NETWORK FORENSIC INVESTIGASI PADA STEGANOGRAFI

Rizal Broer Bahaweres¹, Hapsari Tiaraningtias², Khoirunnisya³, Putra Hadi Kamil⁴

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 benarbenar 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 prinsipprinsip 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 faktafakta 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.





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



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.

OpenPuff v4.00 - Data Hiding	Cardena and	×
[1] Insert 3 uncorrelated data passwords Cupplography (A) Scrambling (C) Passwords check (A) H(X,Y) = Hamming distance	(Min: 8, Max: 32) (B) Enable (B) [(C) [A = B = C cc (×) (Y) >= 25%	(2) Data (Mac 256Mb) Target [C:WsertVnsk1Documentk1mpontant] Size 10 + name(13) + data(22) bytes (4) Bit selection options
(3) Carrier selection [Order sensitive] (Name) Sort by name / (Bytes) Sort by byte	Shuffle Clear	Bitmap (Image) Flv (Stream)
Name E3 03_0ne_RepublicSecrets.mp3 () Move up selected / (+) Move down a	Bytes Chain Order 301 # 000000	b::: > opeg (unage) b:::: > opeg (unage)
Add Selected / Total	304 / 45 bytes	Reset Options Add Decoy! Hide Data!

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.

🔣 Send Message	47		
User	Group	Host	Member
IGO		LENO	2
nisa		NISA	C
	Send	l	al 📃 lock

Gambar 10. IPmsg

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

Kend Message	property.		
User IGO	Group	Host LENO	Member 2
nisa		NISA	C
	r		
this song is so	amazing, chec	.mp3 k it out	
	Send	🔽 se	al 🔲 lock

Gambar 11. IPmsg Reciever

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

Receive Message +++ ×
Message from nisa (NISA-PC/192.168.1.100) at Wed Oct 28 09:50:56 2015
625/5.0MB 195KB/s (12%)
this song is so amazing, check it out
Close Reply Quote

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*.

a	OpenPuff v4.00 - Da	ta Unhiding	×
[1] Inself 3 uncorrelated passwords (M Copstography (A) Scrambing (C) Passwords check H(X,Y) = Hamming dis [2] Carrier selection (Drider sensitive) (Name) Soit by name / (Bytes) Soit by 1 Name [3] Ore_ FleptblogSecrets mp)	n: 8, Max. 32 (8) Enable (8) A = 0 = C ance (×) (V) >= 25% ytes Clear Bytes Clear 100000 100000	[1] Bit statistics options [1] Bit statistics options [1] Bit statistics options [2] All statistics [2] All statistics [3] All statistics	
(.) Move up selected / (.) Move dow Add Carriers Selected	selected / (Del) Delete selected 304 bytes	E Wore (Audio)	Unhidet

Gambar 13. Unhide File Rahasia

11. Meng-Unhide sukses

	OpenPuff v4.00 - Task Report
r	*** Begin of Report ***
	Hidden file: Name <- important.txt Size <- 22 byte(s) CRC32 <- 0x07CC198E **** End of Report ***
	Done

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.

