MEMBANGUN MODEL INFORMASI METADATA UNTUK MENDUKUNG *CHAIN OF CUSTODY* BUKTI DIGITAL

Devi Ratnasari

15917206

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Magister Teknik Informatika

Program Pascasarjana fakultas Teknologi Industri

Universitas Islam Indonesia

2018

Lembar Pengesahan Pembimbing

MEMBANGUN MODEL INFORMASI METADATA UNTUK MENDUKUNG *CHAIN OF CUSTODY* BUKTI DIGITAL

Devi Ratnasari

15917206

Yogyakarta, Februari 2018

Pembimbing

Dr. Bambang Sugiantoro

Lembar Pengesahan Penguji

MEMBANGUN MODEL INFORMASI METADATA UNTUK MENDUKUNG *CHAIN OF CUSTODY* BUKTI DIGITAL

Devi Ratnasari

15917206

Yogyakarta, Februari 2018

Tim Penguji,

Dr. Bambang Sugiantoro
Ketua

Dr. Imam Riadi, M.Kom
Anggota I

Yudi Prayudi, S.Si., M.Kom
Anggota II

Mengetahui,
Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST., M.Sc

Abstrak

MEMBANGUN MODEL INFORMASI METADATA UNTUK MENDUKUNG *CHAIN OF CUSTODY* BUKTI DIGITAL

Tren kejahatan siber yang melibatkan internet, komputer atau ponsel sebagai media atau target kejahatan terus mengalami peningkatan. Selama proses investigasi, barang bukti untuk kasus siber dibagi menjadi dua jenis yaitu barang bukti fisik (elektronik) dan barang bukti digital. Agar dapat digunakan dalam proses penegakan hukum, barang bukti harus terjaga dan sama persis seperti ketika pertama kali ditemukan. Salah satu pembuktian ilmiah yang dapat digunakan adalah memastikan informasi kronologis barang bukti dalam dokumen *chain of custody*. Selama ini belum terdapat standar/regulasi yang menjadi acuan utama bagi organisasi/instansi penegak hukum dalam melakukan aktivitas dan menentukan kebutuhan informasi *chain of custody* untuk barang bukti digital. Hal ini menyebabkan organisasi/instansi penegak hukum memiliki mekanisme, sarana dan informasi dokumentasi yang berbeda-beda. Saat ini praktek dokumentasi *chain of custody* untuk barang bukti (fisik) yang banyak diterapkan adalah berbasis kertas menggunakan formulir atau buku. Karena barang bukti fisik dan bukti digital memiliki karakteristik yang berbeda, konsep tersebut akan sangat mungkin menimbulkan masalah apabila diterapkan pada bukti digital.

Mengingat pentingnya solusi *chain of custody* untuk bukti digital dalam proses investigasi *cyber crime*, penelitian ini mengidentifikasi dan memodelkan kebutuhan informasi serta memberikan sebuah solusi dokumentasi bukti digital secara teknis menggunakan pendekatan XML metadata. Untuk mengidentifikasi dan memodelkan informasi, pendekatan normalisasi diterapkan terhadap beberapa formulir *chain of custody* untuk kejahatan siber atau kejahatan komputer. Sedangkan implementasi model informasi adalah dengan menerjemahkan model informasi ke dalam skema XML metadata menggunakan sebuah aplikasi yang diberi nama aplikasi *Digital Chain Of Custody*.

Dari aktivitas yang telah dilakukan, penelitian ini menghasilkan 9 kelompok informasi dan 42 *field* informasi yang dibutuhkan untuk metadata dokumentasi *chain of custody* bukti digital. Informasi metadata tersebut dibagi menjadi informasi metadata statis dan metadata dinamis yang disimpan di dalam metadata eksternal menggunakan skema *file* XML. Konsep tersebut menyimpan *file* bukti digital dan *file* dokumentasi secara terpisah. Sedangkan untuk model informasi metadata diterapkan layaknya formulir *chain of custody* dalam format digital menggunakan bantuan aplikasi. Untuk mengetahui kualitas hasil penelitian, pengujian dilakukan menggunakan dokumen SNI ISO/IEC 27037, kuesioner dan implementasi aplikasi terhadap beberapa *file* digital. Berdasarkan analisis dan pengujian menunjukkan bahwa informasi yang berhasil diidentifikasi sudah mencakup kebutuhan informasi untuk manajemen *chain of custody* sesuai dalam dokumen SNI ISO/IEC 27037, sebanyak 88% responden kuesioner memberikan nilai positif (setuju/sangat setuju) apabila informasi di dalam formulir sudah cukup baik dan lengkap serta dapat diterapkan untuk mendokumentsaikan *chain of custody* untuk bukti digital dan berdasarkan implementasi aplikasi yang dilakukan menunjukkan bahwa konsep metadata eksternal menggunakan skema XML tidak merubah integritas (nilai *hash*) *file* bukti digital.

