

## **BAB V PENUTUP**

### **1.1 Kesimpulan**

Berdasarkan hasil penelitian dengan menggunakan metode Disk Network Forensic dan berdasarkan skenario skenario penghilangan jejak barang bukti yang sudah dibuat, tidak semua data yang sudah terhapus dapat dikembalikan dan dijadikan barang bukti walaupun dengan bantu tool.

Sehingga, penelitian juga diharapkan dapat memberikan rekomendasi tools yang digunakan terutama pada software dalam mendeteksi dan mengidentifikasi data data digital yang sudah terhapus. Setelah penelitian investigasi USB Flashdisk dengan skema serangan anti forensic selesai dilakukan, maka didapat kesimpulan sebagai berikut :

- a) Penggunaan Penggunaan metodologi forensik NIST dalam tahapan investigasi yang dilakukan memperoleh alur penelitian secara sistematis, dan dapat dijadikan acuan dalam penelitian disk forensic.
- b) Dari keempat skenario anti forensic dengan analisa berbagai metode ataupun tool, kusus pada file dengan tipe xls penulis tidak dapat melakukan recovery sama sekali.
- c) Aktivitas anti forensic (file wiping) yang penulis buat dalam rancangan simulasi berhasil dianalisis dan dijabarkan alurnya dengan menganalisis bukti terkait menggunakan disk dengan bantuan berbagai tool forensik.
- d) Tahap analisis disk forensic dengan skenario anti forensic pada penelitian ini tidak mendalam, hanya sebatas pembuktian perbandingan kinerja tool recovery.
- e) Ketika proses penelitian berjalan, peneliti menemukan tantangan yang benar-benar menarik dari sisi anti forensic (file wiping), yaitu ketika suatu disk penyimpanan dilakukan overwrite secara terus menerus, maka file yang terhapus akan sulit sekali direcovery. Sehingga mungkin ini menjadi kelemahan dari barang bukti disk (hdd, usb) ketika pelaku tau cara menghapus jejak digital dengan metode anti forensic.

## 1.2 Saran

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

- a) Skenario serangan disk anti forensic pada penelitian ini terbatas pada barang bukti USB Flashdisk, masih ada drive penyimpanan lain seperti harddisk, NVME, SSD 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.

