Perancangan prosedur operasional standar penanganan alat bukti digital : studi kasus Kementerian Komunikasi dan Informatika = The Designing of standard operating procedure for digital evidence handling : a case study Ministry of Information and Communication technology

Syofian Kurniawan, author

Abstrak

Perkembangan dan kemajuan teknologi informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung menyebabkan lahirnya bentuk-bentuk perbuatan hukum baru (cybercrimes). Bukti digital, sebagai alat bukti penting untuk mengungkap cybercrime memiliki karakteristik khusus yaitu bersifat rapuh (dapat diubah, dihapus atau dirusak). Dalam Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) terdapat ketentuan terkait bukti digital yaitu bahwa informasi elektronik dan/atau dokumen elektronik akan dianggap sah dan diterima dipengadilan jika informasi yang terkandung di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya dan dapat dipertanggungjawabkan. Oleh karena itu, penelitian kali ini akan berfokus terhadap masalah penjaminan keutuhan alat bukti digital.
Salah satu hal yang dapat mempengaruhi keutuhan alat bukti digital adalah prosedur operasional standar penanganan alat bukti digital. Oleh karena itu, untuk menjamin keutuhan alat bukti digital, dalam penelitian ini dibuat Rancangan Prosedur Operasional Standar (POS) Penanganan Alat Bukti Digital bagi Kementerian Komunikasi dan Informatika. Perancangan dilakukan dengan menggunakan metodologi Soft System Methodology (SSM) yang dimodifikasi, metode hermeneutic untuk analisa data serta dengan memperhatikan standar/acuan Internasional (RFC 3227, NIST 800-86, NCJ 199408, NCJ 199408 dan ISO 27037) dan melakukan benchmark terhadap POS penanganan alat bukti digital yang sudah ada di Puslabfor Mabes Polri.
Penelitian menghasilkan 21 rancangan POS Penanganan Alat Bukti Digital yang terbagi kedalam tahap persiapan, penanganan di TKP, transportasi, penanganan di laboratorium, penyerahan alat bukti ke kejaksaan dan persiapan menjadi saksi ahli.
.....
Developments and advances in information technology have led to changes of human life activities in a variety of areas that directly lead to the birth of the forms of new legal acts (cybercrimes). Digital evidence, as an important evidence to uncover of cybercrime has special characteristics, that is fragile (can be changed, deleted, or destroyed with easily). The Law Number 11 of 2008 about Information and Electronic Transactions (UU ITE) have provisions related digital evidence such as: that the electronic information and/or electronic document shall be deemed valid and accepted in court if information contained in it can be accessed, displayed, guaranteed of it integrity and can be accountability. Therefore, this research will be focus on the problem of the integrity of digital evidence.
One things that can affect the integrity of digital evidence is standard Operating procedure of digital evidence handling. Therefore, to guarantee the integrity of digital evidence, in this research were prepared draft Standard Operating Procedure (SOP) of digital evidence handling for the Ministry of Information and Communication Technology. The draft is done using modified Soft System Methodology (SSM),

hermeneutic methods for data analysis and pay attention to the International standard/reference (RFC 3227, NIST 800-86, NCJ 199408, NCJ 199408 and ISO 27037) and doing benchmark to the SOP of digital evidence handling that have already exist in the Puslabfor Mabes Polri.
The research produce 21 draft of SOP digital evidence handling for the Ministry of Information and Communication Technology which is divided into several stages among others: preparation, scene handling, transport, handling process in the laboratory, submission of evidence and preparation to be an expert witness.