Kata kunci

Forensika Digital, Bukti Digital, *Chain Of Custody* Bukti Digital, Model Informasi, Metadata, Skema XML

Abstract

DEVELOPING METADATA INFORMATION MODEL FOR SUPPORTING CHAIN OF CUSTODY OF DIGITAL EVIDENCE

Cyber crime trends involving the internet, computers or mobile phones as media or crime targets continue to increase. During the investigation process, evidence for cyber cases is divided into two types: physical evidence (electronic) and digital evidence. In order to be used in the law enforcement process, evidence must be maintained and exactly as it was when it was first discovered. One scientific proof that can be used is ensuring chronological information of evidence in the document chain of custody. So far there is no standard/regulation that becomes the main reference for organizations/law enforcement agencies in conducting activities and determining the needs of chain of custody information for digital evidence. This causes law enforcement organizations/agencies to have different mechanisms, facilities and information documentation. Currently the practice of chain of custody documentation for evidence (physical) that is widely applied is paper-based using forms or books. Because physical evidence and digital evidence have different characteristics, the concept will most likely cause problems when applied to digital evidence.

Given the importance of the chain of custody solution for digital evidence in the cyber crime investigation process, this study identifies and models information requirements and provides a technically digital evidence documentation solution using XML metadata approach. To identify and model information, the normalization approach is applied to some chain of custody form for cyber crime or computer crime. While the implementation of the information model is by translating it into the metadata XML schema using an application named Digital Chain Of Custody application.

From the activity that has been done, this study produces 9 groups of information and 42 field information needed for metadata documentation of chain of custody digital evidence. The metadata information is divided into static metadata and dynamic metadata information which stored in external metadata using XML file schema. The concept keeps the digital evidence files and documentation files separately. The metadata information model applied as a form of chain of custody in digital format using the help of the application. To know the quality of study results, the test is done using the SNI ISO / IEC 27037 document, questionnaire and application implementation to some digital files. Based on the analysis and testing indicate that the information that has been identified already includes information needs for chain of custody management as stated in SNI ISO / IEC 27037 document, 88% of questionnaire respondent give positive value (agree / strongly agree) if the information in the form is good and complete enough and also applicable to document chain of custody for digital evidence. And based on the implementation of the application shows that the concept of external metadata using XML schema does not change the integrity (hash value) of digital evidence files.

Keywords

Digital Forensic, Digital Evidence, Digital Chain Of Custody, Information Model, Metadata, XML Schema

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, 2018

Devi Ratnasari

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Ratnasari, D., Prayudi, Y., & Sugiantoro, B. (2018). XML Approach for the Solution of Chain of Custody of Digital Evidence. International Journal of Computer Applications, 179(23), 20-25.

Kontributor	Jenis Kontribusi
Devi Ratnasari	Mendesain eksperimen (60%) Menulis *paper* (70%)
Yudi Prayudi, S.Si., M.Kom	Mendesain konsep dan eksperimen (40%) Menulis dan mengedit *paper* (30%)
Dr. Bambang Sugiantoro	Melakukan evaluasi dan analisis

Halaman Kontribusi

Tidak ada kontribusi dari pihak lain.

Halaman Persembahan

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

"Dengan rahmat Allah yang Maha Pengasih lagi Maha Penyayang,"

Bapak Juminto, Ibu'e Karmiyem,
Mas Erwan & Dhek Bayu

... You're my All, my rhythm and my muse ...

كرابت نمحر لا

Sebuah persembahan untuk keluarga tercinta, sebagai
bukti kesungguhan penulis dalam menimba ilmu,
sekaligus motivasi bagi para penerus.

