NETWORK FORENSIC INVESTIGASI PADA STEGANOGRAFI

Rizal Broer Bahaweres[1], Hapsari Tiaraningtias[2], Khoirunnisya[3], Putra Hadi Kamil[4]
Teknik Informatika, Fakultas Sains dan Teknologi
Universitas Islam Negeri Syarif Hidayatullah Jakarta
rizalbroer@gmail.com, hapsaritiaraningtias@gmail.com, khoirunnisya64@gmail.com, dipaakun1@gmail.com

ABSTRAK

Seiring dengan semakin berkembangnya teknologi semakin bermunculan aplikasi – aplikasi yang memudahkan dalam melakukan aktivitas. Dengan bermunsulannya *Social Media* seperti *Messenger*, setiap orang tidak perlu bertatap muka untuk menyampaikan sesuatu. Hal ini berbanding lurus dengan semakin mudahnya bagi orang yang berniat jahat untuk melakukan aksinya. Tidak perlu bertemu langsung untuk merencanakan sesuatu, mereka dapat dengan mudah bertukar informasi melalu *Messenger* atau aplikasi lainnya. Dengan didukung dengan teknik kriptografi yaitu teknik untuk menyembunyikan pesan dalam suatu file seperti teks, foto dan lainnya, bahkan sekarang kriptografi sudah berkembang dan muncul steganografi yaitu teknik menyemunyikan pesan dalam file berupa video atau audio, yang dapat memudahkan bagi pelaku kejahatan untuk berkomunikasi tanpa diketahui orang lain.

Kata Kunci: *Steganografi, Messenger, Social Media, Audio*.

I. PENDAHULUAN

Steganografi adalah suatu teknik untuk menyembunyikan pesan dalam sebuah objek, dapat berupa gambar, video ataupun audio. Syarat utama untuk steganografi adalah file tersebut harus benar-benar tersembunyi dan tidak ada orang lain yang mengetahui selain si pengirim dan penerima. Teknologi yang digunakan untuk steganografi semakin berkembang, semakin banyak aplikasi bermunculan yang digunakan untuk steganografi. Berawal hanya pada file gambar dan semakin berkembang hingga ke video dan audio.

Banyak aplikasi atau perangkat lunak yang dapat digunakan untuk mengirim pesan dalam bentuk audio seperti *LINE, Whatsapp*, BBM dan lainnya. Dengan menggunakan protokol TCP/IP berbagai macam file dapat diunggah dan diunduh melalui internet. Hal itu membuat penulis tertarik untuk menggunakan file audio sebagai objek dalam steganografi. Dalam proposal ini penulis merancang sebuah studi kasus untuk menggambarkan bagaimana jalannya percobaan ini.

Misalkan terdapat sebuah organisasi hitam di Jepang yang sangat misterius, salah satu pimpinan dari organisasi tersebut bernama Gin. Gin mempunyai banyak kaki tangan, salah satunya adalah Bourbon. Gin merencanakan sebuah pembunuhan kepada seorang anggota legislatif di Jepang. Gin menugaskan Bourbon untuk melakukan pembunuhan tersebut. Lokasi pembunuhan, foto korban, dan skenario pembunuhan diberitahukan Gin lewat IP *Messenger*. Gin dan Bourbon tidak pernah bertemu saat merencanakan pembunuhan ini. Semua hal yang terkait dengan rencana pembunuhan ini diberikan melalui messenger yang tentu saja informasi tersebut disembunyikan dalam sebuah file lain agar tidak diketahui siapapun. Lama kelamaan polisi Jepang mulai mengetahui keberadaan organisasi hitam ini dan melakukan penyelidikan secara diam-diam. Polisi menyelidiki jaringan internet dan menganalisa setiap paket yang ditransfer dengan menggunakan *Wireshark*.

Rumusan masalah pada proposal ini adalah bagaimana melakukan investigasi steganografi forensic yang terdapat pada lalu lintas network dan menganalisa hasil investigasi tersebut.

Adapun dalam proposal ini penulis melakukan investigasi steganografi dengan menggunakan beberapa *tools*, diantaranya openpuff, wireshark, IPMsg, dan EnCase. Penulis mendeteksi dan menganalisa jaringan wireless dan paket-paket yang ditransmisi pada jaringan tersebut. Pembahasan 802.15.4

II. LANDASAN TEORI

2.1 Network Forensic

Forensic jaringan atau lebih dikenal dengan *network forensic* merupakan proses menangkap, mencatat dan menganalisa aktivitas jaringan guna menemukan

bukti digital (*digital evidence*) dari suatu serangan atau kejahatan yang dilakukan terhadap, atau dijalankan menggunakan jaringan komputer sehingga pelaku kejahatan dapat dituntut sesuai hukum yang berlaku. *Network forensic* dapat digunakan untuk menemukan kejahatan di dunia maya seperti *cyber crime*, walaupun kejahatan itu dilakukan melalui internet dan proses digital kejahatan itu pasti mempunyai jejak yang dapat diselidiki. Dalam melakukan komunikasi dengan perangkat lainnya XBee mampu melakukan komunikasi dengan dua macam model komunikasi, tergantung dari perangkat apa yang digunakan.

2.2 Steganografi

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Kata "steganografi" berasal dari Bahasa Yunani steganos yang artinya tersembunyi atau terselubung dan graphein yang artinya menulis.

