BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisis yang telah dilakukan dalam proses forensik digital pada kasus *cyber sexual harassment* terkait penggunaan teknik steganografi dimana terdapat 10 (sepuluh) file foto yang terdapat dalam *flashdisk* dan file tersebut telah dihapus untuk mengilangkan barang bukti digital, maka dapat disimpulkan bahwa penggunaan metode *National Institute of Standards and Technology* (NIST) pada penelitian ini dapat digunakan atau diimplementasikan pada kasus yang berkaitan dengan forensik digital untuk membantu proses investigasi. Metode *National Institute of Standards and Technology* (NIST) memiliki 4 tahapan proses analisis dalam kasus *cyber sexual harassment* terkait penggunaan teknik steganografi. Proses analisis menggunakan metode NIST sebagai berikut:

1. *Collection:* melakukan akuisisi terhadap file-file yang terdapat dalam *flashdisk* serta melakukan *imaging* pada data tersebut agar tidak terjadi kerusakan pada barang bukti asli menggunakan tool FTK Imager. Serta melakukan pencocokan nilai hash dari barang bukti digital dan file *imaging*.
2. *Examination*: melakukan pengujian pada file *imaging* sebelumnya menggunakan tool Autopsy. Pada tahap ini peneliti akan melakukan pencarian terhadap file yang telah dihapus dan mengekstraksi file yang telah dihapus tersebut kedalam perangkat investigator. File yang akan di-*recovery* dan diekstraksi yaitu file 10 file sampel yang terdapat dalam *flashdisk*.
3. *Analysis:* hasil dari proses *recovery* dan ekstraksi sebelumnya akan dilakukan analisis. Proses analisis yang dilakukan yaitu steganalisis pada barang bukti digital. Proses steganalisis menggunakan metode analisis histogram yaitu dimana file sampel akan dianalisis menggunakan grafik dengan melihat perubahan frekuensi dari nilai

pixel gambar tersebut. Perubahan dari frekuensi nilai pixel tergantung dari besarnya perbedaan warna gambar *cover* dan file steganografi. Steganalisis pada penelitian ini menggunakan dua tool dalam mengekstraksi file yang diidentifikasi memiliki pesan rahasia atau file steganorafi didalamnya yaitu OpenStego dan Steganographystudio.

4. *Reporting:* melakukan pelaporan hasil analisis mengenai penggunaan tools yang ada dalam penelitian ini dan evaluasi hasil presentase keberhasilan dari tools yang digunakan.

Terdapat 4 tools yang digunakan dalam penelitian ini, yaitu pertama FTK Imager untuk melakukan *imaging* pada barang bukti digital, Autopsy untuk me-*recovery* file yang telah dihapus dalam *flashdisk* serta OpenStego dan Steganographystudio untuk melakukan ekstraksi file steganografi. File steganografi dapat terdeteksi atau teridentifikasi menggunakan analisis histogam tetapi beberapa file steganografi tersebut tidak dapat diidentifikasi menggunakan tools OpenStego dan Steganographystudio. Analisis histogram dapat mengidentifikasi suatu gambar dari frekuensi nilai pixelnya. Jika terdapat perbedaan besar antara file *cover* dan file steganografi maka dapat terlihat dari grafik yang ditampilkan pada histogram. Proses analisis dan ekstraksi menggunakan OpenStego memiliki akurasi yang sangat kecil dalam mengidentifikasi file steganografi yaitu sebesar 10% dari 10 sampel yang ada. Sedangkan untuk tool Steganographystudio memiliki akurasi yang sama kecilnya dalam mengidentifikasi dan menganalisis file steganografi yaitu sebesar 20% dari 10 sampel gambar.

5.2 Saran

Saran yang akan diberikan oleh peneliti kepadap peneliti selanjutnya adalah sebagai berikut:

1. Kepada peneliti berikutnya agar mencoba menggunakan tools lainnya untuk menganalisis file steganografi
2. Penelitian ini menggunakan metode *National Institute of Standard and Technology* (NIST) dalam menganalisis barang bukti digital,

untuk peneliti selanjutnya bisa menggunakan metode penelitian lain yang dapat digunakan untuk menganalisis bukti digital forensik.

3. Peneliti selanjutnya dapat mengekspor banyak tools yang dapat digunakan agar dapat menyempurnakan proses penelitian selanjutnya.