E-ISSN : 3031-9692 **Vol. 1 No. 3 2024**
Institut Teknologi dan Bisnis STIKOM Bali, 02-10-2024

Simulasi Investigasi pada FlashDisk dalam Mengungkap Pesan pada Kasus Perdagangan Narkoba Menggunakan Metode Steganografi

Gede Andika Arya Permana Putra[1)], Ni Kadek Sukerti[2)], Ni Made Dewi Kansa Putri[3)]
Sistem Komputer[1)], Sistem Informasi[2)], Bisnis Digital[3)]
Institut Teknologi dan Bisnis STIKOM Bali
Denpasar, Indonesia
e-mail: 200010011@stikombali.ac.id[1)], dektisamuh@gmail.com[2)], kansa@stikom-bali.ac.id[3)]

Abstrak

Penelitian ini bertujuan untuk melakukan simulasi investigasi pada perangkat flashdisk dalam upaya mengungkap pesan tersembunyi yang digunakan dalam kasus perdagangan narkoba dengan metode steganografi. Steganografi merupakan teknik menyembunyikan informasi di dalam sebuah file digital seperti gambar, audio, atau video sehingga pesan tersebut tidak mudah terdeteksi. Dalam konteks perdagangan narkoba, pelaku seringkali menggunakan metode ini untuk menyembunyikan komunikasi terkait transaksi ilegal, sehingga penting untuk mengembangkan teknik investigasi digital yang efektif. Penelitian ini melakukan simulasi dengan fokus pada bagaimana pesan dapat disembunyikan di dalam file yang tersimpan di flashdisk dan bagaimana teknik forensik digital dapat digunakan untuk mengekstraksi pesan-pesan tersebut. Berbagai alat dan perangkat lunak yang mendukung forensik digital dan analisis steganografi digunakan seperti FTK Imager, Autopsy, dan Hex Editor Neo dalam mengungkap data tersembunyi. Hasil dari simulasi menunjukkan bahwa dengan menggunakan metode steganografi, pesan tersembunyi dapat diidentifikasi dan diungkap meskipun sudah dienkripsi atau disamarkan di dalam file gambar. Penelitian ini memberikan kontribusi penting dalam pengembangan strategi investigasi forensik digital, terutama dalam penanganan kasus-kasus kejahatan terorganisir yang memanfaatkan teknologi canggih untuk menyembunyikan jejak komunikasi mereka.

Kata kunci: *Steganografi, FlashDisk, Forensik Digital, Perdagangan Narkoba, Pesan Tersembunyi*

1. Pendahuluan

Perdagangan narkoba telah menjadi masalah besar di seluruh dunia seiring dengan meningkatnya penggunaan perangkat penyimpanan modern pada saat ini didalam aktivitas para pelakunya. *FlashDisk* adalah sebuah perangkat penyimpanan data portabel berbasis memori flash yang umum digunakan untuk menyimpan dan mentransfer data secara elektronik[1]. Oleh karena itu, *FlashDisk* telah menjadi sarana penting dalam penjualan narkoba secara digital. Dalam banyak kasus, pelaku menggunakan pesan teks, panggilan *video*, gambar dan berbagai jenis file untuk berkomunikasi dan mengatur transaksi perdagangan narkoba. Pesan dan tampilan digitalnya dapat menjadi sumber informasi berharga dalam penyelidikan perdagangan narkoba. Kasus perdagangan narkoba melibatkan transaksi ilegal yang merugikan masyarakat dan mengancam keselamatan masyarakat.

Oleh karena itu, upaya serius harus dilakukan untuk mengidentifikasi, menangkap dan menghentikan para penjahat yang terlibat dalam kegiatan ilegal tersebut. Salah satu cara efektif untuk mengungkap kasus ini adalah dengan menggunakan metode steganography. Metode steganografi merupakan suatu teknik atau metode yang digunakan untuk menyembunyikan sebuah pesan rahasia dalam suatu media (seperti gambar, audio, atau teks) tanpa menarik perhatian orang yang tidak memiliki kunci atau pengetahuan yang diperlukan untuk mengekstrak pesan tersebut[2]. Tujuan utama dari steganografi adalah menjaga kerahasiaan pesan yang disembunyikan agar pesan tersebut tidak diketahui oleh siapapun[3].