2.3 Openpuff

Openpuff merupakan aplikasi yang memungkinkan untuk menyembunyikan data ke dalam file yang dienkripsi dalam rangka untuk mengirimkannya ke pengguna lain. Program ini menggunakan prinsip-prinsip steganografi untuk menyembunyikan informasi ke dalam file biasa seperti gambar, audio, atau video. File-file pembawa (*carrier*) dapat ditransmisikan dengan menggunakan email, perangkat *removable* atau perangkat lainnya seperti biasa. File teks atau gambar yang ingin disembunyikan maksimum berukuran 256 MB. Anda dapat menggunakan tiga *password* saat mengenkripsi file.

2.4 Wireshark

Wireshark merupakan salah satu *tools* atau aplikasi "*Network Analyzer*" atau Penganalisa Jaringan. Penganalisaan Kinerja Jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan, sampai pada digunakan pula untuk *sniffing* (memperoleh informasi penting seperti password *email*, dan lain-lain). Wireshark sendiri merupakan *free tools* untuk *Network Analyzer* yang ada saat ini. Dan tampilan dari wireshark ini sendiri terbilang sangat bersahabat dengan *user* karena menggunakan tampilan grafis atau GUI (*Graphical User Interface*).

2.5 IP *Messenger* (IPMsg)

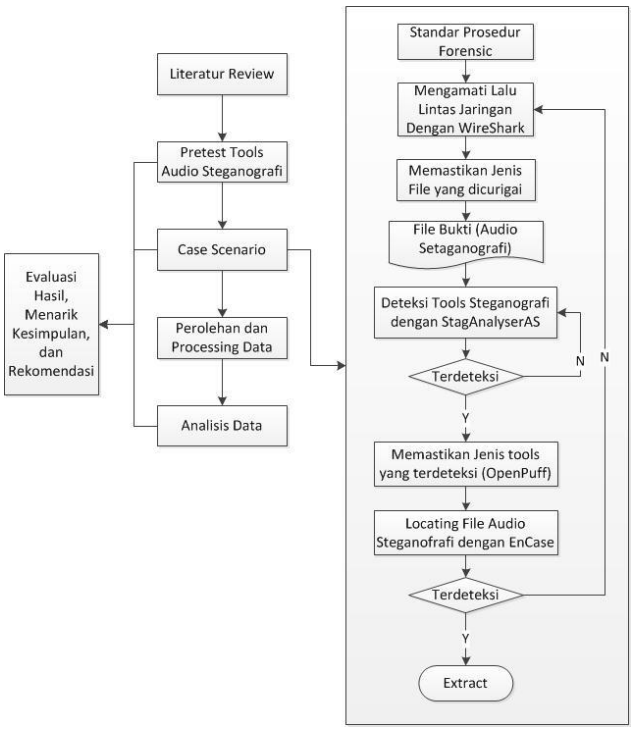
IP *Messenger* (IPMsg) adalah salah satu alat yang mengagumkan yang memungkinkan Anda untuk *chatting* di LAN atau jaringan dengan orang lain apabila mereka menggunakan perangkat lunak yang sama. *Software* perlahan mendeteksi orang yang menggunakan jaringan dalam dan menambah kepada mereka daftar Anda dengan nama ditetapkan dalam perangkat lunak.

2.6 EnCase

Merupakan salah satu *tool* komersil yang banyak digunakan untuk melakukan penyidikan. Tidak hanya dapat membaca data-data yang sudah terhapus, encase juga dapat memberitahukan sistem-sistem yang belum di patch, menerima masukkan dari *intrusion detection system* untuk menyelidiki keanehan jaringan yang terjadi, merespon sebuah insiden keamanan, memonitoring pengaksesan sebuah file penting, dan banyak lagi.

III. METODOLOGI PENELITIAN

Adapun metodologi penelitian yang peneliti lakukan adalah sebagai gambar (Lu, 2014) berikut:



Gambar 1. Alur Metodologi Penelitian

Studi literatur dari *research* yang telah diselesaikan sebelumnya, untuk membantu dan membimbing mengerjakan penelitian ini, khususnya mengenai materi beserta langkah-langkahnya untuk kami menjalankan penelitian.

Pretest tools Steganografi, melakukan eksperimen dengan implementasi pada *tool audio steganography* yang digunakan yaitu OpenPuff, aplikasi IPmsg sebagai *tool* pertukaran data, StegAnalyzerAs sebagai *steganography detection tool*, Wireshark untuk *network capture tool*. Hasil dari eksperimen tergantung pada tools yang digunakan.

Case Scenario, menjalankan *case scenario* dari dunia nyata sebagai bahan untuk *case* investigasi *audio steganography digital forensic*. Tujuan dari phase 2 adalah menghasilkan data mentah dan fakta-fakta untuk kemudian dijadikan bahan untuk diolah dan diproses di tahap selanjutnya untuk dianalisis.

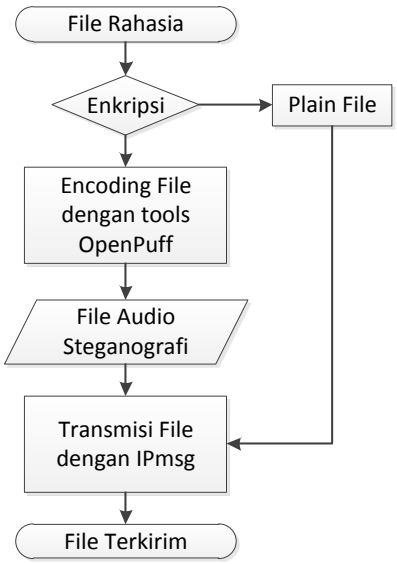
Perolehan data dan *processing data*, data-data hasil dari *case scenario* telah diperoleh dan terproses berdasarkan *digital forensic procedure*. Di tahap ini, EnCase digunakan di tahap ini untuk menganalisis *audio steganography* yang dimaksudkan dalam peneliti ini.

