# Analisis Digital Forensik pada *File Steganography* (Studi kasus : Peredaran Narkoba)

Agung Purnama Saputra[1], Husni Mubarok[2], Nur Widiyasono[3]

*Mahasiswa Teknik Informatika dan Dosen Teknik Informatika, Universitas Siliwangi*
*Jalan Siliwangi No.24 Kota Tasikmalaya Kode Pos 46115 KotakPos 164*
[1]agung.p@student.unsil.ac.id
[3]nur.w095@gmail.com

*Dosen Teknik Informatika,Universitas Siliwangi*
*Jalan Siliwangi No.24 Kota Tasikmalaya Kode Pos 46115 KotakPos 164*
[2]husni.mubarak@unsil.ac.id

*Abstract*— **Advances in technology in addition to bringing positive effects also had a negative impact, some examples of organized crime including the activities that lead to terrorism and illegal trade such as narcotics, have been identified utilizing steganography techniques to communicate and convey messages among the group. Steganography is the art and science of writing hidden messages or hide such a way that besides the sender and the recipient, no one knows or realizes that there is a secret message. then the role of digital forensics as a method of proving a criminal case digitally becomes extremely important, Digital forensics is the use of techniques of analysis and investigation to identify, collect, examine and preserve evidence / information is magnetically stored / encoded on a computer or digital storage media as evidence to expose crimes legally defensible. The purpose and goal of this thesis is to explain how to find digital evidence using the hidden steganographic techniques, so that the information obtained is an accurate facts for their designated purpose. There are many tools that can be used in forensic cases for memeriksabarang evidence, but in this study the tools used is WinHex and InvisibleSecrets.**

*Keywords*— **Digital Evidence, digital forensic, steganography, WinHex, InvisibleSecrets.**

## I. PENDAHULUAN

### A. *Latar Belakang*

Kemajuan teknologi dan industri yang merupakan hasil dari budaya manusia disamping membawa dampak positif, dalam arti dapat didayagunakan untuk kepentingan umat manusia juga membawa dampak negatif terhadap perkembangan dan peradaban manusia itu sendiri. Beberapa contoh *organized crime* termasuk aktivitas yang mengarah pada terorisme dan perdangan ilegal seperti narkotika, telah teridentifikasi memanfaatkan teknik *steganography* untuk berkomunikasi dan menyampaikan pesan-pesan diantara kelompoknya.

Steganografi sebagai sistem dari teknologi informasi bisa dimanfaatkan untuk tujuan kejahatan sekaligus membongkar kejahatan. Steganografi merupakan metode untuk menyembunyikan suatu pesan didalam pesan yang lain dalam bentuk media digital.

Kejahatan berbasis teknologi mengalami peningkatan dalam berbagai modus, oleh karena itu diperlukan suatu mekanisme ilmiah untuk menganalisis dan menelusuri bukti –bukti digital yang ada, baik yang disimpan maupun ditranmisikan melalui komputer atau perangkat digital lainya.

Kejahatan steganografi pernah terjadi pada kasus terorisme yang dilakukan oleh kelompok radikal al-qaeda yaitu ditemukannya ratusan dokumen yang disembunyikan pada *file* video, diantaranya dokumen yang berisi gagasan perebutan kapal pesiar dan rencara penyerangan di eropa.[1]

Merujuk pada data diatas maka pemerintah indonesia mengeluarkan Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik dan/atau hasil cetakannya merupakan bukti yang sah, maka peran digital forensik sebagai metode pembuktian suatu kasus kejahatan secara digital menjadi sangat penting.

Bukti digital yang ditemukan dalam kasus sebagian besar dapat langsung dibaca dan dianalisis oleh analis forensik dan investigator sesuai dengan tahapan forensik. Analis forensik adalah tim yang bertugas mengumpulkan barang bukti digital dan melakukan analisa terhadap barang bukti digital yang ditemukan, sedangkan investigator adalah tim yang melakukan penyelidikan hingga penyidikan pada kasus yang sedang ditangani.

Namun tidak sedikit juga barang bukti digital yang dienkripsi, disembunyikan ataupun disamarkan oleh pelaku kejahatan digital seperti pada kejahatan narkoba dengan tujuan agar bukti tersebut tidak dapat dibaca dan dianalisis oleh analis forensik maupun inestigator sehingga tidak dapat dipreesentasikan dalam persidangan.

### *B. Rumusan Masalah*

Merujuk pada latar belakang yang telah diuraikan sebelumnya maka permasalahan dapat dirumuskan sebagai berikut :

1) Bagaimana proses investigasi file steganography

2) Bagaimana menemukan digital evidance pada file steganography

### *C. Batasan Masalah*

Batasan masalah dalam penelitian mengenai Analisis Digital Forensik pada *File Steganography* ini adalah :

1) Penelitian tidak membahas secara detail algoritma seteganografi yang digunakan terhadap *file* barang bukti

*2) Tools* yang digunakan dalam penelitian ini adalah *WinHex, FTK imager* dan *invesible secrets,*

*3)* Penelitian tidak membahas mengenai jenis barang bukti digital yang lain selain file seganografi.

*4)* Penelitian tidak membahas digital forensik secara keseluruhan, hanya membahas mengenai pengolahan barang bukti digital yaitu *file* steganografi.

### *D. Tujuan Penelitian*

Berdasarkan permasalahan yang telah diuraikan, maka tujuan dari penelitian ini adalah :

*1)* Mengetahui proses investigasi pada file steganografi

2) Menemukan digital evidence pada file steganografi

### *E. Manfaat Penelitian*

Manfaat dari penelitian ini adalah dengan menggunakan tools digital forensik setiap kasus yang menggunakan fasilitas teknologi informasi dapat dibuktikan dan diakui keabsahannya. Sehingga bukti data digital dapat dijadikan barang bukti yang sah untuk digunakan dalam persidangan.

## II. LANDASAN TEORI

### *A. Pengertian steganografi*

Steganografi merupakan seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan cara tertentu sehingga selain si pengirim dan si penerima, tidak ada seorang pun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Istilah steganografi *(steganography)* berasal dari bahasa Yunani, yaitu *steganos* yang berarti penyamaran atau penyembunyian dan *graphein* yang berarti tulisan. Jadi steganografi *(steganography)* bisa diartikan sebagai seni menyamarkan/menyembunyikan pesan tertulis ke dalam pesan lainnya [2].

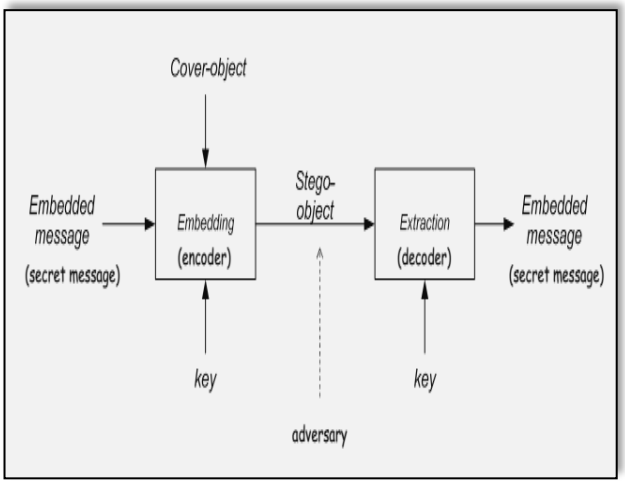
### *B. Tujuan Steganografi*

Teknik steganografi banyak digunakan untuk menyembunyikan informasi rahasia dengan berbagai maksud. Salah satu tujuan dari steganografi adalah mengirimkan informasi rahasia melalui jaringan tanpa menimbulkan kecurigaan. Disamping itu steganografi juga dapat digunakan untuk melakukan autentikasi terhadap suatu hasil karya sebagaimana pemanfaatan watermarking. Namun steganografi juga bisa digunakan sebagai sarana kejahatan yang dapat digunakan oleh para teroris dan sindikat narkoba untuk saling berkomunikasi satu dengan lainnya.

