dan analisis secara digital forensik.

IV. HASIL DAN PEMBAHASAN

A. *Deskripsi kasus*

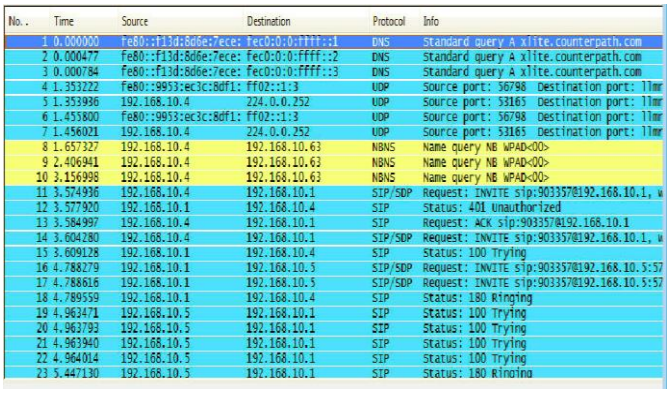
Kemajuan teknologi yang semakin pesat akan mendorong terjadinya perubahan pada sebuah perilaku manusia, salah satu contoh dari perilaku manusia yang terubah akibat kemajuan teknologi ini adalah dengan adanya penyalahgunaan layanan internet yang dijadikan media untuk berbuat kejahatan.

Kejahatan yang dilakukan adalah kejahatan dengan modus penipuan yang melibatkan jaringan telepon internet atau bisa disebut dengan *VoIP* (Voice Over Internet Protocol). Penelitian ini mengambil contoh kasus penipuan dengan alasan kepada korban mendapatkan hadiah langsung on spot sejumlah uang dengan fokus pembahasan pada cara menemukan dan membuka file suara (percakapan).

B. *Collection*

Tahapan ini dilakukan pengumpulan barang bukti yang akan di periksa pada tahapan selanjutnya. Proses yang dilakukan pada tahapan ini adalah dengan melakukan monitoring jaringan terhadap jaringan yang sedang digunakan. Hasil dari monitoring jaringan ini berupa paket – paket yang melalui jaringan tersebut dengan berbagai macam protokol.

Jenis – jenis protokol sangat banyak namun yang digunakan dalam jaringan *VoIP* (Voice Over Internet Protocol) adalah protokol SIP (Session Initation Protocol). Protokol ini merupakan protokol standarisasi dalam jaringan Voice Over IP (*VoIP*) untuk mendapatkan paket data dengan protokol SIP adalah dengan cara memfilter hasil monitoring pada jaringan Voice Over IP berikut hasil dari monitoring pada jaringan *VoIP* dapat dilihat pada Gambar 2.



No. .	Time	Source	Destination	Protocol	Info
1	0.000000	fe80::f13d:8d6e:7ece:	fec0:0:0:ffff::1	DNS	Standard query A xlite.counterpath.com
2	0.000477	fe80::f13d:8d6e:7ece:	fec0:0:0:ffff::2	DNS	Standard query A xlite.counterpath.com
3	0.000784	fe80::f13d:8d6e:7ece:	fec0:0:0:ffff::3	DNS	Standard query A xlite.counterpath.com
4	1.353222	fe80::9953:ec3c:8df1:	ff02::1:3	UDP	Source port: 36798 Destination port: llmr
5	1.353936	192.168.10.4	224.0.0.252	UDP	Source port: 53165 Destination port: llmr
6	1.455800	fe80::9953:ec3c:8df1:	ff02::1:3	UDP	Source port: 36798 Destination port: llmr
7	1.456021	192.168.10.4	224.0.0.252	UDP	Source port: 53165 Destination port: llmr
8	1.657327	192.168.10.4	192.168.10.63	NBNS	Name query NB WPAD<00>
9	2.406941	192.168.10.4	192.168.10.63	NBNS	Name query NB WPAD<00>
10	3.156998	192.168.10.4	192.168.10.63	NBNS	Name query NB WPAD<00>
11	3.574936	192.168.10.4	192.168.10.1	SIP/SDP	Request: INVITE sip:9033570192.168.10.1, w
12	3.577920	192.168.10.1	192.168.10.4	SIP	Status: 401 Unauthorized
13	3.584997	192.168.10.4	192.168.10.1	SIP	Request: ACK sip:9033570192.168.10.1
14	3.604280	192.168.10.4	192.168.10.1	SIP/SDP	Request: INVITE sip:9033570192.168.10.1, w
15	3.609128	192.168.10.1	192.168.10.4	SIP	Status: 100 Trying
16	4.788279	192.168.10.1	192.168.10.5	SIP/SDP	Request: INVITE sip:9033570192.168.10.5:57
17	4.788616	192.168.10.1	192.168.10.5	SIP/SDP	Request: INVITE sip:9033570192.168.10.5:57
18	4.789559	192.168.10.1	192.168.10.4	SIP	Status: 180 Ringing
19	4.963471	192.168.10.5	192.168.10.1	SIP	Status: 100 Trying
20	4.963793	192.168.10.5	192.168.10.1	SIP	Status: 100 Trying
21	4.963940	192.168.10.5	192.168.10.1	SIP	Status: 100 Trying
22	4.964014	192.168.10.5	192.168.10.1	SIP	Status: 100 Trying
23	5.447130	192.168.10.5	192.168.10.1	SIP	Status: 180 Ringing

