

**ANALISIS BUKTI DIGITAL FORENSIK TERKAIT
PENGUNAAN TEKNIK STEGANOGRAFI PADA
KASUS CYBER SEXUAL HARASSMENT**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

ZEPIN NOSSA

18.83.0264

Kepada

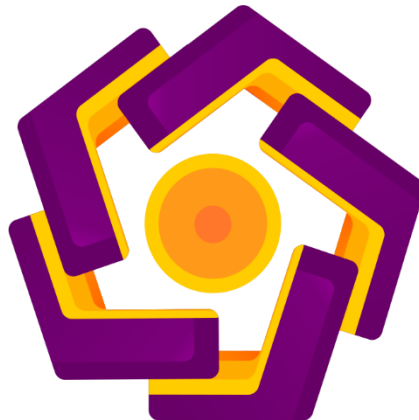
**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2024

**ANALISIS BUKTI DIGITAL FORENSIK TERKAIT
PENGUNAAN TEKNIK STEGANOGRAFI PADA
KASUS CYBER SEXUAL HARASSMENT**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

ZEPIN NOSSA

18.83.0264

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2024

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS BUKTI DIGITAL FORENSIK TERKAIT PENGGUNAAN
TEKNIK STEGANOGRAFI PADA KASUS CYBER SEXUAL
HARASSMENT**

yang disusun dan diajukan oleh

Zepin Nossa

18.83.0264

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 Agustus 2024

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom

NIK. 190302181

HALAMAN PENGESAHAN
SKRIPSI
ANALISIS BUKTI DIGITAL FORENSIK TERKAIT PENGGUNAAN
TEKNIK STEGANOGRAFI PADA KASUS CYBER SEXUAL
HARASSMENT

yang disusun dan diajukan oleh

Zepin Nossa

18.83.0264

Telah dipertahankan di depan Dewan Penguji
pada tanggal 20 Agustus 2024

Susunan Dewan Penguji

Nama Penguji

Andika Agus Slameto, M.Kom
NIK. 190302109

Yudi Sutanto, M.Kom
NIK. 190302039

Joko Dwi Santoso, M.Kom
NIK. 190302181

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Agustus 2024

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom., Ph.D.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Zepin Nossa
NIM : 18.83.0264

Menyatakan bahwa Skripsi dengan judul berikut:

**Analisis Bukti Digital Forensik Terkait Penggunaan Teknik Steganografi
Pada Kasus Cyber Sexual Harassment**

Dosen Pembimbing : Joko Dwi Santoso, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 Agustus 2024

Yang Menyatakan,



Zepin Nossa

HALAMAN PERSEMBAHAN

Segala puji dan syukur saya panjatkan kepada Allah SWT, yang telah memberikan karunia, kekuatan, dan petunjuk-Nya, sehingga saya dapat menyelesaikan skripsi ini dengan baik. Skripsi ini saya persembahkan untuk:

1. Ibu saya tercinta Mama Sutarni dan khususnya untuk almarhum Papa saya La Onga yang telah memberikan cinta dan inspirasi yang tiada henti. Semoga doa dan kebaikannya selalu menyertai langkah saya dalam mencapai cita-cita. Serta adik saya Reevan Arvano Zahir yang selalu mendoakan dan memberi semangat.
2. Berterimakasih kepada diriku sendiri Zepin Nossa, sebagai ungkapan terima kasih atas segala usaha, perjuangan, dan ketekunan yang telah saya tunjukkan dalam menyelesaikan setiap tantangan selama perjalanan ini.
3. Terima kasih kepada Bapak Joko Dwi Santoso, M.Kom selaku dosen pembimbing saya karena bimbingan dan dukungan Anda selama proses ini telah memberikan banyak inspirasi dan pengetahuan.
4. Kepada teman dan sahabat saya, khususnya Nadil, Erlina, dan Laras yang telah memberikan dukungan dan menjadi teman serta sahabat yang baik untuk saya serta membantu saya dalam menyelesaikan skripsi ini. Serta untuk keluarga saya Mida dan Aisyah yang telah memberikan dukungan, menemani, memberikan semangat kepada saya.