### *C. Cara Kerja Steganografi*

Steganografi memerlukan setidaknya dua properti. Properti pertama adalah wadah penampung *(cover)* dan yang kedua adalah data atau pesan yang disembunyikan. Untuk meningkatkan tingkat keamanan data yang disimpan, dapat dilakukan dengan menambahkan properti kunci *(key)* rahasia. Properti kunci ini dapat berupa kunci simetris maupun kunci public atau privat. Berkas hasil dari proses steganografi sering disebut sebagai berkas stego *(stego file)* atau stego objek. [3]

Gambar 1 menunjukan proses atau cara kerja steganografi.




Gambar 1. Cara kerja steganografi

### *D. Pengertian digital forensik*

Ada beberapa definisi yang bisa dijadikan acuan tentang apa sebenarnya Digital Forensik. Menurut Marcella [4] digital forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi barang bukti digital dalam kejahatan komputer. Istilah ini relatif baru dalam bidang komputer dan teknologi, tetapi telah muncul diluar term teknologi (berhubungan dengan investigasi).

Menurut Budhisantoso[5], digital forensik adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat

penyimpanan sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum. Dapat disimpulkan bahwa digital forensik adalah penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti/informasi yang secara magnetis tersimpan/disandikan pada komputer atau media penyimpanan digital sebagai alat bukti dalam mengungkap kasus kejahatan yang dapat dipertanggungjawabkan secara hukum.

### *E. Barang bukti digital*

Menurut buku *Digital Evidence and Computer Crime Third Edition* (2011)[6], pengertian barang bukti digital/*digital evidence* adalah semua jenis tipe data yang disimpan dan atau dikirimkan menggunakan komputer dimana suatu pelanggaran terjadi. Pelanggaran bisa diartikan sebagai "maksud" atau "alibi". (diadapsi dari Chisum, 1999). Pengertian data berdasarkan konteks ini, berupa kombinasi angka *(binary)* yang mewakili informasi dari berbagai teks, gambar, audio atau video. Dengan mempertimbangkan jenis data digital yang ada dan bagaimana kemungkinan manfaat yang diberikan dalam suatu penyelidikan.

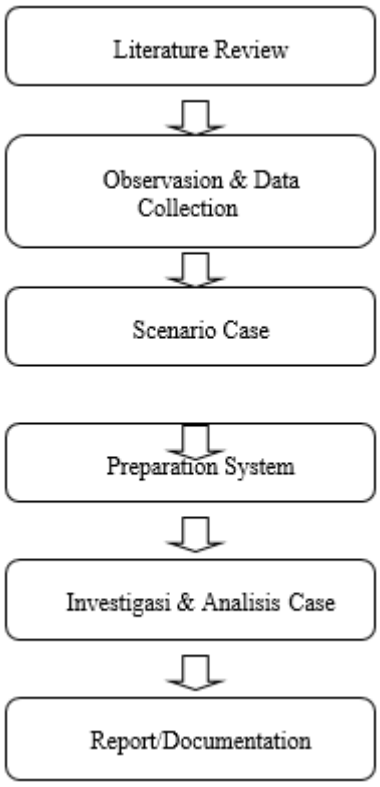
Definisi bukti digital yang diberikan kelompok kerja bersama *"The Scientific Working Group on Digital Evidence"* (SWGDE) adalah *"Information of probative value stored or transmitted in digital form".* Definisi tersebut bila diterjemahkan secara bebas sebagai berikut, bukti digital adalah segala informasi yang bersifat membuktikan terhadap nilai yang tersimpan atau ditransmisikan dalam bentuk digital. Berdasarkan definisi tesebut, bukti digital tidak hanya meliputi bukti yang dihasilkan atau ditransmisikan melalui jaringan komputer saja, akan tetapi juga termasuk perangkat audio, video bahkan telpon selular. [7]

### *F. WinHex*

WinHex adalah editor hexadecimal universal, yang paling utama adalah sangat membantu dalam bidang computer forensics, data recovery, proses data dalam tingkat yang rendah dan keamanan IT. Sebuah peralatan yang semakin maju setiap harinya dan penggunaan dalam keadaan darurat : memeriksa dan mengedit semua jenis file, mengembalikan data yang telah terhapus atau data yang hilang dari hard drives system file yang corrupt, atau dari kartu memory digital kamera.[8]

## III. METODOLOGI

Kejahatan konvensional seperti peredaran narkoba saat ini sudah mulai memanfaatkan teknologi informasi. Penggunaan teknologi ini bermaksud agar terhindar dari pihak yang berwenang/kepolisian, berbagai macam cara dilakukan untuk menyembunyikan informasi yang bersangkutan dengan tersangka pengedaran narkoba di daerah yang dimaksud. Penelitian ini mengambil contoh kasus berkas informasi dari tersangka yang telah disembunyikan menggunakan teknik steganografi dan kemudian dilakukan sebuah analisa terhadap berkas tersebut tentang isi berkas dan jenis ekstensi berkas yang digunakan dengan menggunakan beberapa piranti lunak yaitu *WinHex,Simple steganalisis dan FTK Imager.* Gambar 2 adalah Alur penelitian yang dilakukan dalam penelitian ini.




Gambar 2. Diagram Alur Penelitian

### *G. Literatur review*

Teknik kepustakaan ini dilakukan guna mendukung dalam proses penelitian berupa mencari berbagai referensi yang bersifat teoritis dan melakukan kajian terhadap penelitian-penelitian yang telah dilakukan sebelumnya dengan menyesuaikan dari data yang diperoleh melalui teknik wawancara dan observasi guna menghasilkan solusi untuk proses investigasi forensik pada file steganografi.

### *H. Observasion & data collection*

Tahapan ini menjelaskan bagaimana meneliti dan mencari bukti-bukti, pengenalan terhadap bukti-bukti digital, dan pengumpulan bukti pada baranga bukti elektronik yang ditemukan di TKP .

### *I. Scenario Cases*

Penelitian ini mengambil contoh kasus peredaran narkoba dengan fokus pembahasan pada cara menemukan *file* atau data informasi yang disembunyikan oleh pelaku kejahatan

yang memanfaatkan teknik *steganography*. Barang bukti yang ditemukan di tempat keajdian perkara berupa barang bukti elektronik berbentuk *flashdisk*. Terdapat *file* image dalam *flashdisk* tersebut dengan keterangan *file* tersebut berekstensi .zip.