Gambar 2 Hasil Monitoring pada Jaringan *VoIP*

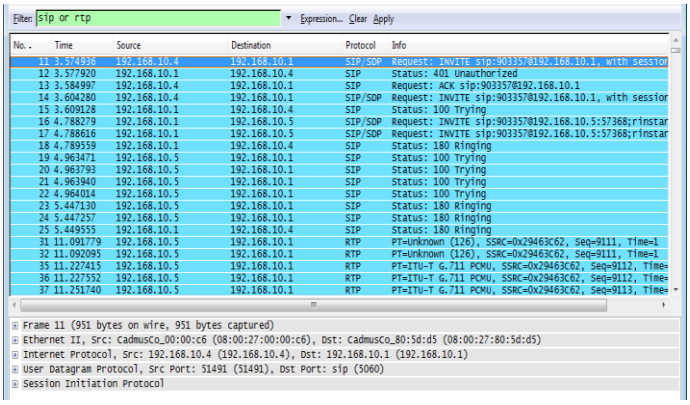
ISSN 2460-0741

Hasil filter tersebut merupakan hasil yang akan diperiksa dan dijadikan barang bukti untuk mendapatkan hasil percakapan.

C. Examination

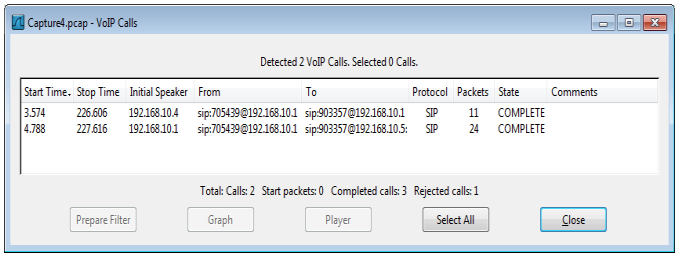
Paket data hasil filter akan diperiksa secara komprehensif dengan maksud untuk mendapatkan data – data digital yang sesuai dengan investigasi. Data – data yang dicari merupakan data – data yang berhubungan dengan identitas dari pelaku dan korban. Proses pencarian ini dilakukan pada aplikasi Wireshark dengan memfilter paket data hasil monitoring dari jaringan *VoIP* yang dipakai oleh pelaku.

Filterisasi dalam aplikasi Wireshark merupakan salah satu fasilitas yang digunakan untuk mempermudah dalam pencarian salah satu paket data, maka untuk mempermudah pencarian paket data pada aplikasi wireshark digunakan field "sip or rtp". Field tersebut akan memfilter dari semua paket data yang didapat menjadi paket data yang berprotokol SIP atau RTP, protokol SIP atau RTP ini adalah protokol yang digunakan dalam jaringan *VoIP*, untuk lebih jelasnya dapat dilihat pada gambar 3.



Gambar 3 Pemilihan Paket Data

Hasil pemeriksaan dari salah satu paket data yang terjaring dari hasil monitoring jaringan dengan menggunakan aplikasi Wireshark diperoleh bahwa dalam paket data tersebut terdapat beberapa file yang mengandung percakapan antara pelaku dan korban, berikut file percakapan tersebut dapat dilihat pada Gambar 4.

