BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil yang diperoleh pada proses penerapan dari live forensik dan disk forensic dengan berbagai cara menyembunyikan barang bukti terhadap skenario aktivitas browsing kejahatan transaksi narkotika pada Browser Chrome maka dapat ditarik beberapa kesimpulan yaitu :

a) Penggunaan metodologi forensik NIJ dalam tahapan investigasi yang dilakukan memperoleh alur penelitian secara sistematis, dan dapat dijadikan acuan dalam penelitian disk forensic.

b) Dari hasil Penelitian, peneliti berhasil melakukan proses pengumpulan data atau tahap collection pada investigasi live forensik berdasarkan standar NIJ, dengan menambahkan sedikit improvisasi pada tools yang digunakan untuk mempersingkat waktu yang dilakukan.

c) Duplikasi atau imaging dilakukan untuk meminimalisir terjadinya sabotase maka dari itu peneliti menggunakan barang bukti yang telah di imaging sebagai bahan yang dianalisa dan barang bukti utamanya disimpan sebagai barang bukti di pengadilan, Dan untuk melakukan analisa perbandingan antara kedua bukti tersebut peneliti berhasil memanfaatkan tools md5 checker dan checksum untuk mencocokan bit dari kedua file tersebut.

d) Teknik File carving yang berhasil diimplementasikan oleh peneliti menggunakan tools foremost, dengan memanfaatkan bukti digital dari ram tersangka peneliti berhasil memperoleh artefak seperti file URL yang telah di kunjungi, email, gambar, audio dan video menggunakan kedua tools tersebut. Selain teknik file carving peneliti juga berhasil menggunakan teknik string analisis atau string filtering dengan memanfaatkan tools volatility dengan tambahan plugin yarascan.

e) Live forensic memiliki keunggulan jauh dalam hal perolehan barang bukti yang lebih banyak dibanding disk forensic, pada semua skenario penghapusan jejak digital oleh pelaku masih dapat berhasil dianalisa menggunakan live forensic.

f) Browser brave pada umumnya sama seperti browser lainnya seperti google chrome atau mozilla namun dikarenakan fitur Private with Tor pengamanan transmisi data nya lebih berlapis karena enkripsi dari jaringan tor itu sendiri, namun bukti digital yang diperoleh dari sistem tersangka yang telah dilakukan skenario sebelumnya tetap melalui teknik live forensik, tetap bisa dibaca atau digali informasi didalamnya seperti, url yang telah dikunjungi, serta keyword yang digunakan dalam surfing, dan sebagainya.

5.2 Saran

Pada penelitian ini masih didapat beberapa kekurangan, sehingga harapan peneliti dalam waktu yang akan datang penelitian seputar *disk forensic* dan live forensic masih dapat terus dikembangkan. Berikut beberapa saran untuk penelitian kedepannya antara lain :

a) Skenario serangan *disk anti forensic* pada penelitian ini terbatas pada skenario browser Chrome, masih ada browser lain seperti Brave, TOR Browser dan lain lain yang mungkin memiliki hasil ataupun peluang yang berbeda.
b) Selain ketiga toolkit yang sudah diuji dalam penelitian ini, masih banyak toolkit yang lainnya. Untuk itu disaran agar melakukan penelitian dengan menggunakan toolkit yang lain tersebut. Diharapkan penelitian selanjutnya dapat menggunakan tools dan teknik yang berbeda sehingga dapat mencari perbandingan pada tools image forensics yang terbaik, efektif dan efisien.
c) Penelitian selanjutnya diharapkan dapat melakukan analisa live forensik memori ram dengan sistem operasi linux.
d) Diharapkan penelitian selanjutnya dapat menggunakan tools dan teknik yang berbeda sehingga dapat mencari perbandingan pada tools image forensics yang terbaik, efektif dan efisien.