*J. Preparation system*

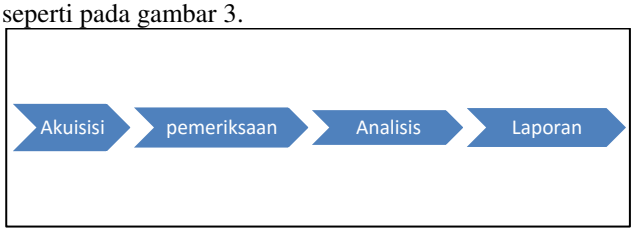
Kebutuhan minimum system perangkat hardware maupun software/tools yang dapat digunakan dalam proses investigasi file steganografi adalah sebagai berikut :

1) ***Hardware :*** Processor Intel(R) Atom(TM) CPU N450 @ 1.66GHz (2 CPUs), ~1.7GHz, memori 2GB, Harddisk 500GB,

2) ***Software :*** Windows 7 Starter 32-bit, Winhex versi 18.9, simple steganalisis, FTK Imager 3.1.2 dan Invisiblesecrets.

*K. Investigasi & Analisis Case*

Proses investigasi dan analisis barang bukti kasus peradaran narkoba dilakukan dengan tahapan-tahapan seperti pada gambar 3.




Gambar 3. Diagram Alir proses investigasi [9]

*1) Akuisisi:* Tahapan ini dilakukan proses akuisisi barang bukti yaitu barang bukti elektronik digandakan atau dilakukan proses forensic imaging, yaitu menggandakan isi dari barang bukti harddisk tersebut secara physical (sektor per sektor atau bit-stream copy) sehingga hasil imaging akan sama persis dengan barang bukti secara physical. Derajat kesamaan ini dapat dipastikan melalui proses hashing yang diterapkan pada keduanya.

Proses hashing ini menggunakan banyak algoritma matematika yang kompleks, namun yang paling sering digunakan untuk kegiatan digital forensik antara lain MD5, SHA1, dan SHA256. Proses hashing ini juga dikenal dengan istilah digital fingerprint (sidik jari digital) yang biasa digunakan untuk membuktikan secara pasti apakah kedua file yang dipertanyakan adalah sama atau berbeda.

Proses *forensic imaging* terdapat dua metode, yaitu ***disk to disk*** (hasil *imaging* akan berupa *harddisk*) dan ***disk to file*** (hasil *imaging* akan berwujud *file*). Dari kedua metode ini, metode yang kedua yang lebih sering digunakan oleh analis forensik saat ini karena metode kedua ini lebih fleksibel, efisien, dan *integrity* dapat lebih terjamin. Permasalahan menggunakan metode yang pertama adalah ketika kasus yang diinvestigasi memiliki benyak *harddisk* yang harus di-*imaging*. Jika menggunakan metode *disk to disk,* maka analis forensik dan investigator harus menyediakan banyak blank *harddisk* (*harddisk* kosong) sebagai target dari *imaging*. [10]

*2) Pemeriksaan:* Tahapan ini dilakukan pemeriksaan secara komprehensif terhadap image file yang telah dibuat dengan maksud untuk mendapatkan data-data digital yang sesuai dengan investigasi.

*3) Analisis:* Data – data yang telah menjadi barang bukti digital tersebut dianalisis secara detail dan komprehensif untuk dapat membuktikan keajahatan apa yang terjadi dan kaitannya pelaku dengan kejahatan tersebut.

*4) Laporan:* Data yang diperoleh dari barang bukti digital dari mulai proses pemeriksaan sampai dengan proses analisis, selanjutnya data-data mengenai barang bukti tersebut dimasukan ke dalam laporan teknis.

*L. Report/Documentation*

Pada proses dilakukan investigasi dibuat dokumentasi setiap proses yang dilakukan dalam bentuk dokumen laporan, foto atau video sebagai bukti tidak adanya rekayasa dalam pengolahan barang bukti digital.

## IV. HASIL DAN PEMBAHASAN

Perkembangan teknologi digital semakin canggih untuk diterapkan dalam kehidupan sehari-hari, namun secara luas telah mengundang berbagai pihak untuk melakukan tindak kejahatan dengan mengggunakan teknologi elektronik dan digital. Beberapa contoh *organized crime* termasuk aktivitas yang mengarah pada terorisme dan peredaran narkoba, telah teridentifikasi memanfaatkan teknik *steganography*.

Bukti digital yang dienkripsi, disembunyikan ataupun disamarkan oleh pelaku kejahatan bertujuan agar bukti tersebut tidak dapat dibaca dan dianalisis oleh analis forensik dan investigator sehingga tidak dapat dipresentasikan dalam persidangan.

Penelitian ini mengambil contoh kasus peredaran narkoba dengan fokus pembahasan pada cara menemukan *file* atau data informasi yang disembunyikan oleh pelaku kejahatan yang memanfaatkan teknik *steganography*. [14]

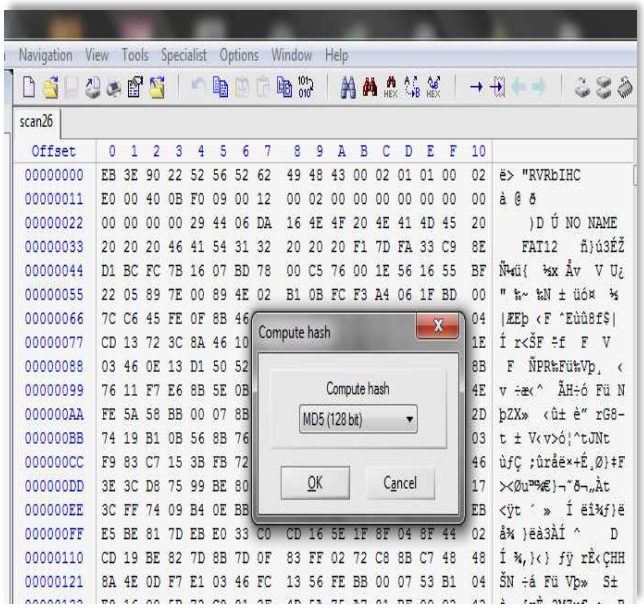
Barang bukti yang ditemukan di tempat kejadian perkara berupa barang bukti elektronik berbentuk *flashdisk*. Terdapat *file* image dalam *flashdisk* tersebut dengan keterangan *file* tersebut berekstensi .zip terlihat pada gambar 4.