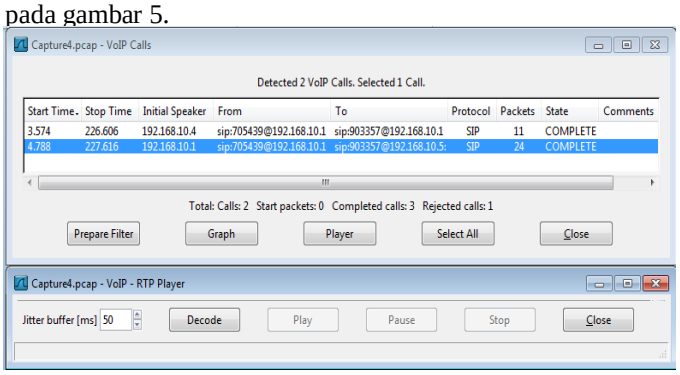


Gambar 4 File Percakapan

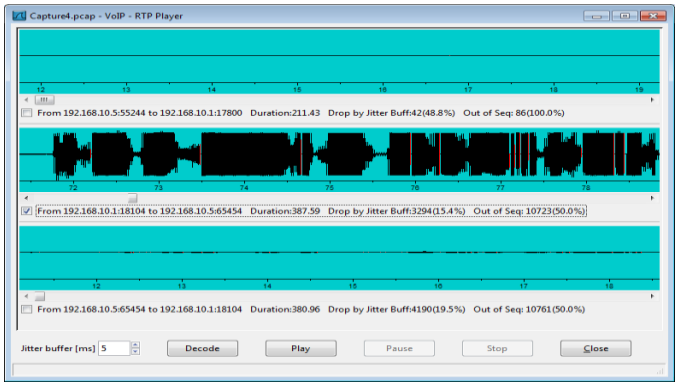
D. Analysis

Tahap selanjutnya adalah tahapan analisis dimana pada tahapan ini akan dilakukan analisis pada paket data yang telah di filter dari paket data tersebut akan didapat barang bukti berupa file suara atau percakapan. Proses yang dilakukan untuk mendapatkan file suara tersebut adalah dengan proses codec.

Proses codec atau pengkodean merupakan proses perubahan sinyal dari sinyal analog ke sinyal digital. Proses ini dilakukan dengan menggunakan aplikasi Wireshark yang memanfaatkan tools *VoIP* Calls. Tahapan codec ini menggunakan codec G.711 codec ini yang biasanya digunakan dalam jaringan *VoIP* yang berbasis LAN (Local Area Network). Pengkodean barang bukti digital dapat dilihat pada gambar 5.



Gambar 5 Pengkodean *VoIP* Calls



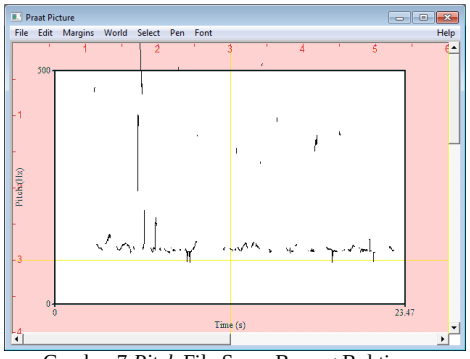
Gambar 6 Hasil Decoding

Barang bukti hasil percakapan ini selanjutnya akan dianalisis agar diketahui identik atau tidak dengan suara pelaku dengan cara membandingkan dengan beberapa subjek yang dicurigai sebagai pelaku. Namun, untuk membuktikan identik atau tidak dengan suara pelaku akan diambil sampel dari hasil percakapan, yaitu kalimat "Perkenalkan saya haji faiz dari perusahaan operator seluler. Perusahaan kami ingin memperbaiki citra buruk yang selama ini sering dimanfaatkan". Analisis yang akan dilakukan adalah sebagai berikut :

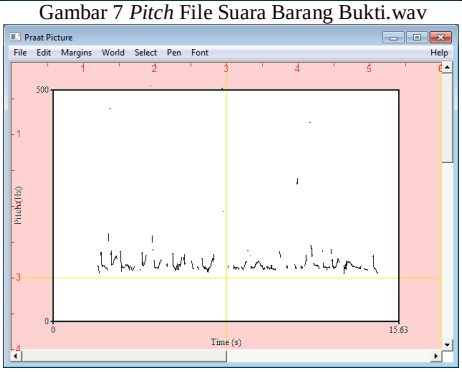
a. Analisis *Pitch*

Komponen suara yang akan dianalisis adalah *Pitch*, yang diambil dari rekaman barang bukti dan rekaman pembanding dengan pengucapan kalimat "Perkenalkan saya haji faiz dari perusahaan operator seluler. Perusahaan kami ingin memperbaiki citra buruk yang selama ini sering dimanfaatkan". Hasil dari pengambilan komponen *Pitch* tersebut dapat dilihat pada Gambar 7.