Kata Pengantar

Puji syukur kehadirat Allah swt., atas rahmat serta karunia-Nya, sehiangga Tesis ini berhasil diselesaikan tepat pada waktunya. Shalawat dan Salam kepada Baginda Rasulullah Muhammad saw., yang membawa cahaya Iman dan Islam. Terima kasih penulis ucapkan kepada berbagai pihak :

1. Rektor Universitas Islam Indonesia, Bapak Nandang Sutrisno, SH., M.Hum., LLM., Ph.D yang memberikan kesempatan kepada penulis untuk menimba ilmu di Universitas Islam Indonesia.
2. Dekan Fakultas Teknologi Indudtri Universitas Islam Indonesia, Bapak Dr. Imam Djati Widodo, M.EngSc yang memberikan fasilitas dan bantuan untuk belajar.
3. Ketua Program Pascasarjana Magister Teknologi Industri Universitas Islam Indonesia, Bapak Dr. R. Teduh Dirgahayu, ST., M.Sc dengan segala kebijaksanannya.
4. Dosen Pembimbing Tesis, Bapak Yudi Prayudi, S.Si., M.Kom, Bapak Dr. Bambang Sugiantoro dan Bapak Dr. Imam Riadi, M.Kom atas segala bimbingan, arahan, motivasi, ilmu dan kebaikannya.
5. Seluruh keluarga baik ayah, Ibu, kakak dan adik yang telah mencurahkan segenap cinta, kasih sayang, perhatian dan dukungan baik moril maupun materil.
6. One Ok Rock dan My First Story, terimakasih untuk musik yang selalu ada, menemani dan menyemangati penulis.
7. Semua pihak, baik individu maupun kelompok yang ikut serta menorehkan warna dalam kanvas kehidupan penulis.

Kritik dan saran dari semua pihak yang bersifat membangun selalu penulis harapkan. Akhir kata, penulis sampaikan terima kasih kepada semua pihak yang telah berperan serta dalam penyusunan Tesis ini dari awal sampai akhir.

Yogyakarta, Februari 2018

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

Glosarium

COC	- *Chain Of Custody*
DCOC	- Digital *Chain Of Custody*
PPBB	- Petugas Pengelola Barang Bukti
XML	- Extensible Markup Language

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era sekarang, penggunaan internet dan data ditigal telah meluas termasuk di dalam dunia bisnis, pendidikan, kesehatan, pemerintah bahkan sosial masyarakat. Lebih dari dua pertiga populasi di dunia memiliki ponsel dan bahkan lebih dari setengah populasi di dunia saat ini juga dapat mengakses internet serta menggunakan komputer dan *smartphone* dalam kehidupan sehari-hari (Kemp, 2017). Hal tersebut menimbulkan sebuah tren kejahatan baru yang melibatkan internet dan komputer atau *smartphone* baik sebagai media maupun sebagai sasaran dari tindak kejahatan yang dikenal dengan istilah *cyber crime*.

Barang bukti untuk proses investigasi *cyber crime* dibagi menjadi dua jenis yaitu barang bukti fisik (elektronik) dan barang bukti digital. Barang bukti fisik (elektronik) adalah semua perangkat elektronik yang dapat digunakan untuk kepentingan aktivitas *cyber crime* atau perangkat lain yang dapat merekam jejak dari kegiatan *cyber crime* tersebut, misalnya *harddisk*, CD, *pendrive*, cctv, komputer, RAM, *handphone* dll. Sedangkan barang bukti digital ialah konten digital hasil akuisisi dan ekstraksi dari barang bukti fisik (elektronik). Bukti digital juga dapat berupa *file* bukti digital hasil ekstraksi (*full copy*) bit per bit dari media penyimpanan yaitu *hard drives, flash drives, floppy disk* dan *optical media* yang dikenal dengan istilah *Disk Image* (Carrier, 2005) (Prayudi, 2014).

