BAB 5
Kesimpulan dan Saran

5.5 Kesimpulan

Berdasarkan hasil pengujian dan analisis yang telah dilakukan dapat diambil kesimpulan bahwa:

1. *Tool* Mail Header Extractor dapat menerjemahkan informasi dari *header email* dan memetakannya ke dalam konsep 4W1H (*Who*, *What*, *When*, *Where*, dan *How*). Pertanyaan *Who* dapat menjawab siapa pengirim dan penerima email, informasi ini diperoleh dari *field From, To,* dan *Cc*. *What* dapat menjawab apa subjek dan file lampiran pada email yang informasinya didapatkan dari *field Subject* dan *Content-Disposition*. Sedangkan untuk pertanyaan *When* dapat menjawab kapan waktu email dikirim oleh pengirim dan diterima oleh penerima, *field Date* dan *X-Received* dibutuhkan untuk menjawab pertanyaan ini. Pertanyaan *Where* dapat menjawab di mana lokasi *server* pengirim email serta alamat IP-nya yang informasinya diperoleh dari *field Received-SPF*. Untuk pertanyaan *How* dapat menjawab bagaimana proses pengiriman email dari pengirim ke penerima, *server* apa saja yang dilewati beserta protokolnya, informasinya didapatkan dari *field Received* dan *X-Received*.
2. *Tool* Mail Header Extractor memiliki kemampuan untuk menunjukkan indikasi adanya *email fraud* maupun *email spoofing* yang dapat membantu investigator dalam melakukan forensik email. Proses deteksi *email fraud* dilakukan dengan membandingkan kata pada pada subjek da nisi dengan kata yang ada pada kamus. Sedangkan proses deteksi *email address spoofing* dilakukan dengan membandingkan nama domain pada *field Message-ID* dengan nama domain pada kamus domain yang berisi nama domain dari situs *fake mailer*. Untuk proses deteksi *email time spoofing* dilakukan dengan membandingkan waktu pengiriman email dengan waktu penerimaan email.

5.6 Saran

Karena terdapat keterbatasan pada penelitian ini, sehingga untuk penelitian selanjutnya diharapkan dapat melakukan hal berikut:

1. Memperkaya fitur *tool* Mail Header Extractor dengan melakukan identifikasi kemungkinan kejahatan email yang memanfaatkan poin *Where* dan *How*.

2. Melakukan optimasi dalam proses deteksi *email fraud* dengan cara melakukan klasifikasi pola dan bentuk kalimat.