Gambar 4. *File* dalam *Flashdisk*

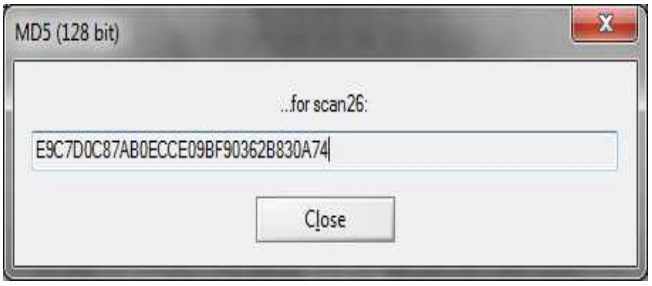
## A. *Proses Akuisisi*

Barang bukti digital yang terdapat dalam flashdisk saat diekstrak sudah dalam bentuk *imaging file.* Ekstensi dari barang bukti digital tersebut adalah "**.raw"** selanjutnya adalah melakukan pemeriksaan nilai *hash* dengan menggunakan aplikasi *WinHex versi 18.9.*

Gambar 5 dan Gambar 6 merupakan proses pemeriksaan nilai *hash* dan hasil proses *hashing* pada file image dengan menggunakan aplikasi *WinHex versi 18.9.*




Gambar 5. Proses *Hashing* MD5




Gambar 6. Nilai *Hashing* MD5

Fungsi *hasing* adalah fungsi yang menerima masukan string atau pesan yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap atau *fixed*. Fungsi hash yang dilakukan biasanya dituliskan dalam notasi persamaan :

h = H (M) .....(6)

keterangan :

h : Nilai *hash* yang dihasilkan

H : Fungsi *hash*-nya itu sendiri

M : Pesan yang akan diubah dan diikonversi menjadi nilai *hash (hash value)*

Algoritma *hash* yang digunakan pada kasus ini adalah algoritma *MD5*. *MD5* adalah fungsi hash satu arah yang dibuat oleh Ron Rivest. *MD5* merupakan perbaikan dari *MD4* setelah *MD4* berhasil diserang oleh kriptalis. Algoritma *MD5* menerima sebuah *input/pesan* dengan panjang sebarang dan akan menghasilkan sebuah output dengan panjang tertentu, yaitu 128-bit.

## B. *Proses Pemeriksaan*

Tahapan ini dilakukan pemeriksaan terhadap *image file* secara komprehensif dengan maksud untuk mendapatkan data-data yang sesuai dengan investigasi. Data-data yang dicari merupakan data-data yang berhubungan dengan kasus peredaran narkoba. Proses pencarian ini menggunakan aplikasi *AccessData FTK Imager versi 3.1.2.0* dan *WinHex versi 18.9* .

Dalam komputasi, tanda tangan file (File Signatures) data yang digunakan untuk mengidentifikasi atau memverifikasi isi file. Secara khusus, mungkin merujuk kepada:

Berkas magic number: byte dalam file yang digunakan untuk mengidentifikasi format file; umumnya urutan pendekbyte (sebagian besar adalah 2-4 byte panjang) ditempatkan pada awal file;

Berkas checksum atau lebih umumnya hasil dari fungsi hash atas isi file: data yang digunakan untuk memverifikasi bahwa integritas isi file, umumnya terhadap kesalahan transmisi atau serangan berbahaya. Tanda tangan dapat dimasukkan pada akhir file atau dalam file terpisah. [11]

Hasil pemeriksaan dengan menggunakan aplikasi *AccessData FTK Imager versi 3.1.2.0* ditemukan beberapa *file* dengan ekstensi .JPEG, .BMP dan informasi berupa teks "*pw=help*" dan "*John Smith's Address: 1212 Main Street, Jones, FL 00001*" dapat dilihat pada Tabel I.

TABEL I

OFFSET FILE DAN SIGNATURE FILE BARANG BUKTI

| File | Offset | Signature | Ascii |
|---|---|---|---|
| images.jpg | 4200 | 70 77 3D 68 65 6C 70 | ÿØÿà JFIF |
| images.bmp | C200 | 42 4D | BM |
| Ascii Text String | 12bb50 | FF D8 FF E0 00 10 4A 46 49 46 | pw=help |
| Ascii Text String | 156760 | 4A 6F 68 6E 20 53 6D 69 74 68 27 73 20 41 64 64 72 65 73 73 3A 20 31 32 31 32 20 4D 61 69 6E 20 53 74 72 65 65 74 2C 20 4A 6F 6E 65 73 2C 20 46 4C 20 30 30 | John Smith's Address: 1212 Main Street, Jones, FL 00001 |

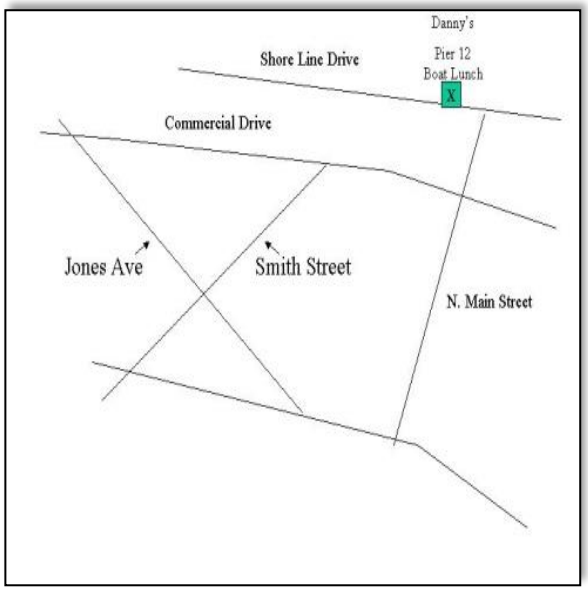
C. *Proses Analisis*

Tahapan ini dilakukan proses *recovery* agar hasil setiap *file* dapat diketahui isinya dan dianalisis data-data yang ditemukan pada barang bukti, sehingga memudahkan untuk mencari data yang dibutuhkan oleh investigator dalam proses investigasi.

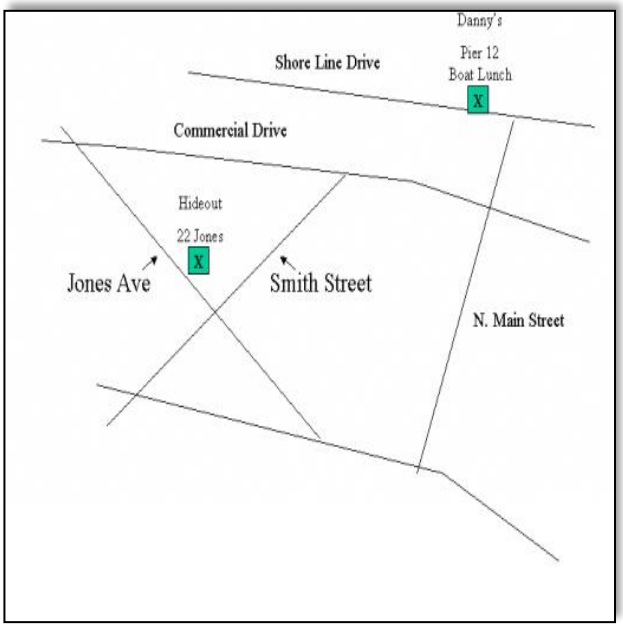
Data *recovery* merupakan bagian dari analisa forensik dimana hal ini merupakan komponen penting di dalam mengetahui apa yang telah terjadi, rekaman data, korespondensi, dan petunjuk lainnya.

Proses rocovery dilakukan dengan menggunakan aplikasi *WinHex versi 18.9* dengan memanfaatkan kelebihan yang dimiliki aplikasi tersebut yaitu menyatukan dan memisahkan *file*.

Gambar 7 dan Gambar 8 merupakan gambar hasil recovery dari file image file yaitu berupa file gambar berekstensi .BMP dan .JPG.