KATA PENGANTAR

Puji syukur saya panjatkan kepada Allah SWT atas segala rahmat dan karunia-Nya, sehingga saya dapat menyelesaikan skripsi ini yang berjudul “Analisis Bukti Digital Forensik Terkait Penggunaan Teknik Steganografi Pada Kasus *Cyber Sexual Harassment*”. Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Pada kesempatan ini, penulis akan menyampaikan banyak terima kasih kepada beberapa pihak:

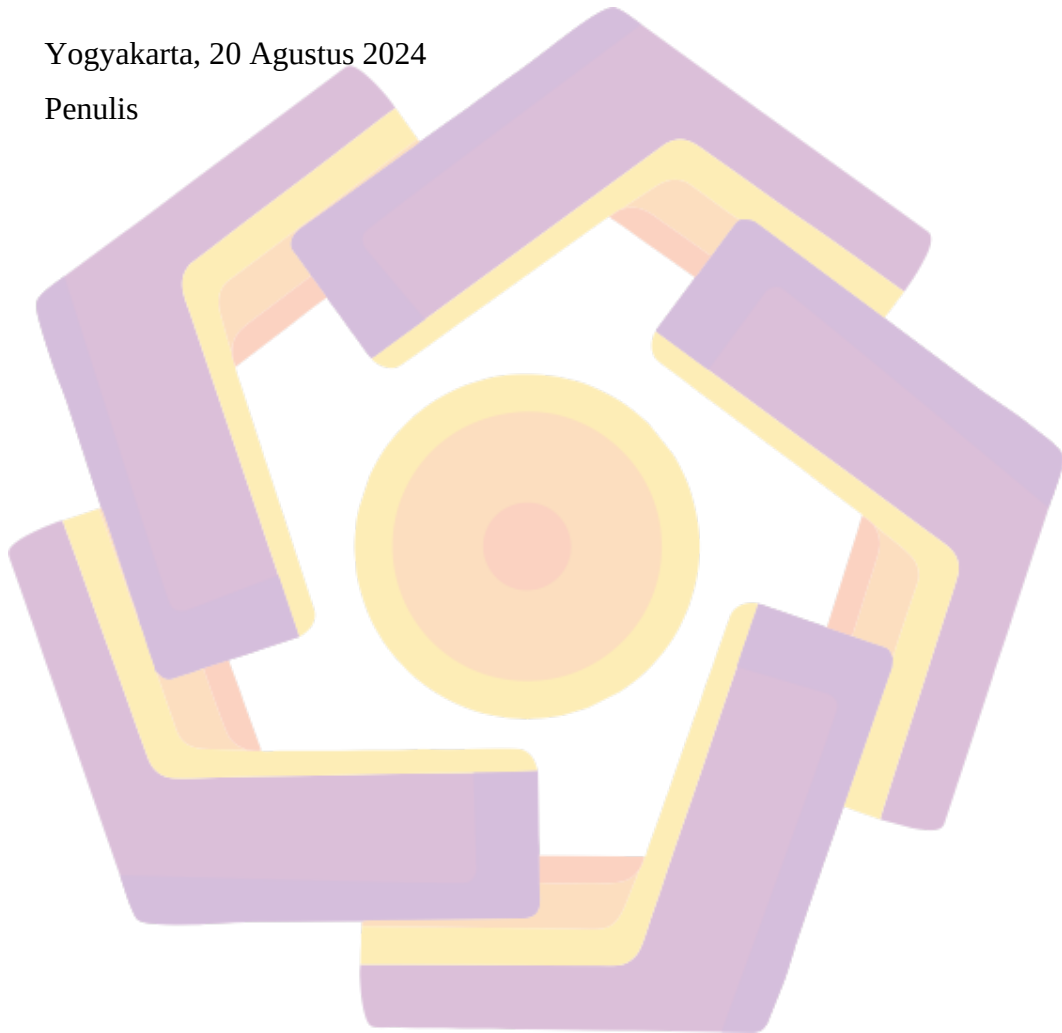
1. Allah SWT karena atas rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan baik tanpa pertolongan-Nya, semua usaha ini tidak mungkin terwujud.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta
3. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta
4. Bapak Joko Dwi Santoso, M.Kom selaku dosen pembimbing yang telah memberikan saya bimbingan, dukungan, dan inspirasi dalam menyelesaikan penyusunan Skripsi ini.
5. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku perkuliahan dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
6. Orang tua, adik, keluarga besar dan sahabat yang selalu mendoakan dan memberikan support mental kepada penulis.