Analisis data, yang yang telah diproses tersadap dan dipulihkan. Petunjuk-petunjuk terkait analisa forensic dan *steganalysis* dilakukan. Hasil dibandingkan dengan data original untuk menjawab pertanyaan mengenai penelitian ini.

Evaluasi hasil, menarik kesimpulan, dan rekomendasi untuk mengumpulkan kesimpulan dan rekomendasi dari hasil penelitian yang telah dilakukan secara berkesinambungan dari tahap 1 sampau tahap 4.

3.1 Implementasi Transmisi Audio Steganografi *Tools* (OpenPuff) dengan IPMsg

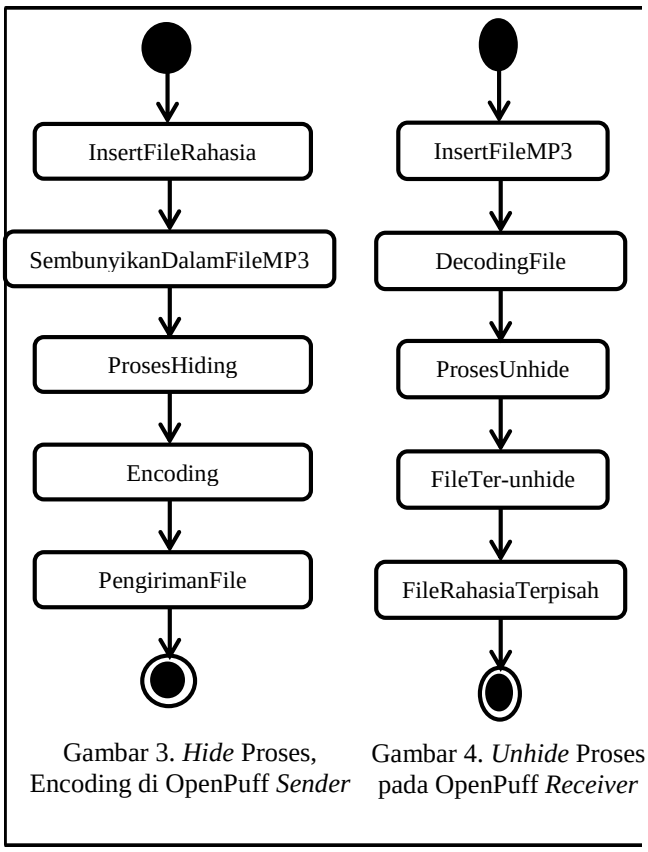
Peneliti melakukan implementasi *encoding audio steganography* dengan OpenPuff dan mengirim file *audio steganography* dengan aplikasi IPmsg.



Gambar 2. Transmisi Audio Steganografi

Pada gambar 2, Peneliti memilih apakah melakukan enkripsi pada file rahasia yang akan dikirim atau tidak, jika ya maka melalui proses *encoding* file dengan aplikasi OpenPuff sebagai tool *audio steganography*. Setelah ter-*encode*, maka file *audio steganography* dikirim ke *receiver* dengan menggunakan IPmsg.

Aktifitas file *audio steganography* yang di lakukan dengan *tool*-nya yaitu aplikasi OpenPuff dijelaskan dengan *data flow* berikut.



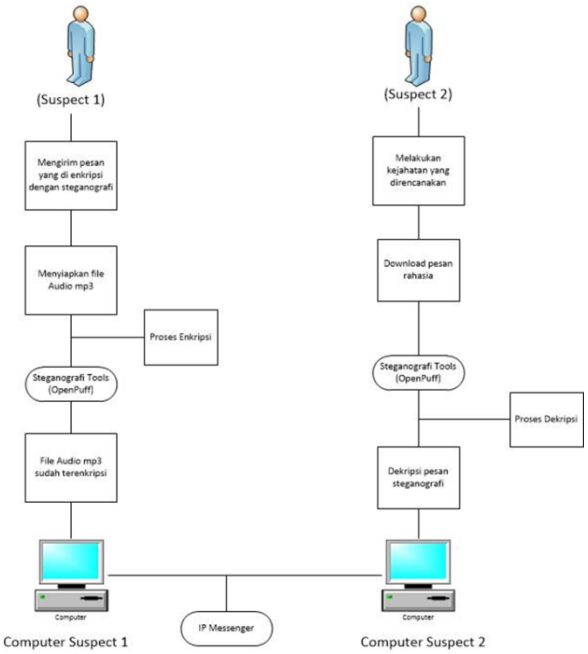
Gambar 3. *Hide* Proses, Encoding di OpenPuff *Sender*

Gambar 4. *Unhide* Proses pada OpenPuff *Receiver*

Gambar 3. *Data Flow Sending Reciever File* 4

Pada OpenPuff *sender* terjadi proses enkripsi file rahasia yang disembunyikan ke dalam file MP3. Openpuff receiver melakukan proses dekripsi file untuk memisahkan file rahasia dari persembunyiannya, yaitu file MP3.