Penelitian ini dilakukan untuk mengumpulkan bukti forensik sebuah pesan rahasi pada perangkat *FlashDisk* yang berkaitan dengan kasus perdagangan narkoba. Metode investigasi yang digunakan mengacu pada *DFRWS (Digital Forensics Research Workshop)*, yang dikenal karena reputasinya dalam mengembangkan metode forensik digital yang handal. Melalui tahapan *identification, preservation, collection, examination, analysis* dan *presentation* yang disediakan oleh *DFRWS*, diharapkan bukti digital yang didapatkan akan memiliki tingkat keandalan dan intergritas tinggi dalam proses penyelidikan yang efektif dan adil[4].

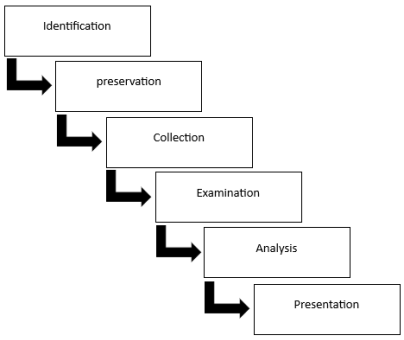
penelitian yang dilakukan oleh Aliy Hafiz dengan judul Steganography Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan *Metode Least Significant Bit (LSB)* menyatakan bahwa Karena maraknya pembajakan data maupun pencurian data. *Steganography* bisa menjadi solusi dalam menjaga kerahasiaan data dan keamanan dari data yang dimiliki. Data yang ada akan disembunyikan sehingga tidak semua orang bisa melihat dan menggunakannya. Dengan metode *Least Significant Bit*, Steganography bisa dilakukan dengan menyisipkan data kedalam gambar yang diinginkan. Proses yang terjadi adalah bit-bit data akan disisipkan ke dalam bit citra digital sehingga bit data akan berada di dalam bit wadah citra digital tersebut untuk disembunyikan[5].

Penelitian yang dilakukan oleh Agung Purnama Saputra dengan judul Analisa *Digital Forensik* pada File *Steganography* (Studi kasus: Peredaran Narkoba) menyatakan bahawa berdasarkan proses investigasi pada file steganografi dapat dilakukan menggunakan beberapa metode, pada penelitian ini metode untuk megetahui indikasi file *Steganography* 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[6].

Steganografi dapat digunakan untuk menyembunyikan data secara aman, khususnya melalui metode *Least Significant Bit (LSB*). Steganografi berbasis citra digital dapat melindungi data dari pencurian atau pembajakan dengan menyisipkan bit data ke dalam bit citra digital. Sementara itu, dengan menggunakan metode *Steganogaphy* analisis forensik digital dapat mendeteksi sebuah file steganografi menggunakan metode *Enhanced LSB*, yang berhasil diimplementasikan dalam mengungkap kasus peredaran narkoba.

Tujuan dilakukannya penelitian ini adalah untuk menganalisis teknik steganografi yang digunakan dalam menyembunyikan data dalam media penyimpanan, serta mengidentifikasi metode forensik yang efektif digunakan dalam mendeteksi dan mengekstraksi pesan tersembunyi, serta mengevaluasi kemampuan metode tersebut dalam membantu penegak hukum mengungkap aktivitas ilegal yang melibatkan penyembunyian informasi sensitif dalam kasus kejahatan narkoba.

2. Metode Penelitian



Gambar 1. Tahapan Metode Penelitian DFRWS

Penerapan metode penelitian ini didasarkan pada metode pengumpulan bukti forensik dari *DFRWS (Digital Forensics Research Workshop)* Metode ini digunakan untuk menjelaskan bagaimana tahapan – tahapan penelitian dilakukan, sehingga alur penelitian dapat diselesaikan secara sistematis dan dapat dijadikan pedoman untuk memecahkan permasalahan yang ada. Menurut penelitian yang telah dilakukan oleh Fanani pengumpulan data forensic mencapai hasil hampir 100% jika teknik dan analisis forensik dilakukan berdasarkan metode yang tepat[7].