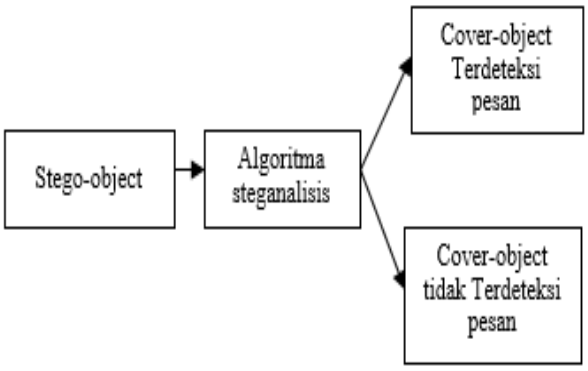



Gambar 7. Hasil *file recovery* images.jpg




*Gambar 8. Hasil file recovery images.bmp*

Tahapan selanjutnya setelah proses *recovery* adalah analisis *steganography* pada *file* yang telah berhasil di-*recovery.* Gambar 9 menjelaskan Proses analisis steganografi dilakukan untuk mengidentifikasi ada tidak nya *file* atau informasi yang tersembunyi pada *file* gambar yang telah di recovery sebelumnya.



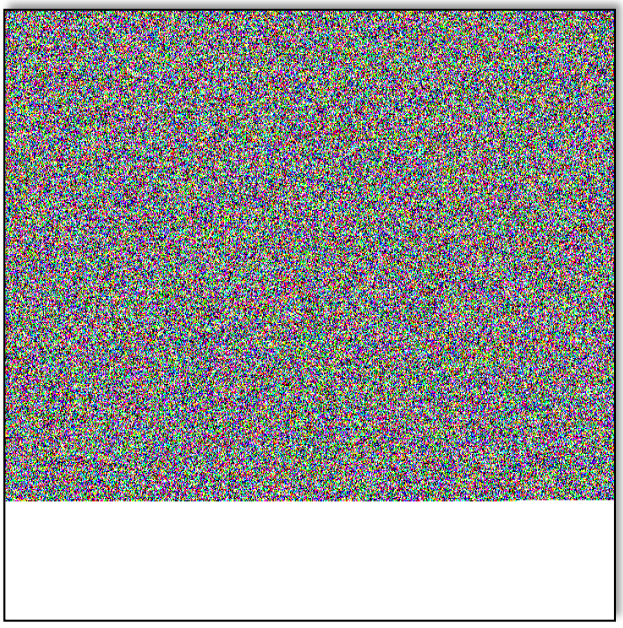

Gambar 9. Skema steganalisis pasif[12]

Analisis steganografi dilakukan menggunakan teknik *enhanced LSB. Enhanced LSB* merupakan metode steganalisis yang dikemukakan oleh Andreas Westfeld untuk mendeteksi adanya pesan rahasia melalui inspeksi secara visual atau sering disebut *visual attack.*

*Visual attack* merupakan serangan terhadap teknik steganografi dengan memanfaatkan keterbatasan indera penglihatan manusia untuk menginspeksi kerusakan-kerusakan pada gambar yang terjadi akibat penyisipan.

Gambar 10 dan Gambar 11 merupakan hasil dari proses steganalisis menggunakan metode *enchanced LSB*.

Gambar10. Hasil LSB enhancement file images.jpg



Gambar 11. Hasil LSB enhancement file images.bmp

Metode ini dipengaruhi oleh kekontrasan citra. Semakin tinggi kontras citra maka akan semakin mudah untukmendeteksi pesan rahasia. Sebaliknya semakin rendah kontras citra maka semakin sulit untuk mendeteksi pesan.

Dari hasil steganalisis gambar diatas menunjukan adanya pesan rahasia pada kedua citra tersebut, namun untuk melakukan extraction file atau pesan rahasia harus menggunakan key stego dengan algoritma tertentu.

Proses selanjutnya dilakukan analisis pada *file* html untuk mencari informasi yang berkaitan dengan *file* steganografi. Pelaku kejahatan digital menggunakan steganografi pada jaringan internet untuk berkomunikasi yaitu dengan cara memanfaatkan halaman web yang dapat disisipi pesan pada script html nya seperti pada Tabel II.

TABEL II
ISI FILE HTML

```
...
<!-- 100 guest rooms have been reserved at a
special conference rate of--><!-- Invisible
Secrets  --><!-- $149.00 per night for non-
government--> <!--
http://www.invisiblesecrets.com --><!--
employed attendees and $86.00 per night for
government-employed attendees.--> <!--
PW=lefty -->Please honor this pricing
arrangement and do not attempt to receive the
government rate without proper identification
and/or government travel orders. <!--
Algorythm= twofish -->In order to ensure room
availability we ask that your room
reservation be completed by July 6, 2003. On
July 7, 2003 all of the remaining guest rooms
will be released to the general public and
availability will be limited. If making a
reservation, please mention DFRWS.
<br><br>
<b> Conference fee</b><br>
<i><b>US $325.00 up to and including Sunday
July 6, 2003.<br>
After July 6, 2003 the conference<!--
PW=right --> fee will increase to US $375.00
....
```

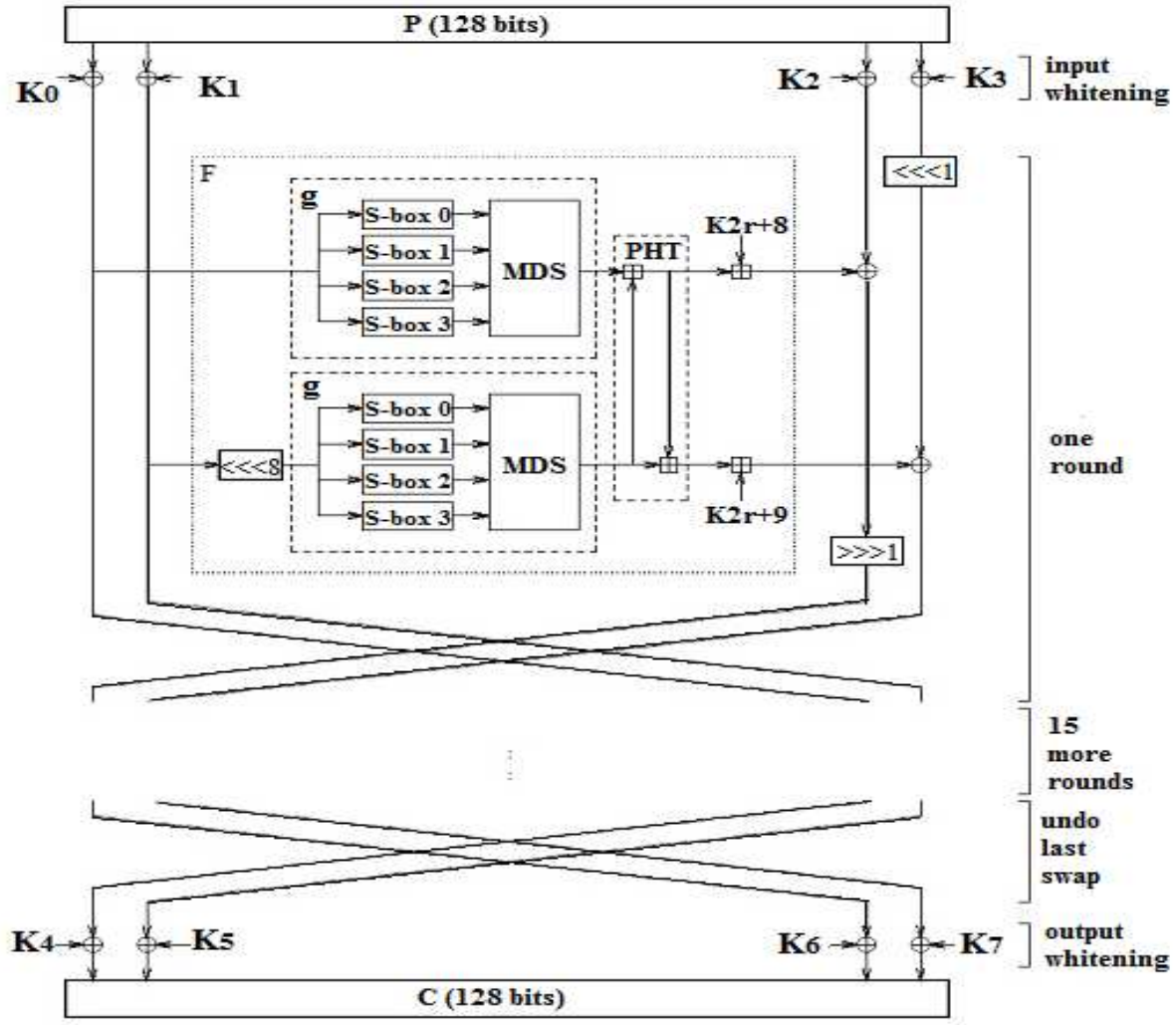
Setelah dilakukan analisa pada *file* html, ditemukan informasi yang berkaitan dengan *file* steganografi, data-data tersebut yaitu " invisibleSecrets", "PW=lefty", "Algoritma=twofish","PW=right". Dari informasi yang didapat, *file* yang telah berhasil di*recovery* merupakan *file* steganografi menggunakan aplikasi steganografi *Invisiblesecrets* dengan algoritma *twofish* dan password lefty dan right.