cepture2 pcaping (Wreshark 1.10.2 (SVN Rev 51534 tron	(trunk-1.10)		The second se	X III II
File Bill View Go Contace Analyze Statistics Tal	enhorse Tools Internals Help			
REAR OPPORTON			20 GB	
OSTET BOXR (AA	••••• • • • • • • • • • • • • • • • •	C 🖉 N 😣	76 B	
Filter topstream eq.35	Expression Clear Ap	pply Save		
No. Time Searce	Distination	Protecel	longth Info	
1105 37.700418.00 147.148.1.100	197.168.1.102	1.07	1214 Littersthud, 2 40040 [YEY] 256-METEL YCK-104 RUN-12226 FUN-1400	
1106 32,706479000 192,188,1,100	192.168.1.102	TCP	1514 Tjittsuepongr > 49640 [ACK] Sed-947621 ACK-884 Win-toS56 Len-1460	
1105 32 705500000 192 160 1 100	197, 160, 1, 102	TCP	1514 fratewaren > 49040 [ACK] Sec 050541 Ack 804 km 85536 [an 1460	
1108 22 705507000 182 159 1 100	102 168 1 102	TYP	1514 Filtransport + 4060 FETT Score/S1014 Actuality ViceS1526 Long 460	
1110 12 200514000 192 165 1 100	192, 165, 1, 102	TCP	1514 fittememory > 49640 [ACK] Sec. 951461 Adv-804 Min-85516 (an-1460)	
1111 32,706521000 192,168,1,100	192, 168, 1, 102	TCP	1514 filtsungener > 49640 [ACK] Secw954921 Ackw884 Winw65526 Lenv1460	
1112 32,708528000 192,148,1,100	197, 188, 1, 102	TEP	1514 fiitsungungr > 41640 [ALK] Seg=356581 Ack=884 Win=85556 Lam=1460	
1113 32.705535000 192.168.1.100	197.168.1.102	TCP	1514 fortsunppopr > 49640 [ACK] Sec-957941 Ack-804 Win-65536 Len-1460	
1114 32,705542000 102.168.1.100	192.158.1.102	TCP	1514 [jitsusppng: > 40640 [ALK] Sug-059201 Ack-884 Win-85526 Lun-1460	
1115 32,700549000 192,168,1,100	192.108.1.102	TCP	1514 fjitsungpogr > 40610 [ACK] See 000761 Ack 804 Win 05550 Len 1600	
1116 32.704516000 102.168.1.100	192.168.1.102	TCP	1514 filtswappmer > 40640 [ACK] Scc=062221 Ack=004 Win+65516 Lon=1460	
1337 32, 210161000 192, 148, 1, 102	197.168.1.100	TEP	14 41040 > fjitsuappage [ACK] Seg-834 Ark=738181 Win=202144 Las=0	
1118 32.710476000 192.168.1.100	192.168.1.102	TCP	1514 fjitsusppngr > 45640 [ACK] Seq=363681 Ack=884 Win+85536 Len+1460	
1110 57.710495000 197.168.1.100	192,188.1.102	TEP	1514 Fjitsaappegr > 40640 [ALK] Saq=005141 Ack=004 Win=05510 Lan=1460	
1120 32.710501000 192.168.1.100	192.168.1.102	TCP	1514 fyitsweppigr > 49640 [ACK] Seq-966601 Ack-884 Win-65536 Len-1460	
1121 32./1051/000 102.168.1.100	192.168.1.102	TCP	1514 []itsuappign > 40640 [ALK] Scg=068061 Ack=884 Win=85556 Lon=1460	
1122 32.713753000 192.166.1.102	192.108.1.100	TEP	14 49040 > T11TSLARDING" [ACK] SEC 834 ACC 711101 W10 702144 LED 0	
1125 52./15501000 152.166.1.100	192.100.1.102	i çe	1514 (Jitsupping & enero (Act) Schebessizt Access #Inepside Company	
1174 37.713419000 197.168.1.100	197, 100, 1, 102	10.0	1514 TITKERphor > 40040 [ALK] Segrerowit Accesse #1040556 Lengtedo	
1123 52.725137000 192.106.1.102	197.186.1.100	100	14 49660 A TJTCSORDARY (ACK) SERVICE ACCOUNTERED AND A TOTAL AND A	
1127 22 22220200 122 120 1 100	102,100,1,102	700	The second	
1121 321723303000 1921200011100		14.6	The chickedball is used for the second second second second	
				,
Frame 1192: 350 bytes on white (2000 bits), 3	50 bytes captured (2800 bits) on in	iterface 0		
Ethernet II, Src: AskeyCom_45:47:73 (24:ec:2)	9:45:4/:73), Date 38:51:cb:cl:f8:e9	(18:b1:cb:c1:f8	e)	
(a) Internet Protocol Version 4, Src: 192.168.1.	100 (192.165.1.100), Det: 192.168.1	.102 (192.168.1.)	(2)	
E Transmission Control Protecol, Sec Port: 131	tsvappmgr (2425), DSt Port: 49640 (49840), 360: 204	1961, Adki 884, Luni 195	
Searce parts tystsuepondr (2425)				
Destination port (49640)				
Concerns and an INCOM				
0000 at 14 db db 18 c0 24 cc 03 45 47 74 09 7	10 45 (0) R \$ 1(n 1			
0010 01 50 Te at 40 00 50 06 38 at c0 at 01 0	64 c0 s8 .Pc.0 8d.			
0120 01 65 09 78 61 68 45 97 34 66 75 09 45 1	37 50 18			
0040 d8 20 78 4d 12 f6 17 64 42 0b 04 74 91 4	te ec 16 . x92.7. 87.9.V			
0050 17 0s 9d 16 56 cc b5 1e 1c 51 7b 5b ce c	As \$5 bdVQ[[
Card Sand or rank on Paris	In APR, Danis on NETL NETCOL, Distanced it	HIGHL LAND NO. 11	175. Public Date in	