3.2 Skenario Keseluruhan

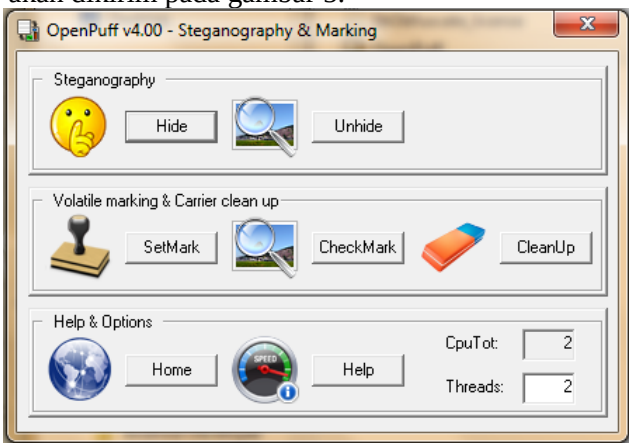


Gambar 4. Skenario Keseluruhan

3.2.2 Proses *Encoding* File Menjadi Audio Steganografi

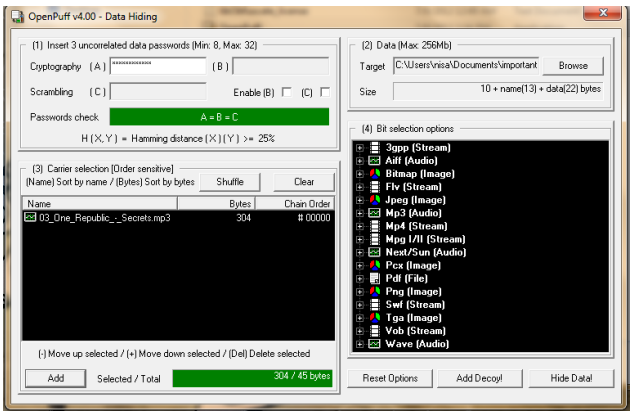
1. Buka aplikasi OpenPuff yang telah terinstal

2. Pilih "*Hide*" untuk *encoding* file rahasia yang akan dikirim pada gambar 5.



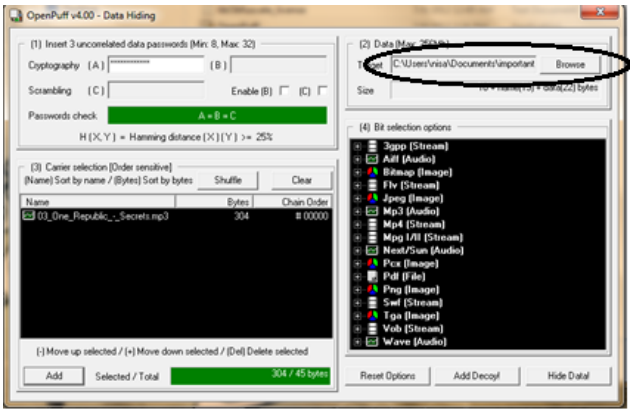
Gambar 5. OpenPuff 1

3. Pada *Cryptography* isi *password*, dalam *case* ini isi *password* di A saja cukup.



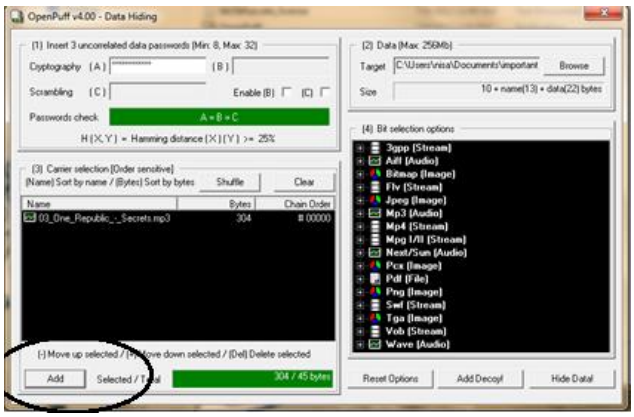
Gambar 6. Pengisian *Password*

4. Pilih file rahasia yang akan disembunyikan.



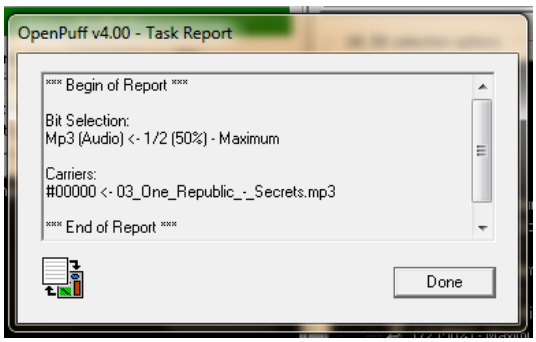
Gambar 7. *Insert File*

5. Pilih file MP3 yang digunakan untuk menyembunyikan file rahasia, kemudian klik hide, simpan di *directory* yang diinginkan.