Algoritma *twofiish* merupakan 128-*bit chipher* yang bisa menerima panjang variabel kunci sebesar 256 *bit. Chipher* tersebut berasal 16-*round* jaringan feitsel dengan fungsi F yang dilanjutkan dengan empat key-dependent 8-by-bit S-boxes, satu fixed 4-by-4 maximum distance separable matrix over GF(28), satu pseudo-Hadamard transform, satu rotasi bitwise dan satu desain key schedule. Suatu implementasi Twofish yang dioptimalkan mengenksripsi pada Pentium Pro dengan 17,8 siklus clock per byte, dan pada smartcard akan mengenksripsi pada 1660 siklus clock per byte.

Algoritma *Twofish* menggunakan struktur Feistel 16-round dengan whitening tambahan dalam input dan outputnya. Satu-satunya elemen yang bukan Feistel adalah rotasi 1 bit. Rotasi tersebut dapat dipindahkan ke fungsi

F untuk menciptakan output berjalan. Plaintext dipecah menjadi empat buah word32-bit. Pada whitening input, keempat worditu di XOR-kan dengan empat key word. Dan di ikuti dengan ke enam belas round. Dalam tiap round, dua word di kiri digunakan sebagai input fungsi g (Salah satunya dirotasikan dengan 8 bitterlebih dahulu).

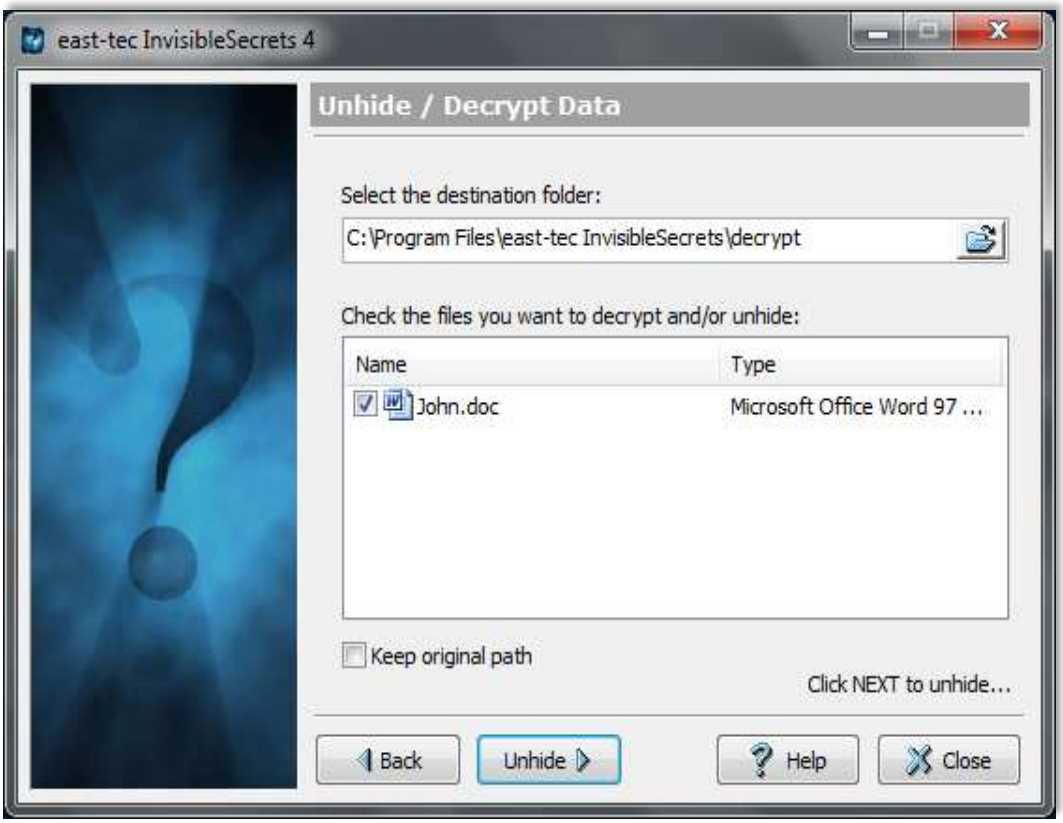
Gambar 12 merupakan gambar dari struktur algoritma *Twofish* yang dikutip dari sebuah jurnal yang berjudul "*Twofish: A 128-Bit Block Cipher*" yang ditulis oleh Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, dan Niels Ferguson:




Gambar 12. Struktur algoritma *twofish*

Setelah didapatkan *key* stego untuk membuka pesan rahasia pada file steganogafi, dilakukan proses *unhide/decrypt* untuk mengetahui isi dari file rahasia menggunakan *tools* steganografi I*nvisibleSecrets.*

Gambar 13 dan Tabel III merupakan proses *Unhide/Decrypt file* steganografi dan isi dari file john.doc yang berhasil di ekstraksi dari file steganografi images.jpg.

