BAB V
PENUTUP

5.1. Kesimpulan

Melihat dari hasil penelitian, Analisis Forensik Jaringan *Virtual Router* Menggunakan *Framework NIST Sp800-86*, berdasarkan rumusan masalah, tujuan penelitian dan hipotesis dapat disimpulkan bahwa:

1. Perancangan *virtual router* sangat dapat memberikan router tambahan jika hanya dimiliki 1(*router*) saja sehingga jelas memastikan dapat mengurangi biaya pembelian *router*.
2. Dibutuhkan waktu yang singkat dalam proses analisis serangan DOS forensik jika memanfaatkan rancangan jaringan pada penelitian ini, terbukti dalam setiap protokol mendeteksi lalu lintas yang tidak biasa.
3. Bukti diperoleh bahwa penyerang menggunakan alamat 192.168.10.252 dan 192.168.20.253 menggunakan perangkat *SonyMobile* dengan *Mac Address* 58:48:22:6e:17:e0
4. Karakteristik bukti pada *virtual router* dalam penelitian ini, mendapatkan alamat IP penyerang, alamat MAC maupun identitas perangkat yang digunakan yaitu SonyMobile.

5.2. Saran

Berdasarkan kesimpulan, rekomendasi utama yang disajikan di bagian ini untuk proses *forensic* selanjutnya adalah sebagai berikut:

1. Analis harus melakukan forensik menggunakan proses yang konsisten, seperti menggunakan kerangka kerja selain NIST, yaitu NIJ maupun DFRWS.
2. Analis harus melakukan forensik menggunakan 2(dua) atau lebih alat *forensic*, guna memvalidasi bukti lebih akurat, seperti *Network Miner*, *WinDump* maupun Metasploit.
3. Analis harus menyadari berbagai kemungkinan sumber data yang dapat menjadi bukti, seperti zona waktu saat terjadi penyerangan.
4. Menerapkan *logging* terpusat, melakukan *backup* sistem secara teratur dan pemantau keamanan sebagai upaya menghasilkan sumber data untuk forensik masa depan.