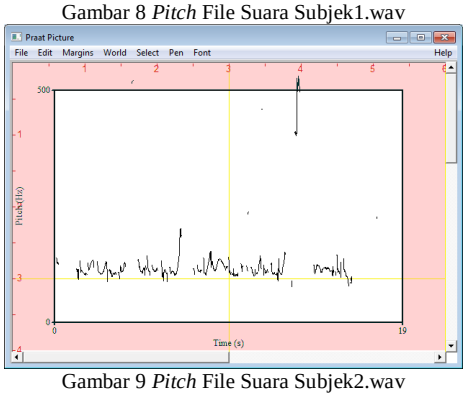
ISSN 2460-0741



Gambar 7 *Pitch* File Suara Barang Bukti.wav



Gambar 8 *Pitch* File Suara Subjek1.wav



Gambar 9 *Pitch* File Suara Subjek2.wav

Gambar 7, 8, dan 9 merupakan analisa dari file audio Suara Barang Bukti.wav, Subjek1.wav, dan Subjek2.wav. dari ketiga gambar tersebut akan didapatkan nilai *Pitch* maximum, *Pitch* minimum, *Pitch* median, dan *Pitch* standar deviation dengan menggunakan aplikasi Praat, berikut nilai hasil dari file audio Suara Barang Bukti.wav, Subjek1.wav, dan Subjek2.wav dapat dilihat pada Tabel 1.

TABEL 1 NILAI STATISTIK *PITCH* DARI FILE AUDIO SUARA BARANG BUKTI.WAV, SUBJEK1.WAV, DAN SUBJEK2.WAV

Analisis Statistik	**Suara Barang Bukti (Hz)**	**Suara Subjek1 (Hz)**	**Suara Subjek2 (Hz)**
Pitch minimum	78.295316	103.179827	75.161762
Pitch maximum	595.714733	587.710609	596.761127
Pitch quantile	118.335892	118.767065	112.464855
Pitch mean	151.892331	130.603729	128.567006
Pitch standard deviation	101.020795	56.143349	71.065025

Jika karakteristik *Pitch* dari masing – masing suara menunjukkan tingkat perbedaan yang besar, maka dapat disimpulkan bahwa *Pitch* dari suara barang bukti dengan suara pembanding adalah berbeda. Analisis Nilai Statistik *Pitch* pada Tabel 1 pada pengucapan kalimat "Perkenalkan saya haji faiz dari perusahaan operator seluler. Perusahaan kami ingin memperbaiki citra buruk yang selama ini sering dimanfaatkan" antara file audio Suara Barang Bukti.wav, Subjek1.wav, dan Subjek2.wav memiliki perbedaan yang kecil, jadi dapat disimpulkan bahwa file audio Suara Barang Bukti.wav, Subjek1.wav, dan Subjek2.wav IDENTIK.

b. Analisis *Formant*

a) Analisis *Anova*

Analisis ini didasarkan pada analisa One-way Anova (Analysis of Variances) yang mengkalkulasi secara statistik nilai-nilai *Formant* 1, *Formant* 2, *Formant* 3 dan *Formant* 4 dari file Suara Barang Bukti.wav, Subjek1.wav, dan Subjek2.wav. Analisis Anova akan menunjukkan tingkat perbedaaan antara 2 (dua) kelompok data pada masing-masing *Formant* dari suara pembanding dan suara barang bukti yang ditandai dengan perbandingan ratio F dan F critical, dan nilai probability P.

Jika nilai ratio F lebih kecil dari F critical, dan nilai probability P lebih besar dari 0.5, maka dapat disimpulkan bahwa kedua kelompok data dari nilai *Formant* yang dianalisa dari suara pembanding dan barang bukti tidak memiliki perbedaan (accepted) yang signifikan pada level 0.05.[5]

Melalui analisis anova didapatkan nilai perbandingan antara ratio F, P value dan F critical. Hasil dari keseluruhan nilai perbandingan ratio F, P value dan F critical dari nilai *Formant* dengan nilai bandwith 1-5 pada tiap - tiap kata suara barang bukti dengan suara pembanding adalah sebagaimana pada Tabel 2, 3, 4, dan 5.

TABEL 2 NILAI STATISTIK *ANOVA* KATA "SAYA"

Formant / Bandwith Kata "Saya"	Ratio F	P-*value*	F *critical*	Kesimpulan
Formant 1	9.553287	9.458663	4.675408	*Rejected*
Formant 2	38.420211	1.314423	4.675408	*Rejected*
Formant 3	40.748529	2.069812	4.675408	*Rejected*
Formant 4	146.45094	3.159232	4.675876	*Rejected*
Formant 5	1259.771076	2.473036	4.694300	*Rejected*
Bandwith 1	26.292346	2.920385	4.675408	*Rejected*
Bandwith 2	2.311112	0.100884	4.675408	*Accepted*
Bandwith 3	7.314103	0.000789	4.675408	*Rejected*
Bandwith 4	49.509456	2.484366	4.675876	*Rejected*
Bandwith 5	56.753463	6.357320	4.694300	*Rejected*