Dalam penyusunan skripsi ini penulis menyadari masih jauh dari kata sempurna karena terbatasnya pengalaman dan pengetahuan penulis, Penulis mengharapkan skripsi ini kedepannya akan memberikan manfaat kepada pihak yang

membutuhkan serta menjadi acuan dalam penelitian kedepannya. Penulis juga mengharapkan saran, kritik serta masukan yang dapat membantu menyempurnakan skripsi ini.

Yogyakarta, 20 Agustus 2024

Penulis



DAFTAR ISI

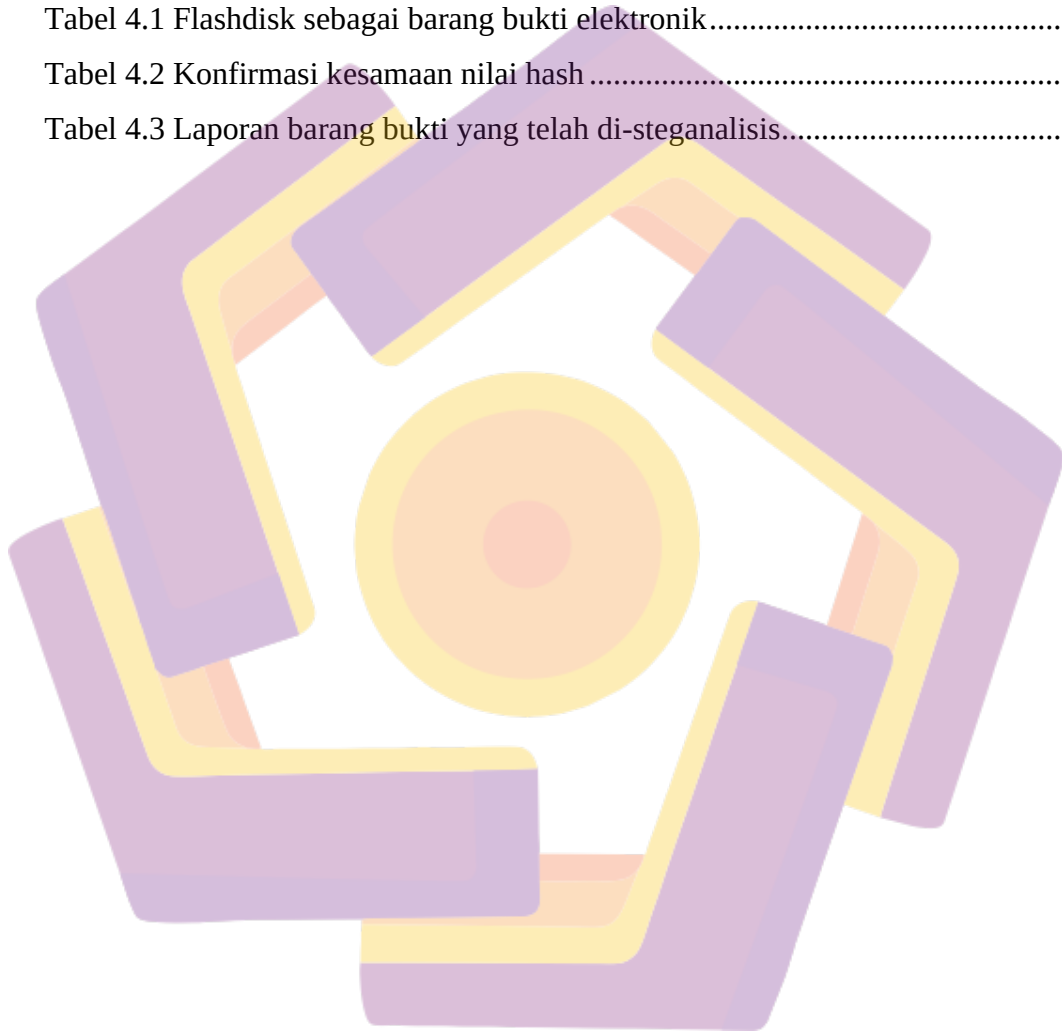
HALAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKIRPSI	iv
HALAMAN PERSEMBAHAN	iv
KATA PENGANTAR	vi
DAFTAR ISI.....	iii
DAFTAR TABEL.....	vi
DAFTAR GAMBAR.....	vii
INTISARI	ix
ABSTRACT.....	x
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Sistematika Penelitian	5
BAB II TINJAUAN PUSTAKA	6
2.1 Studi Literatur	6
2.2 Forensik Digital	17
2.3 Steganografi	18