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	Carrier File	Stego File
File		
important.t	03_One_Republi	03_One_Republi
xt	cSecrets.mp3	cSecrets.mp3
secret.txt	09_Coldplay –	09_Coldplay –
	The	The
	Scientist.mp3	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.

troutience as 15	P Security Char	Annia Sana		
NO STREET ST	- Doubletter Control	And a second	took ble	
101 12.700 102.100	107.100.1.100	THE REAL PROPERTY AND INCOMENTAL PROPERTY AND INTENTE AND INTENTI AND INTENTE AND INTENTE AND INTENTE	THE PUTTING AND	2
1105 32.786479000 192.160.1.100	192.160.1.102	TCP	1514 tystrungengr > 40640 [ADK] Seq-047621 Ack-884 Win-65536 Les-1460	
10/ S2./06456000 102.1eX.1.100	192,188,1,102	102	1514 fjilsangprgr > 41640 [ALX] Sag=345081 Ack=884 Win=553.08 Las=1480	
108 32.766500000 192.168.1.100	192.168.1.102	TCP	1514 toitsiapangr > 49640 [ACK] Seq.956541 Ack-884 Win-65536 Len-1460	
103 32.706507000 132.168.1.100	192.168.1.102	TCP	1514 fjilswapper > 40640 (ACK) Sep+952001 Ack+884 Wir+65536 Lem+1460	
110 32,700514000 192,168,1,100	147,168,1,107	TEP	1514 fjiftsangengr > 49640 [ACK] Swg-W15468 Ack-884 Wis-85556 Lws-1460	
111 32.706521000 192.168.1.100	192.168.1.102	TOP	1514 Fjitskappingr > 49640 [ACK] Seq=954921 Ack=864 Win=65556 Lon=1460	
113 12.700520000 102.100.1.100	107.108.1.107	100	1114 Fyrtramppegr > 40640 [AEX] Imp+H6181 Ach+B84 Wim+B1106 Las+1460	
111 32.706535060 192.166.1.100	192,100,1,102	100	1514 THTERDORP > 49440 [ALA] 540-15/941 ACC-884 WTR-65536 LBH-1460	
117 33 76710000 103 100 1 100	AP2.100.1.100	700	The foregoing a story (see) for an and the story of the last	
116 22 766556060 102 168 1 100	183 168 1 103	178	Till fillcomments a field [NV] Search 111 Actuality March 16	
117 12 735351000 122 165 1 102	182 144 1 100	17.0	MA ANNO & FUTULATIONS (NY) SAMURA AVAILABLE MANAGEMENT	`
115 32, 210426200 132, 165 1, 100	112,164,1,102	TOP	1514 FULFORMARY & 45640 (ACC) SenaMIMAL ACCURATE STRATSTAL PROFILED.	-
110 17./20491060 107.168.1.100	187,108,1,107	TUP	1114 fiitsammer > 40440 [ALX] 100-201141 Ack-204 Min-00100 Lum-1400	
120 32.710501000 192.100.1.100	192,164,1,102	TCP	1514 fortzungener > 49640 [ACK] Sep-900001 Ack-884 Win-05536 Len-1400	
121 22.750517000 102.168.1.100	192.168.1.102	TOP	1514 fjitcooppege > 40640 [ACK] Son-268061 Ack-884 Win-65526 Low-1460	
122 32,715255000 142,160,1,102	197,168,1,100	TCP	54 49940 > fjittsiagong: (ACK) Seg-MAI Ack-711101 Win-762144 Les-0	
123 32.715901000 192.168.1.100	192.168.1.102	TCP	1514 fjitskappingr > 49640 [ADC] Seg=969521 Ack=884 Wir=65536 Les=1460	
124 52,715919060 192,168,1,100	182,168,1,102	TEP	1514 fjitssappnor > 49640 [ACK] Saq=870981 Ack=864 Wiz=85556 Las=1460	
125 32.723137000 152.168.1.102	192,168,1,100	TCP	54 49540 > 73155sappeg: [ACK] Seg=554 Ack=714021 W1#=262144 Les=0	
126 82.728289060 102.168.1.100	197.168.1.107	102	1514 fjitzaappegr > 40040 [ALK] Saq+2/2441 Ack+804 Wis+85520 Las+1480	
127 32.723303000 152.160.1.100	192,164,1,102	TOP	1514 tystrangangr > 49640 [ACK] Seq-973901 Ack-884 Win-65556 Les-1460	
me 1192: 350 bytes an white (2000 bits), 3	0 bytes captured (2000 bits) on a	eterface 0		
erret 11. brut Askaptum_45:47:78 CM:ex.rP	tothe47:730. Date #8thinderilef8es	en (sucharderitarfu	(9)	
erret Protocol Version 4, Soci 192,168.1.	100 (192,168.1,103), Det: 192,168.	1.105 (192.166.1.	(02)	
numission Control Protocol, Snc Port: fji	Lscappegr (2425), Dst Part: 49640	(45640), Seq: 104	1361, Auk: 884, Lon: 235	
ource port: fjitsueponor (2021)				
Destingtion port: 49640 (49640)				
Stream index: 25				
the second				
01 10 1r +1 40 00 A0 00 31 A5 40 A5 01 4	H HD MA . Politica da			
원생안격실생성원 권생감안석!	5.99 38 - it y = A.P.			
dia 20 78 44 32 fe 37 de 42 th 04 74 95 4	e ec 56 . x42.7. 81.9.1			
17 0a 9d 16 56 cc b5 Le Lc 51 7b 5b ce c	a \$5 bdVQ[[