TABEL 3 NILAI STATISTIK *ANOVA* KATA "HAJI"

Formant / Bandwith Kata "Haji"	Ratio F	P-*value*	F *critical*	Kesimpulan
Formant 1	0.259807	0.771553	4.752500	*Accepted*
Formant 2	21.069244	9.005346	4.752500	*Rejected*
Formant 3	11.559252	7.571712	3.917656	*Rejected*
Formant 4	106.65237	3.279964	4.754576	*Rejected*
Formant 5	239.70421	9.555222	4.794607	*Rejected*
Bandwith 1	25.611500	2.864189	4.752500	*Rejected*
Bandwith 2	25.620574	2.844980	4.752500	*Rejected*
Bandwith 3	14.489365	1.805097	4.752500	*Rejected*
Bandwith 4	11.664648	2.007249	4.754576	*Rejected*
Bandwith 5	47.442983	9.464119	4.794607	*Rejected*

ISSN 2460-0741

TABEL 4 NILAI STATISTIK *ANOVA* KATA "FAIZ"

Formant / Bandwith Kata "Faiz"	Ratio F	P-*value*	F *critical*	Kesimpulan
Formant 1	31.557284	6.019932	4.6910519	*Rejected*
Formant 2	59.181417	9.078732	4.6910519	*Rejected*
Formant 3	55.902876	8.571710	4.691051	*Rejected*
Formant 4	131.644772	1.343855	4.692465	*Rejected*
Formant 5	235.140986	1.565937	4.745668	*Rejected*
Bandwith 1	66.5283268	6.833210	4.691051	*Rejected*
Bandwith 2	55.3904046	1.222003	4.691051	*Rejected*
Bandwith 3	46.6206260	6.202494	4.691051	*Rejected*
Bandwith 4	13.2292149	3.492106	4.692465	*Rejected*
Bandwith 5	13.3476121	4.510259	4.745668	*Rejected*

Pada tabel 2, 3, dan 4. dapat ditarik kesimpulan bahwa, hasil analisis anova untuk nilai *Formant* 1, 2, 3, 4, dan 5 berikut nilai bandwith-nya menunjukan dari file audio Suara Barang Bukti.wav, Subjek1.wav, dan Subjek2.wav TIDAK IDENTIK, karena untuk menarik kesimpulan IDENTIK dari analisis Anova dibutuhkan paling tidak *Formant* 1, 2, dan 3 yang dianalisis. Jika dua diantara *Formant* 1, 2, dan 3 menunjukkan accepted, maka hal tersebut sudah cukup untuk menarik kesimpulan IDENTIK berdasarkan Analisis Anova. Sedangkan untuk nilai Bandwith hanya digunakan pada hal – hal yang berifat kasuitas, yaitu dimana subjek berusaha memberikan suara pembanding yang benar – benar berbeda dengan apa yang telah diucapkan pada barang bukti.

b) Analisis *Likelihood Ratio*

Merujuk hasil dari kalkulasi Analisis Anova yang didapat sebelumnya, maka perhitungan LR untuk *Formant* dapat dilihat pada Tabel 5, 6, dan 7.

TABEL 5 ANALISIS *LIKELIHOOD RATIO* KATA "SAYA"

Formant Kata "Saya"	p (E | Hp) = P-*value*	p (E | Hd)	LR
Formant 1	9.458663	- 8.458663	- 1.118221
Formant 2	1.314423	- 0.314423	- 4.180428
Formant 3	2.069812	- 1.069812	- 1.934743
Formant 4	3.159232	- 2.159232	- 1.463127
Formant 5	2.473036	- 1.473036	- 1.678870

TABEL 6 ANALISIS *LIKELIHOOD RATIO* KATA "HAJI"

Formant Kata "Haji"	p (E | Hp) = P-*value*	p (E | Hd)	LR
Formant 1	0.771553	0.228447	3.377382
Formant 2	9.005346	- 8.005346	- 1.124916
Formant 3	7.571712	- 6.571712	- 1.152167
Formant 4	3.279964	- 2.279964	- 1.438603
Formant 5	9.555222	- 8.555222	- 1.116887