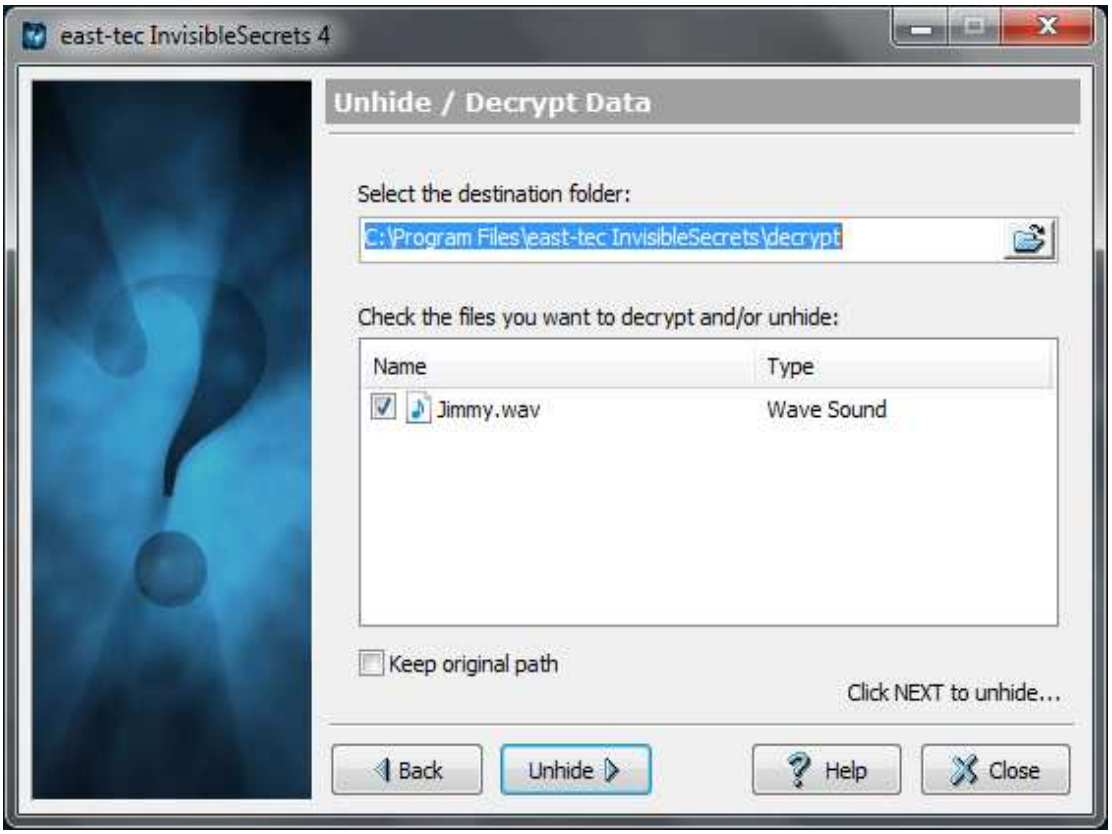



Gambar 13. Proses *Unhide/decrypt file* john.doc

TABEL III
ISI FILE JOHN.DOC

| |
|---|
| Dear John Smith:<br>My biggest dealer (Joe Jacobs) got busted. The day of our scheduled meeting, he never showed up. I called a couple of his friends and they told me he was brought in by the police for questioning. I'm not sure what to do. Please understand that I cannot accept another shipment from you without his business. I was forced to turn away the delivery boat that arrived at Danny's because I didn't have the money to pay the driver. I will pay you back for the driver's time and gas. In the future, we may have to find another delivery point because Danny is starting to get nervous.<br>Without Joe, I can't pay any of my bills. I have 10 other dealers who combined do not total Joe's sales volume.<br>I need some assistance. I would like to get away until things quiet down up here. I need to talk to you about reorganizing. Do you still have the condo in Aruba? Would you be willing to meet me down there? If so, when? Also, please take a look at the map to see where I am currently hiding out.<br>Thanks for your understanding and sorry for any inconvenience.<br><br>Sincerely,<br>Jimmy Jungle |

Seperti pada gambar sebelumnya Gambar 14 dan Tabel IV merupakan proses *unhide/decrypt file* steganografi dan isi file yang disembunyikan yaitu file rekaman suara jimmy.wav yang berhasil di ekstraksi dari hasil file steganografi images.bmp.




Gambar 14. Proses *Unhide/decrypt file* jimmy.waV

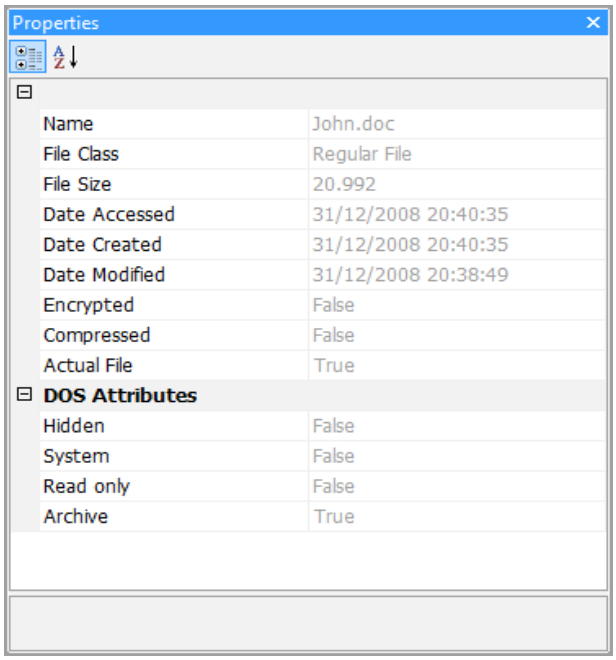
File jimmy.wav yaitu berupa rekaman suara yang berisi informasi pada Tabel IV.

TABEL IV
ISI DARI FILE REKAMAN JIMMY.WAV

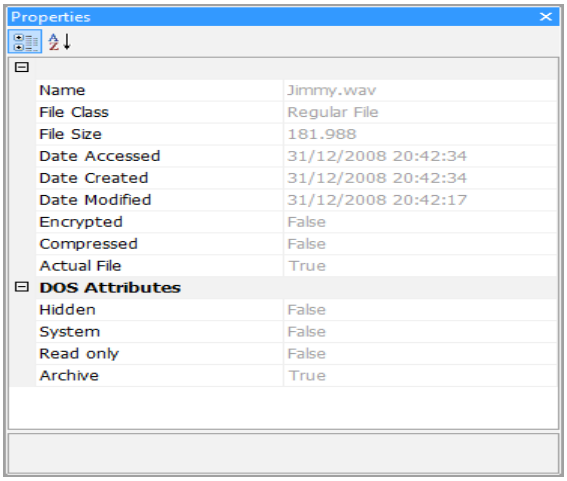
| |
|---|
| "*This is jimmy, meet me at the pier tomorrow. I drive a blue 1978 Mustang with Ontario licence plates*". |

Tahapan selanjutnya adalah analisis metadata *file* yang telah dibuka. Metadata adalah informasi terstruktur yang mendeskripsikan, menjelaskan, menemukan, atau setidaknya membuat menjadikan suatu informasi mudah untuk ditemukan kembali, digunakan kembali, digunakan, atau dikelola. Data perspektif digital forensik, metadata sebagai bukti, penyimpanan secara elektronik, yang menggambarkan karakteristik, keaslian, kegunaan, dan validasi bukti elektronik lainnya.