2.4 Steganalisis	18
2.5 Bukti Digital (Digital Evidence)	19
2.6 Media Penyimpanan <i>Flashdisk</i>	20
2.7 Cybercrime Sexual Harassment	20
2.8 Peraturan Undang-Undang tentang Informasi dan Transaksi Elektronik	21
2.9 Autopsy	25
2.10 FTK Imager	25
2.11 OpenStego	26
2.12 Steganographystudio	27
2.13 Metode National Institute of Standards and Technology	27
2.13.1 Collection	28
2.13.2 Examination	28
2.13.3 Analysis	29
2.13.4 Reporting	29
BAB III METODOLOGI PENELITIAN	30
3.1 Alur Penelitian	30
3.1.1 Tinjauan Pustaka	31
3.1.2 Skenario Kasus	31
3.1.3 Proses Pengambilan Data	33
3.1.4 Alat dan Bahan Penelitian	34
3.2 Analisis Digital Forensik menggunakan NIST	35
3.2.1 Collection	36
3.2.2 Examination	37
3.2.3 Analysis	37
3.2.4 Reporting	38

3.3 Steganalisis	38
3.4 Evaluasi Hasil	38
BAB IV HASIL DAN PEMBAHASAN	39
4.1 Persiapan	39
4.1.1 Instalasi Tools	39
4.2 Skenario Penelitian	41
4.2.1 Implementasi Skenario Penelitian.....	42
4.3 Collection.....	43
4.3.1 Pengambilan Data dari <i>Flashdisk</i>	44
4.3.2 Validasi Nilai Hash	50
4.4 Examination	52
4.5 Analysis.....	53
4.5.1 Analisis Histogram.....	54
4.5.2 Ekstraksi menggunakan OpenStego.....	58
4.5.3 Ekstraksi menggunakan Steganographystudio.....	63
4.6 Reporting.....	66
BAB V KESIMPULAN DAN SARAN	69
5.1 Kesimpulan	69
5.2 Saran	70
REFERENSI	72

DAFTAR TABEL

Tabel 2.1 Tinjauan Pustaka.....	10
Tabel 2.2 Perubahan Undang- Undang.....	22
Tabel 3.1 Proses pengambilan data.....	34
Tabel 4.1 Flashdisk sebagai barang bukti elektronik.....	44
Tabel 4.2 Konfirmasi kesamaan nilai hash	51
Tabel 4.3 Laporan barang bukti yang telah di-steganalisis.....	67