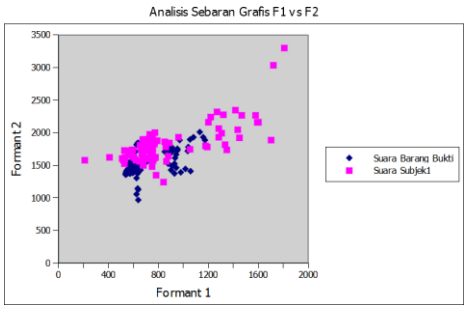
TABEL 7 ANALISIS *LIKELIHOOD RATIO* KATA "FAIZ"

Formant Kata "Faiz"	p (E | Hp) = P-*value*	p (E | Hd)	LR
Formant 1	6.019932	- 5.019932	- 1.199205
Formant 2	9.078732	- 8.078732	- 1.123781
Formant 3	8.571710	- 7.571710	- 1.132070
Formant 4	1.343855	- 0.343855	- 3.908202

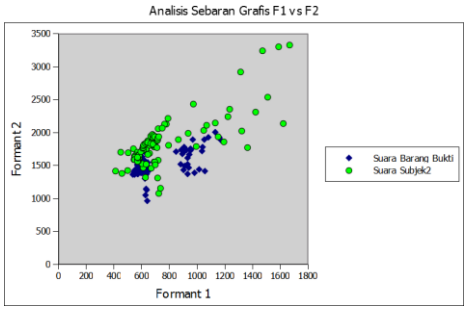
Dari hasil yang analisis LR sebagaimana pada Tabel 5, 6, dan 7 didapatkan kesimpulan bahwa tidak ada satu pun *Formant* yang mendukung hipotesis penuntutan (suara barang bukti dan suara pembanding identik). Namun sebaliknya, hasil kesimpulan menunjukan bahwa keseluruhan *Formant* mendukung hipotesis perlawanan (suara evidence dan subjek tidaklah identik)

c) Analisis *Graphical Distribution*

Analisis *Graphical Distribution* digunakan untuk melihat *range* sebaran grafis dari nilai – nilai *Formant* pada masing – masing suara melalui tampilan grafik. Tampilan grafik akan dapat diketahui apakah suara yang dibandingkan antara suara barang bukti dengan suara pembanding memiliki pola sebaran yang identik atau tidak identik.

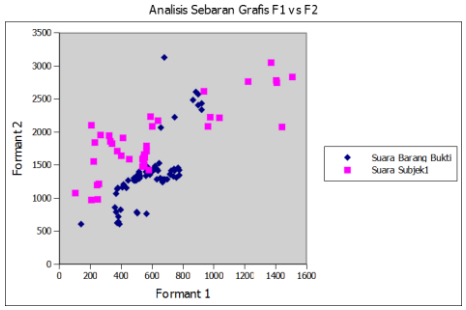


Gambar 10 Analisa Sebaran Grafis F1 vs F2 kata "Saya" dengan Subjek1



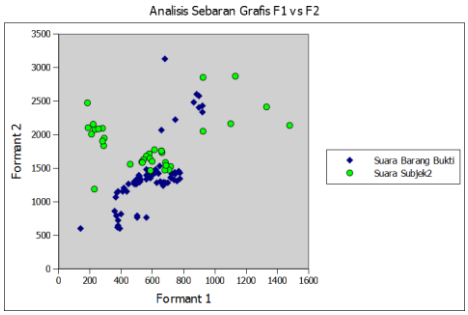
Gambar 11 Analisa Sebaran Grafis F1 vs F2 kata "Saya" dengan Subjek2

Kedua grafik di atas sebaran grafis dari kata "Saya", terlihat bahwa terdapat beberapa sebaran dari nilai F1 vs F2 yang diluar dari kumpulan grafis sebaran yang lainnya. Jika grafis sebaran yang keluar tersebut diabaikan, maka masih terdapat beberapa sebaran grafis dari suara barang bukti dan suara pembanding yang berkumpul pada tempat yang sama. Jadi hal tersebut dapat ditarik sebuah kesimpulan bahwa dari hasil analisa sebaran grafis bahwa antara F1, F2 dari suara barangbukti dengan suara pembanding baik itu suara Subjek1 maupun Subjek2 adalah IDENTIK.