Metodologi pada *DFRWS (Digital Forensics Research Workshop)* ini dibagi menjadi enam fase yaitu : tahapan *identification, preservation, collection, examination, analysis* dan *presentation*[8].

a. Tahap *Identification*

   Tahap *identification* meliputi pengklasifikasian barang bukti pada data digital untuk mendukung proses penyelidikan dalam pencarian barang bukti kriminal digital. Fase ini juga meliputi proses pelebelan, identifikasi, serta pencatatan barang bukti.

b. Tahap *Preservation*

Tahap Preservation merupakan tahap pemeliharaan atau tahap pengamanan yang diperlukan untuk menjaga bahwa barang bukti digital masih terjaga keasliannya. Barang bukti tidak dilakukan perubahan atau disabotase[9].

c. Tahap *Collection*
Tahap *Collection* merupakan sebuah rangkaian kegiatan dalam mengumpulkan data guna mendukung dari proses penyelidikan pencarian barang bukti pada kasus kejahatan digital. Dalam fase ini informasi yang diperoleh berdasarkan sumber data yang relevan.

d. Tahap *Examination*
Tahap *Examination* merupakan sebuah tahapan yang dimana data dikumpulkan, baik secara otomatis ataupun secara manual, diperiksa secara forensic digital dan data yang diperoleh sebagai sebuah file adalah asli dan sesuai dengan data yang diperoleh pada TKP, karena keaslian data merupakan sebuah hal yang sangat penting[10].

e. Tahap *Analysis*
Tahap *Analysis* tahap ini dilakukan ketika file atau barang bukti digital yang sebelumnya ditemukan pada saat proses pemeriksaan diterima, kemudian bukti atau data tersebut dilakukan proses analisis secara rinci menggunakan metode pembuktian yang dibenarkan secara hukum dan teknis.

f. Tahap *Presentation*
Tahap *Presentation* Tahap ini merupakan tahap terakhir pada metode penelitan *DFRWS (Digital Forensics Research Workshop)* yang merupakan tahap pelaporan serta mempresentasikan hasil dari analisis sebelumnya [11].

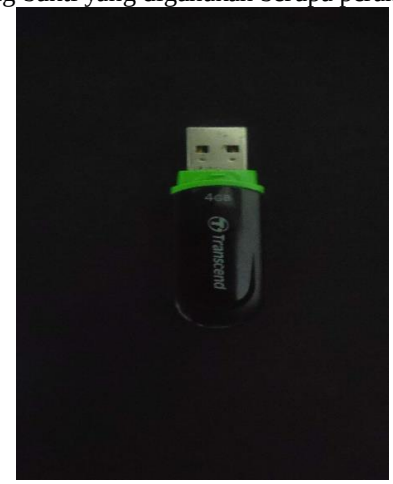
3. Hasil dan Pembahasan

3.1 Identification

Pada tahap ini penyidik melakukan proses simulasi identifikasi pada sebuah perangkat *FlashDisk* dan penyidik juga menyiapkan perlatan yang digunakan dalam melakukan proses pengumpulan barang bukti. Peralatan yang digunakan pada saat simulasi investigasi dalam mengumpulan barang bukti foresnik seperti 1 buah perangkat laptop, kemudian 3 buah tools *forensic* yaitu *FTK Imager*, *Autopsy*, dan *Hex Editor Neo*.

3.2 Preservation

Tahap selanjutnya adalah tahap dimana barang bukti diamankan pada sebuah tempat guna menjaga keasilan dari barang bukti *FlashDisk* yang ditemukan pada saat melakukan proses simulasi investigasi untuk menghindari adanya kerusakan atau hilangnya barang bukti pada kasus tersebut. Gambar 2 menunjukan proses pengamanan barang bukti yang digunakan berupa perangkat *FlashDisk*.