Analisis barang bukti digital yang ditemukan tidak mengalami perubahan. Itu ditunjukan dengan keterangan data created dan data modified. Keterangan data modified-nya menunjukan waktu saat data tersebut dimodifikasi terakhir kali oleh pelaku. Hasil dari modifikasi data ini dapat dilihat pada Gambar 15 dan Gambar 16 sebagai berikut :




Gambar 15. Nilai Metadata *file* john.doc



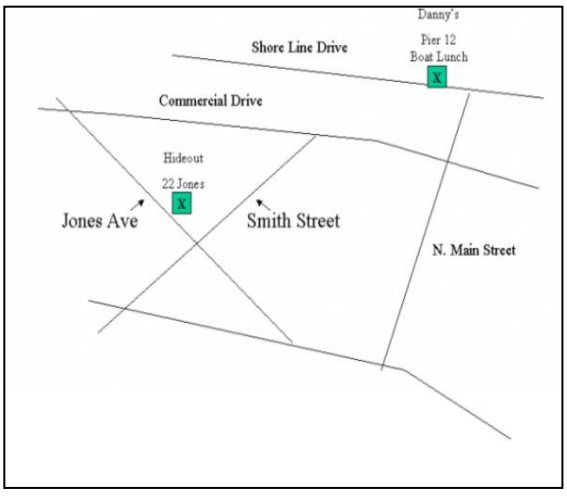

Gambar 16. Nilai Metadata *file* jimmy.wav

Dari hasil analisis 4W1H (*who, when, where, why,* dan *How*) didapat data-data mengenai kasus pengungkapan bandar narkoba.[13]

1) *Who,* pelaku sebagai bandar narkoba adalah John Smith.

2) *When,* (transaksi akan dilakukan) merujuk pada sebuah file rekaman suara jimmy.wav yang berhasil diekstrak dari stego file image.bmp, jimmy junggle pelaku pengedar narkoba bertemu dengan John Smith sehari setelah pengiriman pesan, dimana pesan tersebut berisi jimmy jungle ingin bertemu dengan John Smith di pier, jimmy memberikan petunjuk dia menggunakan mobil mustang berwarna biru tahun 1978 dengan plat Ontario . *"This is jimmy, meet me at the pier tomorrow. I drive a blue 1978 Mustang with Ontario licence plates".*

3) *Where,* (persembunyian jimmy jungle) merujuk pada sebuah file image.bmp yang terlihat pada Gambar 17, tempat persembunyian jimmy jungle adalah di 22 Jones Ave.




Gambar 17. Lokasi persembunyian jimmy jungle

*4) Why,* (jimmy jungle mengirim pesan pada john smith) merujuk pada file John.doc yang berhasil di ekstrak dari file images.jpg, jimmy jungle mengirim laporan pada john smith bahwa Joe Jacob telah tertangkap oleh polisi. *"My biggest dealer (Joe Jacobs) got busted. The day of our scheduled meeting, he never showed up. I called a couple of his friends and they told me he was brought in by the police for questioning. I'm not sure what to do."*

*5) How,* (file yang dikirim), file dokumen dan rekaman yang di kirim jimmy jungle pada john smith menggunakan teknik steganografi yang bertujuan untuk memanipulasi petugas, file tersebut disembunyikan pada file gambar lokasi, untuk membuka file stego tersebut jimmy menyembunyikan informasi dalam sebuah file html.

### D. *Laporan*

Setelah barang bukti digital melalui proses pemeriksaan dan analisis didapatkan data-data yang sesuai dengan kebutuhan investigasi, selanjutnya data-data mengenai barang bukti tersebut dimasukan ke dalam laporan teknis. Berikut laporan teknis dari barang bukti kasus pengungkapan bandar narkoba, dapat dilihat pada lampiran.

## V. KESIMPULAN

Berdasarkan tahapan-tahapan yang telah dilakukan dalam analisis forensik pada *file* steganografi, dimana dalam pengungkapan kasus kejahatan peredaran narkoba yang telah diskenariokan sebelumnya, maka dapat disimpulkan sebagai berikut :

Proses investigasi pada file steganografi dapat dilakukan mengunakan beberapa metode, pada penelitian ini metode untuk megetahui indikasi file steganografi menggunakan metode visual attack yaitu enhanced LSB. Metode penelitian yang digunakan telah berhasil diterapkan pada proses investigasi file steganografi dengan hasil terungkapnya kasus peredaran narkoba.

Ditemukannya beberapa digital evidence berupa barang bukti elektronik berupa flashdisk yang berisi file image dan beberapa informasi pada file html, sehingga didapat dua file rahasia yang membuktikan john smith adalah seorang bandar narkoba, tempat tinggal jonh smith dan tempat transaksi dengan pengedar narkoba yaitu jimmy jungle dengan menggunakan beberapa tools digital forensik yaitu WinHex, AccessData FTK imager, dan InvisibleSecrets.

## DAFTAR PUSTAKA

[1] (2012)arstechnica homepage. [Online]. Tersedia : https://arstechnica.com/business/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/
[2] Munir Rinaldi. "*Kriptografi",* Informatika, Bandung 2006.
[3] Johnson Neil F,, "Steganography",. Center for Secure Information Systems, George Mason University, 2006.

[4] Marcella, A. J. & Greenfiled, R. S. 2002. Cyber Foensics a field manual for collecting, examining, and preserving evidence of computer crimes". Florida : CRC Press LLC.

[5] (2010)Budhisantoso, Nugroho, Personal Site, [online]. Tersedia : : (http:// www.forensik-komputer.info).

[6] Casey, E. "Digital Evidence and Computer Crime : Forensic Science, Computer and Internet (3rd edition)". California : Elsevier Inc.2011

[7] *"The Scientific Working Group on Digital Evidence"* (SWGDE). (2015). *"Information of probative value stored or transmitted in digital form".*

[8] Solihah, S. (2014). *Analisis Digital Forensik untuk File Terenkripsi dengan menggunakan Winhex dan Tools Kali Linux Autopsy.* Tasikmalaya: Universitas Siliwangi.

[9] Al-Azhar, M. (2012). *Digital Forensik Panduan Praktis Investigasi Komputer.* Jakarta: Salemba Infotek.

[10] EC-Council | Press. (2010). *Investigating Data and Image Files.* USA.

[11] Widiyasono, N. (2014). *ANALISA FILE SIGNATURES DAN FUNGSI HASH.* YOGYAKARTA: UNIVERSITAS ISLAM INDONESIA.

[12] Wijaya, E. S., & Prayudi, Y. (2009). Konsep Hidde Message Menggunakan Teknik Steganografi Dynamic Cell Spreading. *Media Informatika* , Vol. 9, No. 9.

[13] Widiyasono, N. (2014). *ANALISA DAN PEMANFAATAN BUKTI DIGITAL (Who, When, Where, Why and How) Studi kasus:MEMBUKA FILE ENKRIPSI JADWAL PENGIRIMAN NARKOBA.* YOGYAKARTA: UNIVERSITAS ISLAM INDONESIA.

[14] (2016)honeynet.org, [online]. Tersedia : : (http://old.honeynet.org/scan26/ ).