Barang bukti agar dapat digunakan di dalam proses penegakan hukum adalah harus terjaga dan sama persis dengan ketika pada saat pertama kali ditemukan. Dalam dunia forensika digital, salah satu pembuktian secara ilmiah adalah dengan tahap dokumentasi (*documentation*) bukti digital. Cosic, (2017) juga mengungkapkan bahwa agar bukti digital dapat diterima di pengadilan, *chain of custody* (dokumentasi barang bukti) dan aspek informasi dari *chain of custody* menjadi domain penting yang harus diperhatikan.

Peraturan Kepala Kepolisian Republik Indonesia (Perkap) No. 10 Tahun 2009 Paragraf 3 telah mengatur segala hal yang berkaitan dengan barang bukti elektronik dan barang bukti digital di Indonesia. Paragraf tersebut berisi informasi tentang pemeriksaan barang bukti elektronik, telekomunikasi, komputer (Bukti Digital) dan penyebab proses elektrostatis. Paragraf tersebut juga mengatur bahwa dalam tata cara pemeriksaan barang bukti, setelah barang bukti diperoleh, barang bukti kemudian dibungkus, diikat, disegel, diberi label dan dilakukan dokumentasi untuk kepentingan pengelolaan dan audit barang

bukti. Sedangkan peraturan yang menjelaskan tentang tata cara pengelolaan barang bukti tertuang pada Perkap (Peraturan Kepala Kepolisian Indonesia) No. 10 Tahun 2010.

Chain of custody merupakan salah satu tahapan penting dari serangkaian proses investigasi terkait dengan dokumentasi barang bukti. Berdasarkan Ashcr*o*ft, Daniels, & Hart, (2004) dalam laporan *National Institute of Justice* dokumen formulir *chain of custody* berisi *history* atau kronologi perjalanan barang bukti yang memuat informasi lengkap seperti subyek/obyek yang terlibat dalam aktivitas pengumpulan dan analisis, tanggal/waktu serta tempat pengumpulan dan analisis, nama lengkap dan nama panggilan korban maupun pelaku, nama agensi serta deskripsi lengkap barang bukti.

Life cycle dan rantai perjalanan bukti digital merupakan bagian yang sangat penting dalam proses investigasi,. Seorang investigator dan saksi ahli harus mengetahui secara detail bagaimana barang bukti telah ditangani (Cosic & Baca, 2010b). Terdapat banyak faktor yang dapat mempengaruhi dan mengganggu nilai dari barang bukti pada setiap tahap *life cycle*. Faktor tersebut diantaranya faktor alam, teknik maupun adanya interaksi manusia dengan barang bukti. *Chain of custody* seharusnya dapat membuktikan bahwa barang bukti digital tidak mengalami perubahan di seluruh fase *life cycle* (*Creation, Acquisition, Identification, Storage, Preservation* dan *Access*). Untuk membuktikan proses *chain of custody*, dokumentasi informasi mengenai 5W+1H harus diterapkan pada barang bukti (Cosic & Cosic, 2012). Namun pada saat ini, informasi untuk kepentingan *chain of custody* yang terkandung pada bukti digital di dalam metadata masih belum memunculkan informasi terkait *life cycle* bukti digital.

Dokumentasi *chain of custody* untuk barang bukti fisik dan barang bukti digital seharusnya memiliki konsep dan informasi yang sama. Sedangkan pada prakteknya, mekanisme dokumentasi *chain of custody* untuk barang bukti digital berbeda dengan barang bukti fisik karena adanya perbedaan karakteristik (Luthfi & Prayudi, 2015). Praktek dokumentasi *chain of custody* untuk barang bukti fisik pada Perkap (Peraturan Kepala Kepolisian Indonesia) No 10 Tahun 2010 selama ini dilakukan dengan menggunakan berita acara, buku kontrol dan buku register. Selanjutnya untuk melakukan dokumentasi barang bukti digital, salah satu konsep yang dapat digunakan untuk mendukung dokumentasi *chain of custody* bukti digital adalah menggunakan konsep metadata (Prayudi, Ashari, & Priyambodo, 2014).

Metadata kini menjadi kebutuhan dasar bagi pelaku bisnis di perusahaan maupun organisasi terutama pada era budaya berbasis data (*Data-driven culture*). Untuk memiliki budaya berbasis data, organisasi dan perusahaan memerlukan mekanisme strategi data.