latiophore.pcoproj (Weeshark 1.00.2 (SVN Rev 53	554 hore (trank-1.12)		States and a subscription of the subscription	
ie Edit View Go Capture Analyze Statisti	s Telephony Iools Internals	Help		
	* * • • * • (1)	QQE	1. 🗇 📓 (K) 👭 (K) 🔛	
Ret	· Espress	and Charl	Appy Saw	
Time Source	Destruction	Protocol	Length Info	
33242 324.057243000192.168.1.100	192-165-1-101	TCP	1314 Filtseapper > 55457 [ACK] Sep+657060 Ack+884 Win+65336 Len+1460	
33262 \$24.057250000 192.168.1.100	192.168.1.101	TCP	1514 fjitsvappnpr > 55657 [ACK] Seg=658520 Ack+884 Win=65536 Len=1460	
33163 524.074942000 192.168.1.101	192.168.1.100	TCP	54 55857 > fjitsuapangr (ACK) Seg+884 Ack+643920 Win+202144 Len+0	
33164 524.075088000192.168.1.100	192,168.1.101	TCP	1514 fjitssappngr > 55657 (ACK) Seq=653980 Ack=884 Win=65536 Len=1460	
33185 324.075118000 192.168.1.100	192.168.1.101	TCP	1514 fjitsumppngr > 55857 [ACK] Seq+661440 Ack+854 Win+65516 Len+1460	
33166 524.096045000 192.165.1.101	192,168.1.100	TCP	54 55657 > fjitsuappegr [ACK] Seq=804 Ack>6468040 Win+262144 Len=0	
33287 124.096196000192.168.1.100	192.168.1.101	TCP	1514 Fjitsuappegr > 55617 [ACK] Sep+662900 Ack+864 Win+65136 Len+1460	
33168 524.096219000192.168.1.100	192,168.2.101	TCP	1514 fjitsamppegr > 55617 [ACK] Seq=664360 Ack=884 Win=65336 Lev=1460	
33169 524.119357000192.168.1.101	192.168.1.100	TCP	54 55657 > fjitsuappmpr (ACK) Seq=884 Ack=652660 Win=262244 Let=0	
11110 100 11011000 107.168.1.100	192.188.1.191	10	THE ALIGNMENTS PARTY (WEST PROPERTY VERSEL AND ALIGNMENTS	
33171 524,119436000 192,168,1,100	192.168.1.101	TCP	1514 fjitsampengr > 55657 (ACK) Seg=667280 ACK=884 Win=65536 Len=1460	
33172 524.119443000192.168.1.100	192.165.1.101	TCP	1514 fjitzaappegr > 15617 [ACK] Seq=668740 Ack=884 Win=65156 Len=1460	
11173 524.119450000 197.168.1.100	192.168.1.101	TCP	1514 fjitsingpngr > 55437 (ACK) Seq+670200 Ack+884 Win+65526 Len+1440	
33174 524.135154000132.168.1.101	192.168.1.190	TOP	54 55657 > 1)105wappegr (ACK) 560+684 A2K-653520 Win+262244 Lee+0	
33175 524.135792000192.168.1.100	197.168.1.101	TCP	1514 fjitsappnpr > 55657 (ACK) Seg=671660 Ack=884 Win=65536 Len=1460	