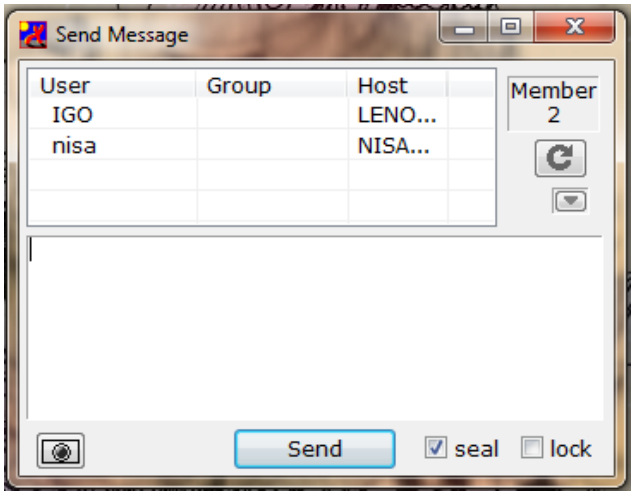
Gambar 8. Pemilihan *File* MP3

6. Tampilan ketika proses menyembunyikan file rahasia sukses.



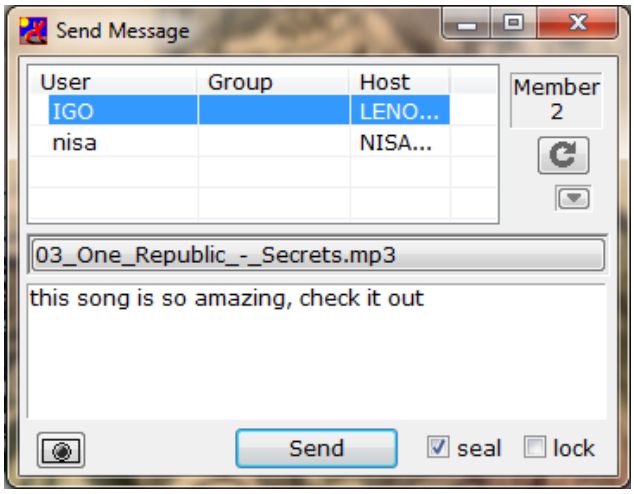
Gambar 9. *Hide File* Rahasia Success

7. Setelah berhasil ter-*hide*, maka kirim file *audio steganography* tersebut dengan IPmsg.



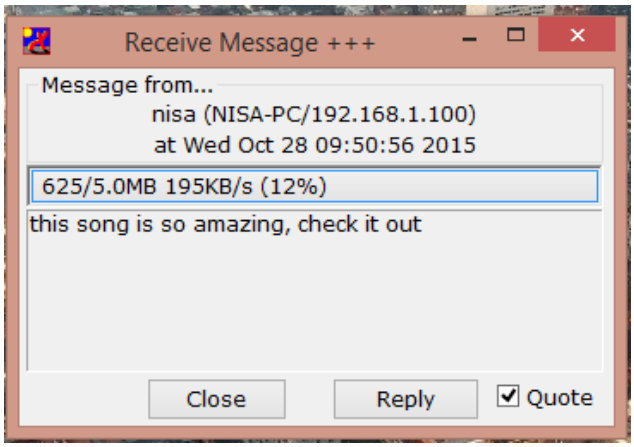
Gambar 10. IPmsg

8. Pilih *receiver*, kemudian *insert* file *audio steganography* yang akan dikirim ke *receiver*, kemudian *send*.



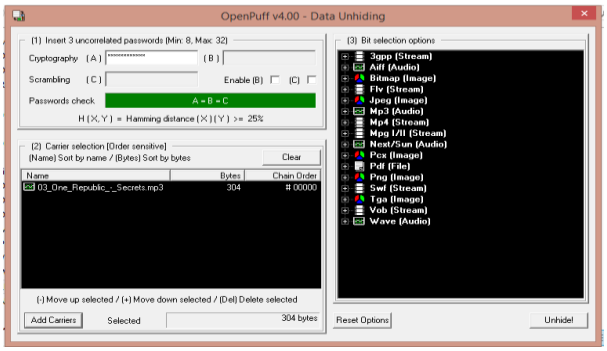
Gambar 11. IPmsg *Reciever*

9. Setelah file *audio steganography* sampai ke penerima, maka save di *directory* yang diinginkan.



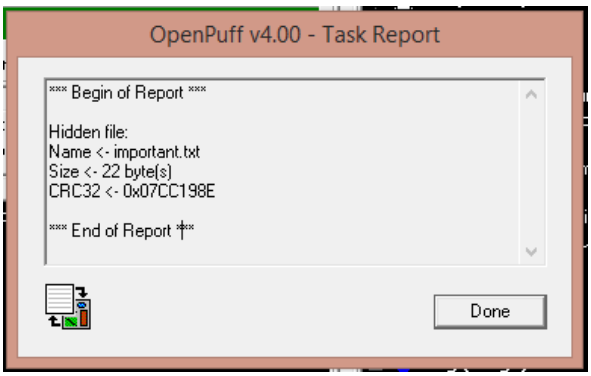
Gambar 12. Penerimaan Pesan

10. Untuk meng-*decode* atau meng-*unhide* file rahasia, maka buka OpenPuff pada *computer receiver* tersebut (Gambar 13). Masukkan *password* cryptography, kemudian pilih file yang di-*save* dari IPmsg, kemudian *unhide*.