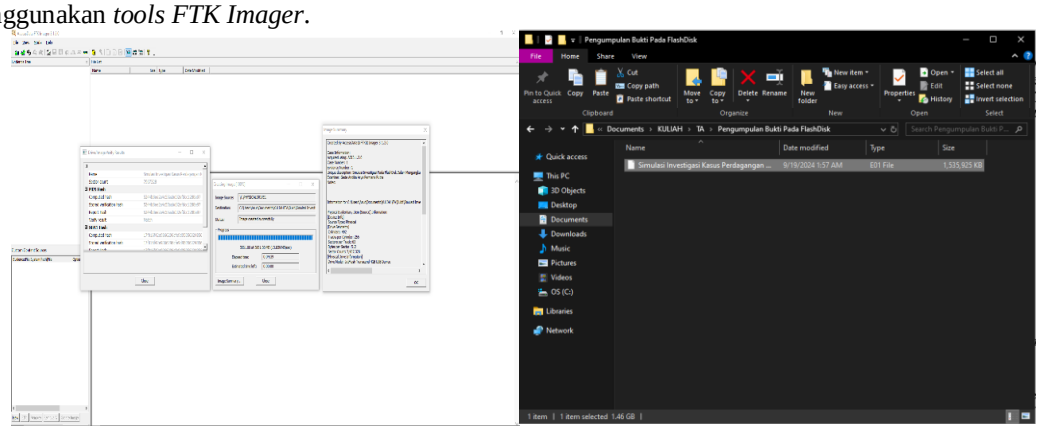


Gambar 2. Proses pengamanan barang bukti berupa *FlashDisk*

3.3 Collection

Tahap selanjutnya merupakan tahap dimana bukti data yang diperlukan pada perangkat *FlashDisk JetFlash Transcend 4GB USB Device* dikumpulkan dalam membantu melakukan proses simulasi. Untuk

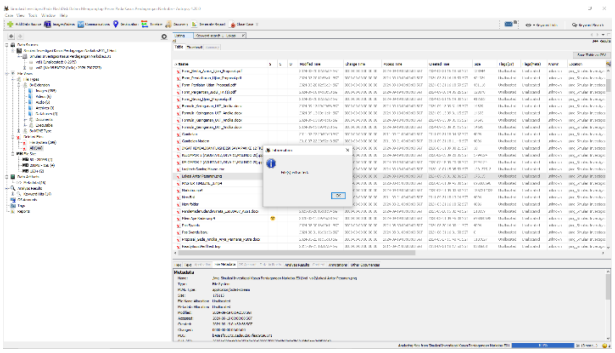
mengumpulkan bukti digital yang diharapkan pada simulasi ini menggunakan *tools FTK Iamger*. Gambar 3 menunjukan proses pengumpulan data pada perangkat *FlashDisk JetFlash Transcend 4GB USB Device* menggunakan *tools FTK Imager*.



Gambar 3. Pengumpulan data digital menggunakan *tools Autopsy* pada perangkat *FlashDisk*

3.4 Examination

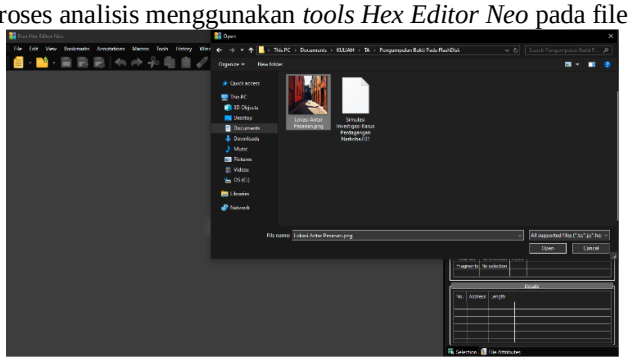
Tahap *Examination* merupakan tahap pemerikasan data digital yang sudah diperoleh sebelumya pada barang bukti *FlashDisk JetFlash Transcend 4GB USB DeviceI* menggunakan *tools FTK Imager*. Selanjutnya Gambar 4 menunjukan proses pemeriksaan data menggunakan *tools Autopsy* dan menemukan sebuah file gambar dengan format *.png* yang diduga didalam file tersebut sengaja disisipkan sebuah pesan tersembunyi.