Strategi data diperlukan agar sebuah data dapat disajikan dan digunakan dengan kualitas yang lebih baik. Dan dalam strategi data pada tahun 2017, poin penting yang seharusnya menjadi perhatian adalah terkait dengan metadata (Zaino, 2016). Metadata yang merupakan data di dalam data dan melekat pada sebuah *file* digital dapat digunakan sebagai media untuk mendeskripsikan seluruh kebutuhan informasi terkait dokumentasi *chain of custody*. Namun hingga saat ini belum ada mekanisme dan sarana untuk mengimplementasikan kebutuhan informasi untuk metadata yang mendukung kebutuhan *chain of custody* untuk bukti digital.

Beberapa penelitian tentang metadata terkait perancangan model metadata telah dilakukan pada bidang manufaktur oleh Yang, Qiao, Cai, Zhu, & Wulan, (2017), bidang pendidikan oleh Liu & Qin, (2014), bidang pemrograman oleh Shah & Ibrahim, (2014), bidang transportasi oleh Ge & Rao, (2015) bidang informasi oleh Zheng, (2015) dan Xiankun, Lei, & Shan, (2010), iklim oleh Dunlap, Mark, & Rugaber, (2008) dan penelitian terkait lainnya. Akan tetapi, dalam hal ini penelitian untuk menghasilkan model metadata untuk kepentingan *chain of custody* barang bukti digital masih belum menjadi bahan kajian para peneliti.

Mengingat pentingnya solusi digital *chain of custody* dalam proses investigasi *cyber crime* maka solusi tentang metadata *chain of custody* sangatlah diperlukan. Oleh karena itu perlu adanya penelitian terkait dengan dokumentasi *chain of custody* sebagai solusi untuk kepentingan tersebut. Solusi yang ditawarkan adalah penggunaan konsep metadata sebagai media penyimpanan informasi *chain of custody* sesuai dengan alur perjalanan atau *life-cycle* barang bukti. Model metadata nantinya akan diimplementasikan menggunkan skema XML (*Extensible Mark-up Language*) karena sifatnya yang *flexible* dan *extendsible*. Konsep metadata yang akan dibuat akan tetap menjaga integritas nilai hash *file* barang bukti sehingga barang bukti dapat didokumentasikan dengan baik dan dapat diterima di persidangan.

1.2 Permasalahan

Di Indonesia, institusi yang berwenang untuk melakukan pengelolaan barang bukti adalah RUPBASAN (Rumah Penyimpanan Benda Sitaan Negara). Pengelolaan barang bukti meliputi barang bukti yang berwujud (fisik) maupun barang bukti tidak berwujud (digital). Sesuai Perkap (Peraturan Kepala Kepolisian Indonesia) No 10 tahun 2010 BAB V menjelaskan bahwa prosedur pengelolaan barang bukti terdiri dari penerimaan dan penyimpanan, pengamanan dan perawatan serta pengeluaran dan pemusnahan barang bukti. Pada tiap-tiap prosedur yang dikenakan pada barang bukti dilakukan dokumentasi atau

pencatatan administrasi. Pada BAB VIII tentang administrasi dan pelaporan, praktek administrasi pengelolaan barang bukti dituangkan dalam bentuk berita acara, buku kontrol dan buku register.

Dokumentasi *chain of custody* selama ini banyak diterapkan untuk barang bukti fisik. Sementara untuk barang bukti digital terdapat sejumlah solusi yang diberikan oleh peneliti lainnya seperti model bisnis penanganan bukti digital oleh Luthfi & Prayudi, (2015), pembuatan framework *chain of custody* bukti digital dengan konsep *digital cabinet* oleh Prayudi, Ashari, et al., (2014), framework *chain of custody* proses investigasi bukti digital oleh Ćosić, (2010) penjabaran kebutuhan informasi manajemen *chain of custody* menggunakan pendekatan ontology oleh Prayudi, Luthfi, et al, (2014) dan Cosic, Cosic, & Baca, (2011) dan lain-lain. Namun solusi tersebut masih belum sesuai dengan kebutuhan *chain of custody* untuk barang bukti digital. Pendekatan metadata ada sebagai salah satu solusi yang akan diusulkan untuk memperkaya solusi *digital chain of custody* yang sudah ada. Pendekatan metadata akan menghasilkan model metadata yang cocok untuk kepentingan *digital chain of custody*.