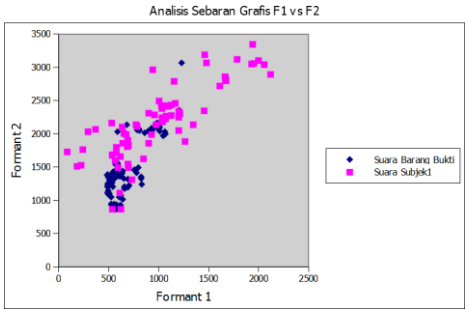
Gambar 12 Analisa Sebaran Grafis F1 vs F2 kata "Haji" dengan Subjek1

ISSN 2460-0741



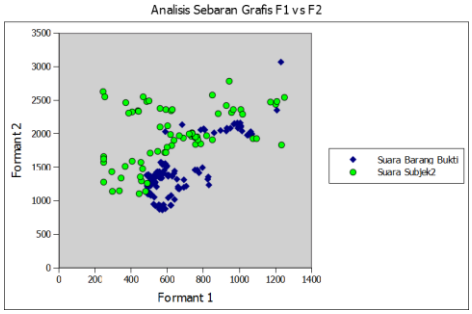
Gambar 13 Analisa Sebaran Grafis F1 vs F2 kata "Haji" dengan Subjek2

Analisa Grafik yang terdapat pada Gambar 12 sampai Gambar 13 menunjukan bahwa sebaran dari suara barang bukti dengan suara pembanding keluar dari kelompoknya. Jika sebaran tersebut dieleminir, maka dapat dilihat bahwa masih ada nilai sebaran grafis F1 vs F2 antara suara barang bukti dengan suara pembanding dalam rentang kelompok yang sama. Namun, hal itu masih kurang, jadi dapat ditarik kesimpulan bahwa F1 vs F2 antara suara barang bukti dengan suara pembanding adalah TIDAK IDENTIK.



Gambar 14 Analisa Sebaran Grafis F1 vs F2 kata "Faiz" dengan Subjek1

Grafik di atas sebaran grafis dari kata "Faiz", terlihat bahwa terdapat beberapa sebaran dari nilai F1 vs F2 yang diluar dari kumpulan grafis sebaran yang lainnya. Jika grafis sebaran yang keluar tersebut diabaikan, maka masih terdapat beberapa sebaran grafis dari suara barang bukti dan suara pembanding yang berkumpul pada tempat yang sama. Jadi hal tersebut dapat ditarik sebuah kesimpulan bahwa dari hasil analisa sebaran grafis bahwa antara F1, F2 dari suara barangbukti dengan suara pembanding baik itu suara Subjek1 maupun Subjek2 adalah IDENTIK.

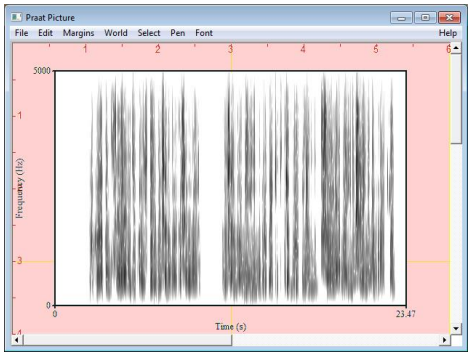


Gambar 15 Analisa Sebaran Grafis F1 vs F2 kata "Faiz" dengan Subjek2

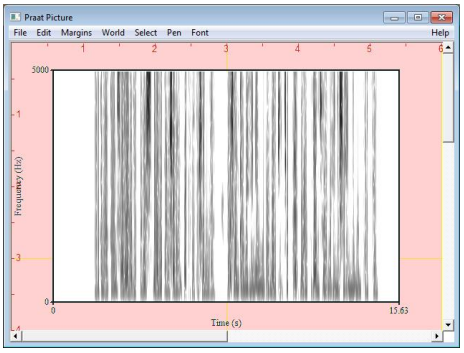
Gambar 14 pada Analisa Sebaran Grafis dari kata "Faiz" F1 vs F2 dengan pembanding Suara Subjek2 menunjukan banyak sebaran yang keluar dari kelompok Suara Barang Bukti, hal ini membuktikan bahwa Tidak Identik antara Suara barang bukti dengan suara pembanding. Namun, pada F2 vs F3 menunjukan banyak sebaran yang masih bergabung dengan sebaran Suara Barang Bukti. Jadi dapat disimpulkan untuk Analisis Sebaran grafis dengan Kata "Faiz" adalah TIDAK IDENTIK.

c. Analisis *Spectogram*

Selanjutnya dilakukan pengambilan komponen suara *Spectogram* dengan pengucapan kata "Perkenalkan saya haji faiz dari perusahaan operator seluler. Perusahaan kami ingin memperbaiki citra buruk yang selama ini sering dimanfaatkan". Hasil dari pengambilan komponen *Spectogram* tersebut akan terlihat bentuk *visualisasi grafis* nilai masing - masing *Formant*, berikut *level* energinya yang pada masing-masing kata atau suku kata membentuk pola-pola yang khas pada masing-masing *Formant* pada pengucapannya. Hasil tersebut dapat dilihat pada Gambar 16, 17, dan 18 berikut.

