BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini berhasil membandingkan beberapa tool live forensic dengan studi kasus skenario dimana artifak-artifak tersebut dapat dicari dan dianalisis. Berbagai artefak seperti riwayat browser, riwayat command line, karakter yang diketikkan oleh user dan semua skenario yang dibuat dapat dibuktikan, dari perolehan perbandingan performa tools maka dapat diambil kesimpulan sebagai berikut :

1. Dari hasil analisis yang didapatkan terdapat berbagai informasi yang sekiranya cukup penting atau riskan. Mulai dari aktivitas browsing yang sifatnya private hingga catatan penting yang tulis pada notepad ataupun stickynote.
2. Penelitian ini juga telah berhasil mengevaluasi performa dari masing-masing tools yang telah digunakan. Mulai dari tools *Volatility* mendapatkan persentase keberhasilan sebesar 90% kemudian *Rekall* mendapatkan persentasi keberhasilan sebesar 70% serta *Redline* mendapatkan keberhasilan hanya sebesar 45%. Yang dimana tools *Volatility* dan *Redline* dapat dijalankan pada sistem operasi Windows, sedangkan pada tools *Rekall* hanya dapat dijalankan pada sistem operasi Linux.
3. Teknik yang digunakan untuk mengakuisisi sebuah artefak yakni *String Analysis* yang dimana dengan memanfaatkan sebuah tools mulai dari Volatility untuk mencari sebuah kata kunci atau memfilter sebuah keyword sesuai dengan data yang perlu dicari.
4. Berdasarkan hasil Analisa dan pembahasan pada bab sebelumnya, maka dapat disimpulkan bahwa terdapat beberapa data atau artefak yang tidak sepenuhnya dapat ditemukan.

5.2 Saran

Pada penelitian ini masih terdapat banyak kekurangan, sehingga peneliti berharap akan datang penelitian seputar live forensic dengan objek ataupun studi kasus lain masih dapat terus dapat dikembangkan. Berikut beberapa saran untuk penelitian kedepannya antara lain :

1. Masih terdapat beberapa perintah atau plugin yang penulis masih belum diketahui sehingga tidak dapat memberikan hasil yang optimal dan tidak dapat memberikan data digital sesuai dengan skenario yang telah dibuat.
2. Skenario yang telah dibuat oleh penulis masih terbatas pada lingkungan sistem operasi Windows 7 dan pada proses pengcaptureannya berbagai aplikasi masih di dalam kondisi terbuka atau aktif sehingga masih di perlukan berbagai uji coba atau eksperimen dengan kondisi lain dan sistem operasi yang lain.