Analisis Metode Live Forensics Pada Perangkat Memory Laptop Untuk Pencarian Artefak Digital Berbasis Linux

M.Ainul Yaqin[1],Triawan Adi Cahyanto[2]
Sarjana Teknik Informatika
Universitas Muhammadiyah
Jember, Indonesia
Email : ainul.yakin009@gmail.com

ABSTRAK

Abstrak - Perkembangan teknologi komputer saat ini berdampak pada meningkatnya kasus kejahatan *cybercrime*. Seiring meluasnya penggunaan komputer maka dimungkinkan peluang kejahatan yang melibatkan komputer juga semakin meningkat baik secara langsung maupun tidak langsung. Untuk menanggulangi peristiwa tersebut selain dibutuhkan manajemen keamanan yang bertujuan untuk mencegah, diperlukan pula prosedur penanggulangan apabila peristiwa sudah terlanjur terjadi, dimana salah satu prosedur yang dilakukan adalah komputer forensics. Kasus *cybercrime* sekarang dapat mencuri informasi digital sensitif dan rahasia. Informasi tersebut dapat berupa email, user_id, dan password. Informasi berupa user_id, email dan password selain tersimpan pada cookies browser, juga tersimpan didalam memory perangkat laptop. Untuk itu diperlukan teknik atau metode yang tepat untuk menganalisis memory pada perangkat laptop. Hal ini dikarenakan data yang ada di memory perangkat bersifat volatile, data akan hilang jika komputer dimatikan atau mengalami restart. Dalam penelitian ini telah berhasil melakukan akuisisi pada memory perangkat laptop berbasis linux menggunakan metode live forensics dan telah berhasil menemukan artefak digital yang berkaitan dengan penelitian yaitu informasi mengenai user_id, email dan password pada facebook, account gmail, paypal dan link url. Pada Hasil Pengujian ditemukan jumlah total keseluruhan dari hasil pengujian sebagai berikut yaitu pada artefak_1 sebesar 100%, pada artefak_2 sebesar 57,14% dan pada artefak_3 adalah sebesar 71,42%.

Kata Kunci : Live Forensics, Memory Laptop, Artefak Digital

ABSTRACT

The development of computer technology now has an impact on the increasing cases of cybercrime. Along with the widespread use of computers, it is possible that the chances of crimes involving computers also increase both directly and indirectly. In order to cope with these events, in addition to the need for security management that aims to prevent, it is also necessary to overcome the procedure if the event has already occurred, where one of the procedures carried out is computer forensics. The case of cybercrime can now steal sensitive and confidential digital information. This information can be in the form of email, user_id, and password. Information in the form of user_id, e-mail and password besides being stored in browser cookies, is also stored in the laptop device memory. For that we need the right technique or method to analyze memory on a laptop device. This is because the data in the device memory is volatile, the data will be lost if the computer is turned off or restarted. In this study, it has been successful in acquiring memory on Linux-based laptop devices using the live forensics method and has succeeded in finding digital artifacts related to research, namely information about user_id, e-mail and passwords on facebook, gmail account, paypal and url link. In the test result found the total number of overall results of the test as follows, namely the artifacts_1 at 100% on the artifacts at 57,14% and the artifacts at 71,42%.

Keywords*: Live Forensics, Laptop Memory, Digital Artifacts*