BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan analisis live forensic dengan metode NIST pada skenario yang telah dibuat dapat diambil beberapa kesimpulan yaitu :

1. Analisis menggunakan live forensic memerlukan kehati-hatian karena setiap hal yang di lakukan pada komputer akan berdampak pada hasil analisis. Khusus nya dalam skenario yang di lakukan pada penelitian ini spesifikasi dari komputer tersangka yang di gunakan hanya memiliki kapasitas 2GB RAM yang berarti hanya mampu menampung proses sebesar 2GB saja dan apabila lebih dari itu proses akan di timpa dengan proses yang baru.
2. Dalam penelitian live forensic menggunakan teknik string analisis dengan tools volatility dan plugin yara memberikan keefektifan dalam analisis karena mampu memfilter secara keseluruhan PID dengan keyword yang diinginkan, namun kecepatan dari analisa tersebut bergantung dari seberapa besar resource dari komputer investigator
3. Analisa live forensic menggunakan teknik file carving dengan tools foremost dapat mempermudah investigator dalam mengambil gambar – gambar apa saja yang di download atau di kirimkan oleh tersangka namum ukuran gambar yang mampu di ambil oleh tools ini hanya 20-30% dari ukuran sebenarnya. Yang menyebabkan gambar yang di ambil oleh tools ini terkadang terpotong atau blur.

5.2 Saran

1. Melakukan pengembangan *plugin* dari *tool volatility* memori forensik untuk analisa *web browser* dari *engine browser* yang lain atau mengembangkan *tools volatility* untuk melakukan *automation string filtering*
2. Penelitian selanjutnya diharapkan dapat mengimplementasikan analisa *live forensic* dengan teknik *string filtering* untuk menemukan *chatting* dengan platform *telegram web*.
3. Penelitian selanjutnya diharapkan dapat melakukan analisa *live* forensik memori RAM dengan sistem operasi linux.