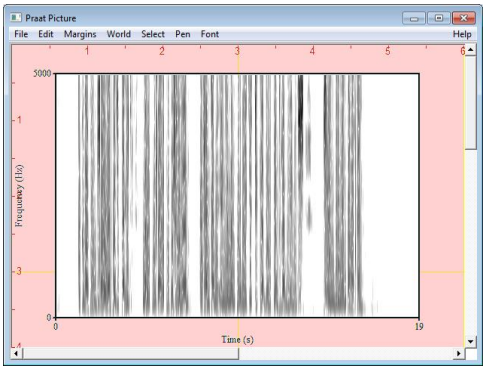


Gambar 16 *Spectogram File* Suara Barang Bukti.*wav*



Gambar 17 *Spectogram File* Suara Subjek1.*wav*

ISSN 2460-0741



Gambar 18 *Spectogram File* Suara Subjek2.*wav*

Gambar 16, 17, dan 18 menunjukan komponen *spectrogram* dari *file* suara barang bukti dengan *file* suara pembanding (Subjek1 dan Subjek2), dimana pada *spectrogram* antara Suara Barang Bukti dengan Suara Subjek1 memiliki kesamaan. Jadi dapat disimpulkan bahwa antara Suara Barang Bukti dengan Suara Subjek1 adalah IDENTIK. Namun, perbandingan pola *Spectogram* antara Suara Barang Bukti dengan Suara Subjek2 menunjukan perbedaan yang signifikan sehingga dapat ditarik kesimpulan melalui analisis *spectrogram* ini bahwa antara *file* Suara Barang Bukti dengan Suara Subjek2 TIDAK IDENTIK

E. Report and Documentation

Bukti digital berupa paket data dan rekaman percakapan yang telah melalui proses pemeriksaan dan analisis didapatkan data – data yang sesua kebutuhan investigasi, selanjutnya data – data mengenai barang bukti tersebut akan dimasukkan ke dalam laporan teknis.

V. KESIMPULAN

Merujuk dari penelitian yang sudah dilakukan mengenai Analisis Data *Digital Evidence* pada Layanan *Voice Over IP* maka dapat ditarik kesimpulan sebagai berikut :

1. Bukti digital berupa *file* suara atau percakapan antara pelaku dan korban dari layanan *Voice over IP* dapat diperoleh dari aplikasi *Wireshark* dengan menggunakan fasilitas *VoIP Calls.*
2. Rata – rata hasil dari Analisis *Pitch* menunjukan IDENTIK, hasil dari Analisis *Formant* ada beberapa yang TIDAK IDENTIK, yaitu Analisis *Anova*, *Likelihood Ratio*, dan *Graphical Distribution* pada kata "Haji". Sedangkan pada Analisis *Spectogram* hasilnya adalah IDENTIK dengan Subjek1.
3. Keseluruhan jenis metode analisis yang digunakan dalam melakukan tahap analisis *voice recognition*, didapatkan hasil bahwa hampir keseluruhan metode yang digunakan menunjukan kesimpulan bahwa antara suara barang bukti dengan suara pembanding adalah Identik. Meskipun pada analisis *anova* dan *likelihood ratio* kesimpulan bahwa adalah tidak identik namun kemungkinan itu tereliminir oleh hasil metode yang lain, sehingga hasil tersebut dapat diabaikan.

REFERENSI

[1] Jaya Patih, D. F., Fitriawan, H., & Yuniati, Y. Analisa Perancangan Server *VoIP* (Voice over Internet Protocol) dengan Opensource Asterisk dan VPN (Virtual Private Network) sebagai Pengaman Jaringan antar Client. 2012.

[2] Adeyemi, I. R., Razak, S. A., & Nor Azhan, N. A. A Review of Current Research in Network Forensic Analysis. *International Journal od Digital Crime and Forensics*, 1-26. 2013

[3] Prayudi, Y., & Afrianto, D. S. Antisipasi Cybercrime menggunakan Teknik Komputer Forensik. *Seminar Nasional Aplikasi Teknologi Informasi*. 2007.

[4] Rosnelly, R., & Pulungan, R. Membandingkan Analisa Trafik Data pada Jaringan Komputer antara Wireshark dan NMAP. Konferensi Nasional Sistem Informasi. 2011.

[5] M. N. Al-Azhar, Audio Forensic: Theory And Analysis. Pusat Laboratorium Forensik Polri Bidang Fisika Dan Komputer Forensik, 2011

[6] Putri, R. U., & Istiyanto, J. E. Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. *IJCCS, Vol.6, No.2, July 2012, pp. 101-112*, 101-112. 2012.