INTISARI

Chain of Custody adalah elemen penting dalam aktivitas forensik digital dan penanganan *cybercrime*. *Chain of Custody* berfungsi untuk menjaga integritas dan kredibilitas bukti digital dalam bentuk kronologis pencatatan interaksi dan pendokumentasian terhadapnya. Mengacu pada peraturan Perkap 10/2010 dan Perkap 08/2014 tentang Tatacara Penanganan Barang Bukti serta ISO 27037 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi bukti digital, maka saat ini terdapat kesenjangan dalam hal penanganan bukti digital serta *chain of custody* terhadapnya bila dibandingkan dengan barang bukti fisik. Kesenjangan ini dikarenakan tidak adanya framework yang menjadi acuan dalam hal penanganan bukti digital serta mekanisme interaksi terhadapnya. Hal ini terjadi karena karakteristik bukti digital yang spesifik dan kompleks sehingga implementasi *chain of custody* untuk bukti digital lebih sulit dibandingkan dengan barang bukti fisik.

Tiga permasalahan utama tentang penanganan barang bukti, yaitu: penyimpanan barang bukti, pencatatan informasi kontekstual dan kontrol terhadap aksesibilitas pada barang bukti menjadi fokus kajian pada penelitian ini. Hal ini dilakukan sebagai upaya untuk memberikan solusi terhadap permasalahan penanganan bukti digital dan *chain of custody* agar memiliki mekanisme yang sama dengan penanganan bukti fisik. Solusi tersebut dibangun dengan pendekatan regululasi sehingga menghasilkan sebuah Framework yang memuat aspek konseptual dan teknis yang kemudian diintegrasikan menjadi satu kesatuan terminologi dengan nama *Digital Evidence Cabinet* (DEC).

Digital Evidence Cabinet dibangun dari tiga komponen konseptual yaitu: *Post-Acquisition Handling, Workflow Process Chain of Custody (WPCoC-3IR)* dan *Pseudo-Metadata Chain of Custody*. Komponen konseptual tersebut menjadi landasan bagi aspek teknis *chain of custody* yang terdiri dua komponen, yaitu Lemari Imaginer Penyimpanan Bukti Digital (LIPBID) serta *Access Control for LIPBID*. Asumsi dasar yang digunakan pada framework ini adalah sentralisasi penyimpanan melalui analogi bentuk fisik dari kantong, label, rak dan lemari menjadi bentuk struktur digital melalui

pendekatan xml untuk komponen *evidence identifier, evidence unit, evidence bags, evidence rack, evidence cabinet dan evidence repository*. Selanjutnya untuk menunjukkan pentingnya *chain of custody* dalam aktivitas forensik digital, diberikan *general model* dan *conceptual model* yang melibatkan *primary source*, *original source* dan *working copy* dari bukti digital.

Implementasi *Digital Evidence Cabinet* telah diujicobakan untuk mendokumentasikan bukti elektronik dari kasus yang ditangani oleh Laboratorium Forensika Digital FTI UII serta kasus yang terdokumentasi pada arsip Putusan Mahkamah Agung. Hasil ujicoba menunjukkan kemampuan *Digital Evidence Cabinet* dalam merekam bukti elektronik, bukti digital, integritas serta interaksi pengguna terhadap bukti digital yang tersimpan di dalam media penyimpan. Output dokumen *chain of custody* yang dihasilkan oleh setiap bukti digital telah menujukkan ketersediaan data dan dokumentasi interaksi yang sesuai dengan keperluan pencatatan *chain of custody*.

Evaluasi terhadap *Digital Evidence Cabinet* dilakukan dengan menggunakan dua tahap evaluasi. Tahap pertama adalah evaluasi terhadap masing-masing komponen framework sesuai dengan karakteristiknya. Sementara tahap kedua adalah pengujian secara kesatuan framework melalui beberapa issue, seperti: spesifikasi umum, dampak penerapan dan kesesuaian dengan regulasi, metrik keamanan dan feedback expert melalui Daubert Criteria. Kedua tahap evaluasi tersebut menunjukkan bahwa *Digital Evience Cabinet* adalah solusi yang sesuai untuk problem *chain of custody* pada bukti digital serta menundukung konsistensi penerapan regulasi dalam hal penanganan barang bukti, baik yang sifatnya fisik maupun digital.

Kata kunci: bukti digital, bukti elektronik, forensik digital, *chain of custody*, metadata, *access control, digital evidence cabinet*, Perkap, Framework.

ABSTRACTION

Chain of Custody is an essential element in digital forensic activities and cybercrime. Chain of Custody serves to maintain the integrity and credibility of digital evidence in a chronological form of recording interactions and documenting evidence. Referring to Perkap 10/2010 and Perkap 08/2014 as regulations on Procedures for Handling Evidence and ISO 27037 on Guidelines for Identification, Collection, Acquisition, and Preservation of digital evidence, there are currently gaps in digital evidence handling and chain of custody when compared with the handling and chain of custody for physical evidence. This gap is due to the absence of framework that become a reference in terms of handling digital evidence and the mechanism of interaction with it. The characteristics of digital evidence are more complex so that the implementation of the chain of custody for digital evidence turns out to be more difficult than handling physical evidence.

The dissertation research proposes solutions in the form of Digital Evidence Cabinet as a framework for the chain of custody on digital evidence. The Digital Evidence Cabinet has been built on three conceptual components, namely: post-acquisition handling, Multiview workflow process, and pseudo metadata chain of custody. The conceptual component is the basis for the technical aspects of the chain of custody, which consists of two components, namely the Digital Evidence Storage Imaginer Cabinet (LIPBID) and Access Control. The basic assumptions used in conceptual and technical component are centralization of storage through the analogy of the physical form of bags, labels, shelves, and cabinets in the form of digital structures through the XML approach. Furthermore, to show the importance of chain of custody in digital forensic activities, then given a general model and conceptual model involving primary source, an original source, and working copy of digital evidence.

Implementing the Digital Evidence Cabinet has been tested to document the existence of electronic evidence from cases handled by the Digital Forensics

Laboratory as well as documented cases in the archives of the Decision of the Supreme Court. The test results show the ability of Digital Evidence Cabinet in recording electronic evidence, digital evidence, integrity, and user interaction with digital evidence stored in storage media. The chain of custody document output produced by each digital evidence has shown the availability of digital evidence data, documentation of interactions that are needed for recording chain of custody.

An evaluation of the Digital Evidence Cabinet is carried out using two stages of evaluation. The first stage is the evaluation of each element of the framework according to its characteristics. While the second stage is to use several issues, such as: general specifications, formal models, the impact of implementation and compliance with regulations, security metrics and expert feedback through Daubert Criteria. The two stages of evaluation strengthen the hypothesis that the Digital Evidence Cabinet is the right solution for the problem of the chain of custody of digital evidence that has been faced by examiners or agencies that handle digital evidence.

This study provides a solution to the gap in the application of chain of custody to digital evidence when compared with physical evidence. The solution provided is technical support for the implementation of digital evidence from a number of regulations such as: Perkap 10/2010 and its revision Perkap 08/2014, and ISO 27037, which so far is still oriented on physical evidence.

Keyword: Digital Evidence, electronic evidence, digital forencics, chain of custody, metadata, access control, digital evidence cabinet, regulation, framework.