Gambar 13. *Unhide* File Rahasia

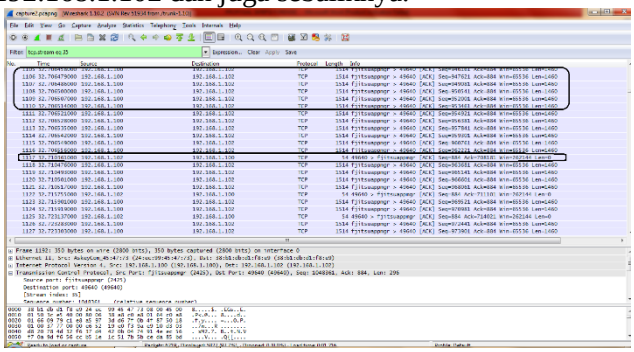
11. Meng-*Unhide* sukses



Gambar 14. *Unhide*

3.2.3 Pengamatan Lalu Lintas Data dengan *Wireshark*

Lalu lintas pertukaran data diamati dengan Wireshark. Dalam gambar di bawah terlihat jika ada pertukaran data antara kedua *host*. Data/informasi tersebut tersebut terkirim dari laptop dengan IP 192.168.1.100 ke laptop tujuan dengan IP 192.168.1.102 dan juga sebaliknya.



Gambar 15. Lalu Lintas *Wireshark*

3.2.4 Penemuan Deteksi Audio Steganografi dan Ekstraksi

Dengan tools StegAlyzerAS mengimplementasikan pendeteksian *audio steganography*. Pertama StegAlyzerAS mengecek pada laptop sender apakah terdapat aplikasi *audio steganography* tool. Pengecekkan terbukti pada gambar (Lu, 2014) berikut.LEACH memiliki fitur-fitur sebagai berikut:

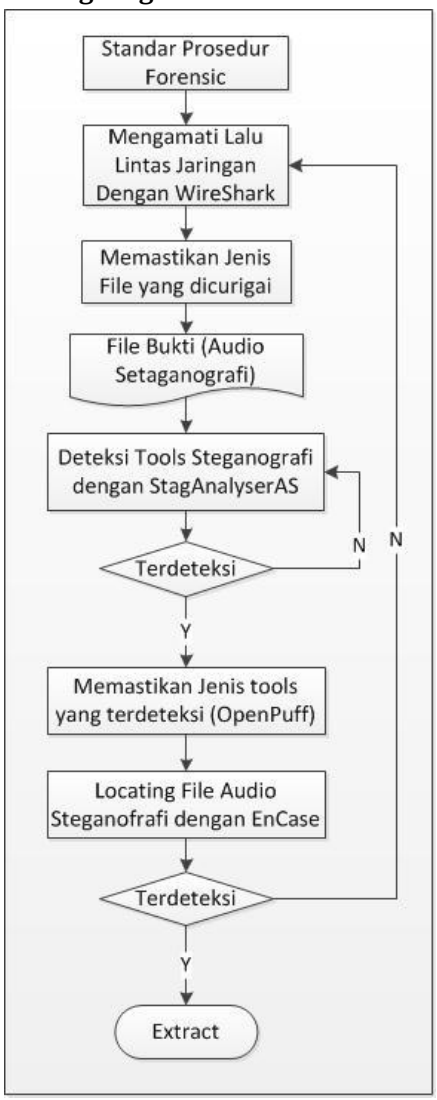
Figure 4.7: StegAlyzerAS detection result (1)

Gambar 16. Lalu Lintas Terdeteksi

Dalam gambar tesebut, terdeteksi tools *audio steganography* yaitu OpenPuff, MP3Stego,

OpenStego, MP3Stegz. Terbukti adanya tools *audio steganography* di laptop *sender*.

3.3 Diagram Flow Chart Audio Steganografi



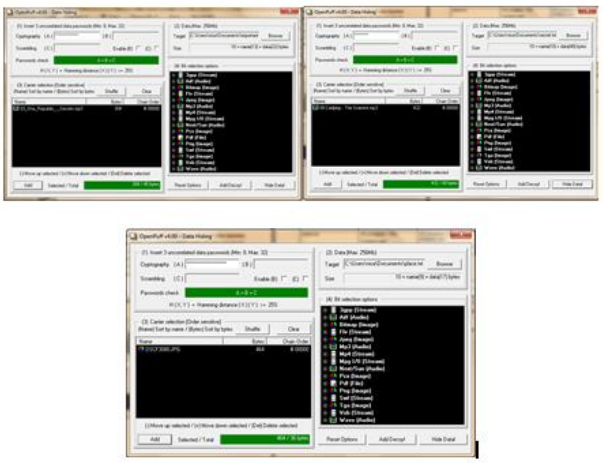
Gambar 17. *Data Flow Case Scenario*

IV. ANALISA DAN PEMBAHASAN

4.1 Pengumpulan Data

Data yang digunakan dalam proposal ini adalah sebuah file audio yang digunakan sebagai pembawa pesan (*carrier*) yang akan ditransferkan melalui IP Messenger dari PC Gin kepada Bourbon. Gin menyembunyikan sebuah pesan yang berupa .txt kedalam sebuah audio file .mp3. gin menyembunyikan file tersebut menggunakan aplikasi steganografi OpenPuff. Dalam OpenPuff Anda dapat menyembunyikan berbagai macam file ke dalam file pembawa. File pembawa juga bermacam-macam dapat berupa *image*, audio, atau video.

Dalam kasus ini, Gin menyembunyikan 3 file .txt yang berupa pesan penting kepada Bourbon di dalam sebuah lagu dan image yang biasa agar tidak diketahui atau dicurigai orang lain.