Gambar 4. Proses pemeriksaan data digital menggunakan *tools Autopsy*

3.5 Analysis

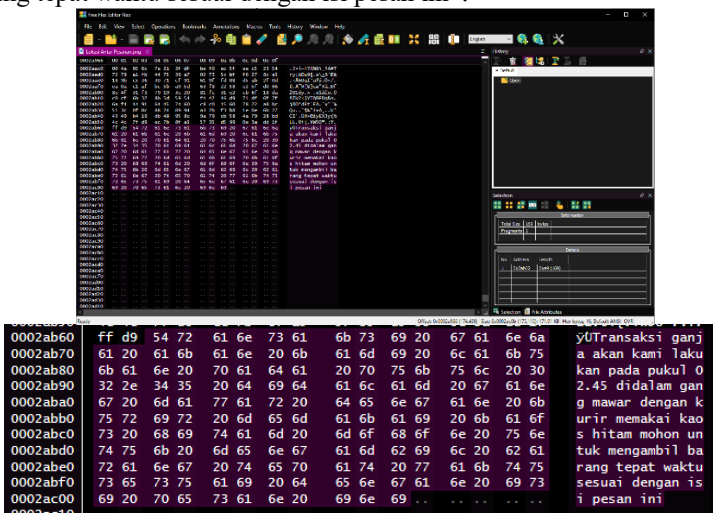
Hasil dari ekstraksi data digital menggunakan *tools Autopsy* sebelumnya, ditemukan sebuah file gambar dengan format *.png* yang mencurigakan, yang diduga menyimpan sebuah pesan tersembunyi pada file tersebut. Untuk memperkuat dugaan adanya pesan tersembunyi pada file gambar tersebut maka Gambar 5 menunjukan sebuah proses analisis menggunakan *tools Hex Editor Neo* pada file gambar tersebut.



Gambar 5. Proses analisis menggunakan *tools Hex Editor Neo*

Setelah file tersebut dianalisis menggunakan *tools Hex Editor Neo* Gambar 6 menunjukan ditemukannya bukti bahwa file gambar tersebut mengandung sebuah pesan tersembunyi yaitu “Transaksi

ganja akan kami lakukan pada pukul 02.45 didalam gang mawar dengan kurir memakai kaos hitam mohon untuk mengambil barang tepat waktu sesuai dengan isi pesan ini".



Gambar 6. Hasil proses analisis menggunakan *tools Hex Editor Neo*

3.6 Presentation

Setelah proses analisis file gambar selesai dilakukan pada barang bukti *FlashDisk* selanjutnya tahap presentation dilakukan guna memaparkan hasil yang didapat dengan melakukan proses forensik pada perangkat *FlashDisk* berupa bukti pesan yang sengaja disembunyikan pada file gambar sebelumnya berhasil diuangkap. Berdasarkan hasil proses simulasi investigasi yang dilakukan Tabel 1 menunjukan hasil yang didapat selama proses simulasi investigasi tersebut dilakukan serta hasil tersebut disajikan kedalam bentuk tabel agar hasil yang diperoleh tersebut dapat dengan mudah dipaparkan.

Tabel 1. Hasil proses simulasi investigasi

Barang Bukti	Nama Barang Bukti	Keterangan
FlashDisk	*JetFlash Transcend 4GB USB Device*	Barang bukti ditemukan tergeletak diatas sebuah meja pada saat proses simulasi investigasi dilakukan.
File *Image .png*	Lokasi Antar Pesanan.png	Barang bukti tersebut setelah dilakukan analisa menggunakan *tools Hex Editor Neo* ditemukan sebuah pesan berupa "Transaksi ganja akan kami lakukan pada pukul 02.45 didalam gang mawar dengan kurir memakai kaos hitam mohon untuk mengambil barang tepat waktu sesuai dengan isi pesan ini".

