ABSTRAK

Seiring dengan berjalannya waktu, tingkat kriminalitas yang ada di Indonesia pun juga semakin meningkat. Kriminalitas yang dilakukan juga ada banyak ragam, baik dengan cara tradisional ataupun dengan cara modern. Untuk cara modern, pelaku biasanya melakukan teknologi, teknologi yang paling sering pelaku gunakan biasanya merupakan komputer. Untuk mengatasi hal tersebut, maka terdapat hal yang bernama forensik digital.

Pada penelitian ini dilakukan perhitungan risiko yang berdasar pada pendekatan *vulnerability* dan *threat*, setelah mendapatkan peringkat risiko dilakukan penentuan fungsi forensik berdasarkan peringkat risiko. Setelah mendapatkan fungsi forensik dilakukan pemilihan *software* yang dapat melakukan forensik pada VulnOS2 berdasarkan *framework Digital Forensic Readiness*. Data *vulnerability* didapatkan berdasarkan hasil *scanning* OpenVAS, sementara data *threat* didapatkan berdasarkan 10 *walkthrough* yang telah dipilih.

Dari hasil analisis data didapatkan risiko terbesar memiliki nilai 120, sementara untuk peringkat kedua memiliki risiko 28.6 dan risiko ketiga dan keempat memiliki nilai 0. Berdasarkan peringkat risiko didapatkan bahwa VulnOS2 memiliki fungsi forensik wajib pada *network forensic*. Sementara *computer forensic* merupakan fungsi pelengkap. Kemudian dilakukan pemilihan *software* yang dapat melakukan forensik pada VulnOS2 berdasarkan *framework Digital Forensic Readiness* dan didaatkan bahwa *software* yang dapat melakukan forensik pada VulnOS2 adalah Wireshark, Xplico dan NetworkMiner.

Kata Kunci : forensik digital, peringkat risiko, *framework Digital Forensic Readiness* dan fungsi forensik.