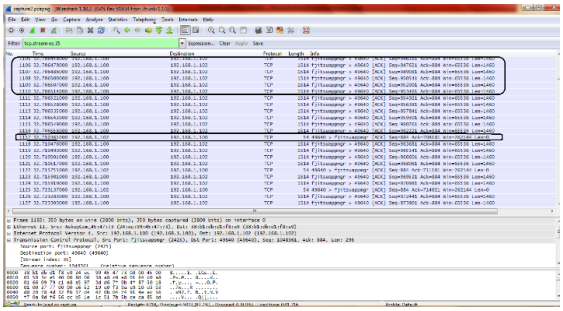
Gambar 18. Bukti File yang Disembunyikan

Secret File	Carrier File	Stego File
important.txt	03_One_Republic_-_Secrets.mp3	03_One_Republic_-_Secrets.mp3
secret.txt	09_Coldplay – The Scientist.mp3	09_Coldplay – The Scientist.mp3

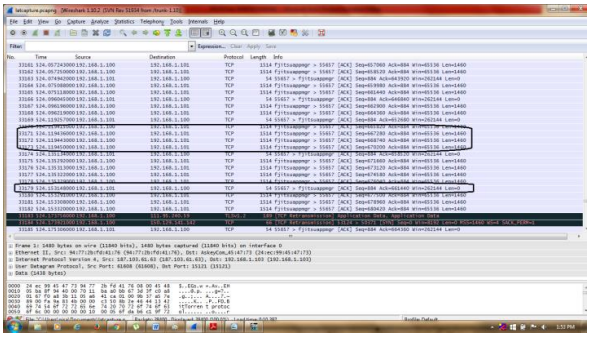
4.2 Analisa Data yang ditemukan

Analisa data yang ditemukan ini bertujuan untuk mengetahui data apa yang dikirim oleh tersangka dan jejak-jejak dari data tersebut. Hal yang pertama dilakukan adalah mengamati jaringan menggunakan wireshark. Dalam wireshark tertangkap banyak sekali aktivitas dalam jaringan tersebut, menurut buku Practical Packet Analys 2nd Edition karangan Chris Sanders, ukuran paket dalam wireshark mengandung banyak sekali informasi.

Berikut penulis tampilkan hasil *capture* jaringan dengan menggunakan wireshark yang diberi nama latcapture.pcapng dan capture2.pcapng.

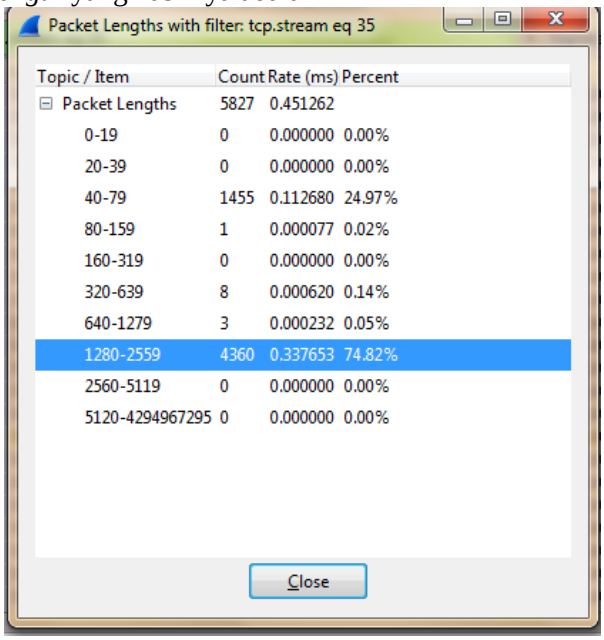


Gambar 19. *Capture* Lalu Lintas *Wireshark*



Gambar 20. *Capture* Lalu Lintas *Wireshark*

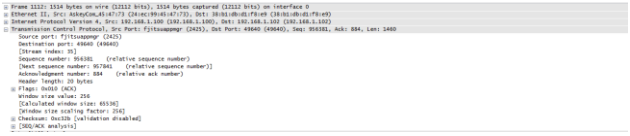
Dari hasil *capture* tersebut penulis menyelidiki *packet length* yang hasilnya adalah



Gambar 21. Bukti *Length*

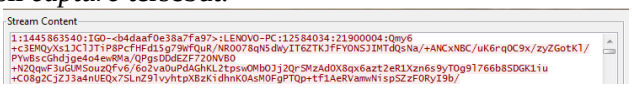
Dalam *packet length* tersebut penulis fokus di ukuran paket 1280-2559, terlihat cukup banyaknya jumlah paket yang ada di ukuran itu 74.82%. Ukuran paket yang besar mengindikasikan adanya transfer data sedangkan ukuran paket yang kecil menandakan *protocol sequence*. Berdasarkan paket *length* tersebut dapat disimpulkan bahwa file tersebut mengandung setidaknya satu atau lebih transfer data. Dapat dalam bentuk HTTP download, FTP upload atau lainnya.

Kembali pada file latcapture.pcapng, dapat dilihat jika terdeteksi adanya transfer data antara IP Address 192.168.1.100 dan 192.168.1.101 yang diduga adalah IP Address dari komputer Gin dan Boubon. Dengan menggunakan TCP *header* dapat diketahui source dan destination dari data tersebut.



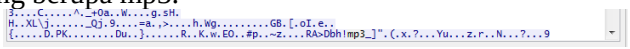
Gambar 22. *Source* dan *Destination*

Dalam wireshark penulis menggunakan fungsi Follow TCP Stream untuk melihat lebih jelas tentang hasil *capture* tersebut.