4. Kesimpulan

Berdasarkan hasil dari pembahasan diatas, dengan menggunakan *framework DFRWS* serta menggunakan *tools FTK Imager* dan *Autopsy* mampu melakukan pengumpulan data forensik pada salah satu perangkat penyimpanan khususnya *FlashDisk* serta dengan metode steganografi dan bantuan *tools Hex Neo Editor* pesan yang sebelumnya disembunyikan pada file gambar dapat diungkap menggunakan tools tersebut. Hasil yang didapat pada penelitian tersebut dapat digunakan oleh penyidik sebagai alat bukti yang mendukung dalam penanganan kasus pidana dan menjadi rujukan dalam pencarian alat bukti pada perkara pidana perdagangan narkoba pada perangkat *FlsahDisk* menggunakan *tools FTK Imager, Autopsy* dan *Hex Neo Editor* dapat mengungkap semua bukti pesan yang telah disembunyikan.

Daftar Pustaka

[1] N. Berliano Novanka Putra, F. Amalia Raihana, W. Michael Albert Mondong, A. Rosadi Kardian,

P. Siber dan Sandi Negara, and J. Barat, "Analisis Enkripsi Kriptografi Asimetris Algoritma RSA Berbasis Pemrograman Batch pada Media Flashdisk," *J. Ris. Sist. Inf. Dan Tek. Inform.*, vol. 8, no. 2527–5771, pp. 51–61, 2022, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik.

[2] S. Supardi, A. A. Alkodri, and B. Isnanto, "Teknik Steganografi Penyembunyian Pesan Text Rahasia Pada Citra Digital Dengan Metode Least Significant Bit," *J. Sisfotek Glob.*, vol. 11, no. 1, p. 70, 2021, doi: 10.38101/sisfotek.v11i1.351.

[3] D. Andika and D. Darwis, "Modifikasi Algoritma Gifshuffle Untuk Peningkatan Kualitas Citra Pada Steganografi," *J. Ilm. Infrastruktur Teknol. Inf.*, vol. 1, no. 2, pp. 19–23, 2021, doi: 10.33365/jiiti.v1i2.614.

[4] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Mengungkap Dan Menguji Keaslian Bukti Digital Pada Kejahatan Cybercrime Dengan Metode Digital Forensic Research Workshop," *J. Apl. Teknol. Inf. dan Manaj.*, vol. 2, no. 2, pp. 120–127, 2021, doi: 10.31102/jatim.v2i2.1068.

[5] M. Fadlan, Haryansyah, and Rosmini, "Three Layer Encryption Protocol: An Approach of Super Encryption Algorithm," *3rd Int. Conf. Cybern. Intell. Syst. ICORIS 2021*, vol. XVII, no. April, pp. 194–198, 2021, doi: 10.1109/ICORIS52787.2021.9649574.

[6] A. P. Saputra, H. Mubarok, and N. Widiyasono, "Analisis Digital Forensik pada File Steganography (Studi kasus : Peredaran Narkoba)," *Tek. Inform. dan Sist. Inf.*, vol. 3, no. 1, pp. 179–190, 2017.

[7] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. Media Inform. Budidarma*, vol. 6, no. 2, p. 1263, 2022, doi: 10.30865/mib.v6i2.3946.

[8] A. Yudhana, I. Riadi, and R. Y. Prasongko, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," *J. Inform. J. Pengemb. IT*, vol. 7, no. 1, pp. 43–48, 2022, doi: 10.30591/jpit.v7i1.3639.

[9] R. M. Genggam *et al.*, "Analisis Bukti Digital Forensik pada Aplikasi Threads Menggunakan Metode Digital Forensic Research Workshop," *Afrizal Ajuj Mudzakkar \ Afrizal Ajuj Mudzakkar*, vol. 22, no. 2, pp. 1–10, 2024.

[10] R. Umar, A. Yudhana, and M. N. Fadillah, "Perbandingan Tools Forensik Pada Aplikasi Dompet Digital," *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 2, p. 242, 2022, doi: 10.26798/jiko.v6i2.621.

[11] S. Sunardi, I. Riadi, and M. H. Akbar, "Steganalisis Bukti Digital pada Media Penyimpanan Menggunakan Metode Static Forensics," *J. Nas. Teknol. dan Sist. Inf.*, vol. 6, no. 1, pp. 1–8, 2020, doi: 10.25077/teknosi.v6i1.2020.1-8.