33176 524.135313000192.168.1.100	192,168.1.101	TCP	1514 fjitsvappepr > 55857 (ACK) Seg+673120 Ack+884 Win+65536 Len+1460	
33377 324.135322000192.168.1.100	192.168.1.101	TCP	1514 Fjitssappage > 55657 [ACK] Seq=674580 Ask=884 Win=65536 Lan=1460	
12128 524 155129000 182 168 1 100	192 165 1 185	TCP	1114 Faitzussenge x 15812 (#FF) Separations Ariselli Ariselli Ariselli (ariselli Ariselli Ari	
33179 524.153140000 192.168.1.101	192.160.1.100	TCP	54 55657 > fjitsuappegr [ACK] Seq+804 Ack+661440 Win+262144 Len+0	
33153 324.155291000 197.168.1.100	197.115.1.105	TOP	1514 FJTELEDDADF > 55657 (ACK) SEDME7/500 ACKWESE WINNESSIE LWIN1460	
33181 324.153308000 192.168.1.100	192,168.1.101	TCP	1514 Fjitsamppngr > 55657 (ACK) Seg+678560 Ack+884 Win+65536 Len+1460	
33182 524.153320000 192.168.1.100	192,168,5,100	TCP	1514 fjitssappngr > 55657 [ACK] Seq=680423 Ack=884 Win=65136 Len=1460	
		TEMIN	189 [TEP Retransmission] Application Data: Application Data	
11134512411739210001924158111100	100000000000000000000000000000000000000	105	66 [TCF Retrainelission] 33124 - 55321 [SW] See-0 With-BIR2 Letted RS-1440 WS-4 5404 [PDB	41
33145 124.175306000182.144.1.101	192,168,1,100	TCP.	54 55857 > fjitsuappegr (ACK) Seq+884 Ack+864350 Win+202144 Len+0	
raws 1: 5480 bytes as wire (13840 bits therest II, Src; 5417728rf043178 (pt hierest Pational Yawiss 4, Src; 187, ser Bargen Protocol, Src Port: 4440 Alls (5418 bytes) 0 24 et 09 45 47 73 94 77 15 66 41 7 0 55 hs PT 94 45 00 70 11 hs 40 50 6 0 58 00 f 94 43 14 50 00 50 11 hs 40 50 6 0 58 00 f 94 43 14 50 00 50 11 58 40 50 6 0 58 00 f 94 43 14 50 00 50 11 58 40 50 6 0 58 00 f 94 43 14 50 00 50 11 58 40 50 6 0 58 00 f 94 43 14 50 00 50 11 58 40 50 6 0 58 00 f 94 40 14 50 50 51 50 50 50 50 50 50 50 50 50 50 50 50 50	 1480 hytes captured (115 1177;16):163:41176), Dot: Aske 03.65.63 (1277:103.65.63), Dot (61660), Ont Port: 35121.0 6 00 00 45 48 5.150, v = 7 36 7 f co 36, 0, v = 7 36 7 47 03, 0, v = 	00 bits) er Com_451471 it: 102.166 (5121) aEN g=7 	(derface 0 () (24 (− (34) − (34) (17)) () (34) (34) (34) (34) (34) (34) (34) (3	
0 19 74 14 11 72 72 16 1e 74 29 79 7	2 67 74 65 63 itTorren t #	retec		
A 14 14 100 100 100 100 100 100 100 100 1	- lot (1 lot 71 - c)			