Gambar 23. *Source* dan *Destination*

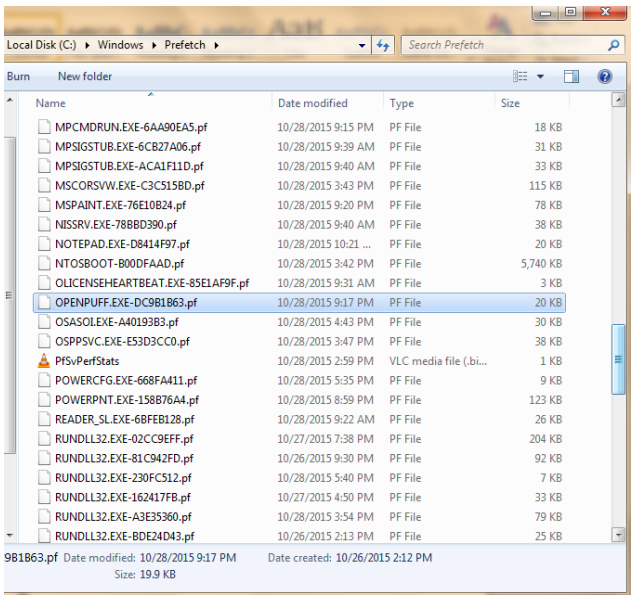
Pada *stream content* terlihat bahwa tujuan dari data tersebut adalah ke IGO-Lenovo-PC. Dapat disimpulkan jika itu adalah computer yang digunakan oleh Bourbon. Dalam *stream content* juga penulis dapat melihat jenis file yang dikirim yaitu audio file yang berupa mp3.



Gambar 24. *Stream Content*

Dalam stream content disini penulis belum dapat menemukan pesan atau chat yang dikirim antara Gin dan Bourbon. Hasil dari pengamatan jaringan menggunakan wireshark adalah diketahui IP Address dari Gin dan Bourbon dan juga format file yang dikirim dari Gin ke Bourbon adalah format mp3. Setelah melakukan analisa pada wireshark dilanjutkan dengan analisa menggunakan EnCase.

Setelah diketahui bahwa Openpuff terinstall di PC tersangka, langkah selanjutnya adalah memeriksa apakah aplikasi tersebut pernah digunakan atau tidak. Untuk mengethaui hal tersebut penulis perlu melihat dan memeriksa Windows prefect file (*.pf). Prefect file di PC tersangka terdapat di folder C:. C:\\Wimdows\Prefect. Di sana terdapat openpuff, yang berarti openpuff pernah dieksekusi.



Gambar 25. File pada *directory*

Pada analisa menggunakan wireshark sebelumnya, penulis menemukan petunjuk yang berupa pesan berikut “Hotel California” “The Very Best of The Eagles” dan “Eaglesles”. Kata tersebut digunakan sebagai kata kunci untuk mencari dengan menggunakan EnCase. Setelah dilakukan pencarian ditemukanlah sebuah file mp3 yang berupa lagu 03_Secret_One Republic.mp3 yang ada di folder D:\OpenPuff\!!”. Tidak hanya itu, masih banyak file lainnya yang ada di dalam folder tersebut.

File pertama 03_Secret_One Republic.mp3 diuji karena diduga telah dilakukan steganografi, dan terbukti jika di dalam file tersebut disembunyikan sebuah file .txt yang berisi pesan penting mengenai rencana pembunuhan mereka. 1 buah mp3 file dan 1 buah foto juga ditemukan dan terdapat pesan tersembunyi juga di dalamnya. Dalam encase juga terlihat jika masih terdapat 700 file .mp3 yang ada, tetapi hanya 3 file tersebut yang ditemukan adanya pesan tersembunyi.

V. PENUTUP

5.1 Kesimpulan

Hasil dari penelitian yang penulis lakukan adalah penggabungan beberapa tools seperti wireshark dan encase dapat sangat membantu dalam hal investigasi kasus yang berhubungan dengan network forensic ini. Semua hasil dari *capture* pada wireshark dapat menjelaskan apa saja yang terjadi pada jaringan. Wireshark digunakan untuk menangkap segala aktivitas yang terjadi pada jaringan. Encase digunakan untuk menyelidiki dan menginvestigasi serta openpuff dan IPMsg yang digunakan untuk membuat file steganografi serta untuk bertukar informasi dengan IP Address.

5.2 Saran

Penulis menyadari masih banyaknya kekurangan dari proposal ini dan tidak lengkapnya *tools* yang kami gunakan, maka dari itu penulis menyarankan untuk penelitian selanjutnya agar lebih detail dan lengkap lagi.

DAFTAR PUSTAKA

[1] Indradeep, B., & Gautam, S. (2013). Hiding & analyzing Data In Image Using Extenden PMM.

[2] Josiah, D., & Alan, S. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques.

[3] K, S., & B, M. (2014). Digital Forensic Tools And Procedures.

[4] Lu, Y. (2014). Investigating Steganography in Audio Stream for Network Forensic Investigation: Detection & Ekstraction. New Zealand.

[5] Natarajan, M., & Lopamudra, N. (2010). Steganalysis Algorithms for Detecting The Hidden Information in Image, Audio and Video Cover Media.

[6] Sanders, C. (2011). Practical Packet Analysis 2nd Edition. San Fransisco: William Pollock.

[7] Steve, B., & William, W. (2006). EnCase Computer Forensics. USA: Wiley Publishing.

[8] Vitap, K., & Narendra, B. (2013). Embedding Cypher Text In Audio Signal Using Steganography Techniques.