DAFTAR GAMBAR

Gambar 2.1 Alur kerangka kerja NIST	28
Gambar 3.1 Alur Penelitian	30
Gambar 3.2 Simulasi Kasus	32
Gambar 3.3 Proses pengambilan data	33
Gambar 3.4 Tahapan metode NIST	36
Gambar 4.1 Proses instalasi Autopsy	40
Gambar 4.2 Proses instalasi OpenStego	41
Gambar 4.3 File sampel pada flashdisk	42
Gambar 4.4 File foto pada flashdisk setelah file sample dihapus	42
Gambar 4.5 File Sampel	43
Gambar 4.6 proses akuisisi pada flashdisk	44
Gambar 4.7 Pemilihan tipe Drive barang bukti digital	45
Gambar 4.8 USB Device 15GB sebagai media penyimpanan barang bukti	45
Gambar 4.9 Pengaturan spesifikasi <i>Image Destination</i>	46
Gambar 4.10 Spesifikasi pertama : <i>Image Type</i>	46
Gambar 4.11 Spesifikasi kedua : <i>Evidence Item Information</i>	47
Gambar 4.12 Spesifikasi ketiga: <i>Image Destination Folder, Image Filename</i> dan <i>Image Fragment Size</i>	47
Gambar 4.13 Hasil <i>Image Destination</i> dari semua spesifikasi	48
Gambar 4.14 Proses <i>Imaging</i> yang sedang berjalan	48
Gambar 4.15 Tampilan prose verifikasi <i>image</i>	49
Gambar 4.16 <i>Image Verify Results</i>	49
Gambar 4.17 <i>Output file image flashdisk</i> yang berhasil di akuisisi	50
Gambar 4.18 Konfirmasi nilai hash menggunakan FTK Imager	51
Gambar 4.19 Analisis Hasil Akuisisi Menggunakan Autopsy	52
Gambar 4.20 Hasil Ekstraksi File yang Telah Terhapus	53
Gambar 4.21 File yang berhasil diekstrak	53
Gambar 4.22 Histogram Ilustrasi1	54
Gambar 4.23 Histogram Ilustrasi2	54
Gambar 4.24 Histogram Ilustrasi3	55

Gambar 4.25 Histogram Ilustrasi4	55
Gambar 4.26 Histogram Ilustrasi5	56
Gambar 4.27 Histogram Ilustrasi6	56
Gambar 4.28 Histogram Ilustrasi7	57
Gambar 4.29 Histogram Ilustrasi8	57
Gambar 4.30 Histogram Ilustrasi9	58
Gambar 4.31 Histogram Ilustrasi10	58
Gambar 4.32 Ekstraksi file Ilustrasi1: Tidak berhasil	59
Gambar 4.33 Ekstraksi file Ilustrasi2: Tidak berhasil	59
Gambar 4.34 Ekstraksi file Ilustrasi3: Tidak berhasil	60
Gambar 4.35 Ekstraksi file Ilustrasi4: Tidak berhasil	60
Gambar 4.36 Ekstraksi file Ilustrasi5: Tidak berhasil	61
Gambar 4.37 Ekstraksi file Ilustrasi6: Berhasil.....	61
Gambar 4.38 Ekstraksi file Ilustrasi7: Tidak berhasil	62
Gambar 4.39 Ekstraksi file Ilustrasi8: Tidak berhasil	62
Gambar 4.40 Ekstraksi file Ilustrasi9: Tidak berhasil	62
Gambar 4.41 Ekstraksi file Ilustrasi10: Tidak berhasil	63
Gambar 4.42 Ekstraksi file Ilustrasi1: Tidak berhasil	63
Gambar 4.43 Ekstraksi file Ilustrasi2: Berhasil.....	64
Gambar 4.44 Ekstraksi file Ilustrasi3: Tidak berhasil	64
Gambar 4.45 Ekstraksi file Ilustrasi4: Tidak berhasil	64
Gambar 4.46 Ekstraksi file Ilustrasi5: Berhasil.....	65
Gambar 4.47 Ekstraksi file Ilustrasi6: Tidak berhasil	65
Gambar 4.48 Ekstraksi file Ilustrasi7: Tidak berhasil	65
Gambar 4.49 Ekstraksi file Ilustrasi8: Tidak berhasil	66
Gambar 4.50Ekstraksi file Ilustrasi9: Tidak berhasil	66
Gambar 4.51 Ekstraksi file Ilustrasi10: Tidak berhasil	66
Gambar 4.52 File yang berhasil diekstraksi.....	67