Gambar 20. Capture Lalu Lintas Wireshark

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

Packet Lengths with fit	lter: tc	p.stream e	eq 35	x
Topic / Item	Count	Rate (ms)	Percent	
Packet Lengths	5827	0.451262		
0-19	0	0.000000	0.00%	
20-39	0	0.000000	0.00%	
40-79	1455	0.112680	24.97%	
80-159	1	0.000077	0.02%	
160-319	0	0.000000	0.00%	
320-639	8	0.000620	0.14%	
640-1279	3	0.000232	0.05%	
1280-2559	4360	0.337653	74.82%	
2560-5119	0	0.000000	0.00%	
5120-4294967295	0	0.000000	0.00%	
	ſ	Close		
		_,		

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.

۰.	Have aller and over on the (little over), and over capter or (little over) on meetings o
e.	Ethernet II, Src: AskeyCom_45147173 (241ec199145147173), Dst: 381b1/db1d1/f81e9 (381b1/db1d1/f81e9)
£.	Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Ost: 192.168.1.102 (192.168.1.102)
5	Transmission Control Protocol, Src Port: fjitsuappmgr (2425), Est Port: 49640 (40640), Seq: 956381, Ack: 834, Len: 2460
	Source port: fjitsuappmgr (2425)
	Destination port: 49640 (49640)
	[Stream index: 35]
	Sequence number: 956381 (relative sequence number)
	[Next sequence number: 957841 (relative sequence number)]
	Acknowledgment number: 854 (relative ack number)
	Header Tength: 20 bytes
	# Flags: 0x010 (ACK)
	Window size value: 256
	Calculated window size: 655861
	Diindow size scaling factor: 266
	Checksum: Osc32b [validation disabled]
	[Sto/ACK analysis]
	Fred one work of

Gambar 22. Source dan Destination

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



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.

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.

ca	Disk (C:) Vindows Prefetch		Search Prefetch		
ırn	New folder			8≡ ▼ 🗍	
	Name	Date modified	Туре	Size	
	MPCMDRUN.EXE-6AA90EA5.pf	10/28/2015 9:15 PM	PF File	18 KB	
	MPSIGSTUB.EXE-6CB27A06.pf	10/28/2015 9:39 AM	PF File	31 KB	
	MPSIGSTUB.EXE-ACA1F11D.pf	10/28/2015 9:40 AM	PF File	33 KB	
	MSCORSVW.EXE-C3C515BD.pf	10/28/2015 3:43 PM	PF File	115 KB	
	MSPAINT.EXE-76E10B24.pf	10/28/2015 9:20 PM	PF File	78 KB	
	NISSRV.EXE-78BBD390.pf	10/28/2015 9:40 AM	PF File	38 KB	
	NOTEPAD.EXE-D8414F97.pf	10/28/2015 10:21	PF File	20 KB	
	NTOSBOOT-B00DFAAD.pf	10/28/2015 3:42 PM	PF File	5,740 KB	
	OLICENSEHEARTBEAT.EXE-85E1AF9F.pf	10/28/2015 9:31 AM	PF File	3 KB	
	OPENPUFF.EXE-DC9B1B63.pf	10/28/2015 9:17 PM	PF File	20 KB	
	OSASOI.EXE-A40193B3.pf	10/28/2015 4:43 PM	PF File	30 KB	
	OSPPSVC.EXE-E53D3CC0.pf	10/28/2015 3:47 PM	PF File	38 KB	
	📥 PfSvPerfStats	10/28/2015 2:59 PM	VLC media file (.bi	1 KB	
	POWERCFG.EXE-668FA411.pf	10/28/2015 5:35 PM	PF File	9 KB	
	POWERPNT.EXE-158B76A4.pf	10/28/2015 8:59 PM	PF File	123 KB	
	READER_SL.EXE-6BFEB128.pf	10/28/2015 9:22 AM	PF File	26 KB	
	RUNDLL32.EXE-02CC9EFF.pf	10/27/2015 7:38 PM	PF File	204 KB	
	RUNDLL32.EXE-81C942FD.pf	10/26/2015 9:30 PM	PF File	92 KB	
	RUNDLL32.EXE-230FC512.pf	10/28/2015 5:40 PM	PF File	7 KB	
	RUNDLL32.EXE-162417FB.pf	10/27/2015 4:50 PM	PF File	33 KB	
	RUNDLL32.EXE-A3E35360.pf	10/28/2015 3:54 PM	PF File	79 KB	
	RUNDLL32.EXE-BDE24D43.pf	10/26/2015 2:13 PM	PF File	25 KB	

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.