INTISARI

Perkembangan teknologi dan komunikasi memiliki banyak manfaat yang didapatkan dari berbagai hal seperti, pengguna teknologi diberi kemudahan dalam mencari dan mengakses semua yang ingin diketahui. Dan banyak dampak positif lainnya yang didapatkan dengan berkembangnya teknologi komunikasi. Tetapi hal ini juga menjadi celah yang digunakan oleh pelaku kejahatan dengan memanfaatkan teknologi yang ada untuk melakukan kejahatannya. Salah satu bentuk kejahatan yang terjadi dengan memanfaatkan teknologi yaitu penggunaan teknik steganografi untuk berbuat kejahatan. Penggunaan teknik steganografi merupakan salah satu bentuk kejahatan yang memanfaatkan teknologi komputer. Dengan menyisipkan pesan atau informasi rahasia kedalam suatu citra, sehingga pihak yang lain tidak dapat mengetahui adanya pesan rahasia dalam suatu media atau data seperti kasus *cyber sexual harassment*. *Cyber sexual harassment* merupakan tindak kejahatan berupa pelecehan seksual secara tidak langsung tetapi melalui dunia maya. Pelaku menyisipkan informasi pribadi korban kedalam *flashdisk* dan terjadi transaksi elektronik terhadap barang bukti tersebut. Penelitian ini bertujuan untuk melakukan implementasi dengan mengakuisisi serta mengekstraksi semua barang bukti digital dalam kasus *cyber sexual harassment*. Tools yang digunakan dalam penelitian ini yaitu FTK Imager, Autopsy, Steganographystudio dan OpenStego. Metode yang digunakan dalam penelitian ini yaitu metode *National Institute of Standard and Technology* (NIST). Hasil yang diperoleh dalam penelitian ini yaitu OpenStego berhasil mengekstraksi 10% file bukti digital, sedangkan Steganographystudio berhasil 20% dalam mengekstraksi file bukti digital.

Kata kunci: Steganalisis, Autopsy, Openstego, Steganographystudio, NIST

ABSTRACT

The development of technology and communication has many benefits derived from various things, such as technology users being given the convenience of finding and accessing everything they want to know. And there are many other positive impacts that can be had with the development of communication technology. However, this is also a loophole criminals use to use existing technology to commit crimes. One form of crime that occurs by utilizing technology is using steganography techniques to commit crimes. Using steganography techniques is a form of crime that utilizes computer technology by inserting a secret message or information into an image so that other parties cannot know that there is a hidden message in a media or data, such as in cases of cyber sexual harassment. Cybersexual harassment is a crime in the form of sexual harassment indirectly but through cyberspace. The perpetrator inserted the victim's personal information into a flash disk, and an electronic transaction occurred with the evidence. This research aims to implement it by acquiring and extracting all digital evidence in cases of sexual harassment. The tools used in this research are FTK Imager, Autopsy, Steganographystudio, and OpenStego. The method used in this research is the National Institute of Standards and Technology (NIST) method. The results obtained in this research were that OpenStego successfully extracted 10% of digital evidence files, while Steganographystudio was 20% successful in extracting digital evidence files.

Keyword: *Steganalysis, Autopsy, Openstego, Steganographystudio, NIST*