1.3 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah yang akan dibahas adalah :

1. Apa saja kebutuhan informasi dalam manajemen *chain of custody* untuk bukti digital?
2. Bagaiamana model informasi dalam metadata yang dapat digunakan serta mudah dipahami untuk mendukung konsep *chain of custody* bukti digital?
3. Bagaimana bentuk implementasi model metadata agar tidak merubah nilai integritas bukti digital sehingga dapat digunakan untuk mendukung konsep *chain of custody* bukti digital?

1.4 Batasan Masalah

Agar permasalahan tidak terlalu luas, maka penelitian ini dibatasi pada beberapa topik permasalahan diantaranya :

1. Penelitian ini adalah membuat model informasi untuk metadata *chain of custody* untuk bukti digital

2. *File* bukti digital yang digunakan di dalam pengujian model informasi metadata *chain of custody* adalah *file* bukti digital hasil dari proses akuisisi program perangkat lunak EnCase dan *file* raw image.
3. Aplikasi yang dibuat sebagai media implementasi dan pengujian terbatas pada implementasi model informasi metadata seperti membuat metadata baru, menyimpan metadata, melakukan edit metadata dan menampilkan informasi metadata *chain of custody*.

1.5 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut :

1. Mengidentifikasi kebutuhan informasi di dalam manajemen *chain of custody* untuk bukti digital.
2. Memodelkan dan mendeskripsikan informasi metadata sehingga dapat digunakan untuk mendukung konsep *chain of custody* bukti digital.
3. Mengetahui bentuk implementasi model informasi metadata yang dapat digunakan untuk mendukung konsep *chain of custody* untuk bukti digital.

1.6 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut :

1. Mampu memberikan ilmu pengetahuan tentang informasi penting terkait manajemen *chain of custody* untuk bukti digital menggunakan konsep metadata.
2. Mampu memberikan salah satu solusi implementasi manajemen *chain of custody* untuk bukti digital menggunakan konsep metadata.
3. Mampu memberikan informasi kebutuhan informasi dan model informasi untuk metadata di dalam manajemen *chain of custody* untuk bukti digital.

1.7 Metode Penelitian

Langkah-langkah yang akan ditempuh selama melakukan penelitian ini adalah sebagai berikut :

1. Studi Pustaka

   Penelitian ini melakukan studi pustaka dengan cara mengumpulkan referensi yang relevan dengan objek penelitian melalui buku, makalah, literatur maupun jurnal ilmiah yang membahas mengenai manajemen bukti digital, formulir *chain of custody* barang

bukti, *chain of custody* bukti digital, model metadata, bahasa pemrograman java dan xml serta referensi pustaka lainya.

2. Analisis Kebutuhan Metadata *Chain of Custody*

   Melakukan analisis terhadap berbagai sumber pustaka terkait dengan model metadata, proses dokumentasi pengelolaan barang bukti digital dan melakukan identifikasi kebutuhan informasi untuk merancang model informasi metadata yang dapat digunakan untuk mendukung konsep *chain of custody* bukti digital.

3. Perancangan Model Metadata

   Merupakan aktivitas untuk menentukan *field* informasi yang dibutuhkan dalam manajemen *chain of custody* untuk bukti digital serta menggambarkan pola keterkaitan atau relasi dari masing-masing *field* informasi ke dalam sebuah rancangan model informasi metadata *chain of custody* bukti digital.

4. Implementasi model metadata

   Implementasi pada penelitian ini adalah menerjemahkan model informasi metadata ke dalam skema XML dan membuat program aplikasi DCOC (*Digital Chain of Custody*) untuk menerapkan model informasi metadata. Implementasi program adalah berupa aplikasi desktop yaitu dengan menggunakan bahasa pemrograman Java.

5. Pengujian Model Metadata

   Pengujian model metadata adalah menggunakan pendekatan pengujian secara konseptual dan fungsional. Model metadata akan diuji kualitasnya secara konseptual berdasarkan aspek-aspek dokumentasi. Sedangkan pengujian secara fungsional ialah dengan melakukan percobaan dokumentasi pengelolaan bukti digital menggunakan program aplikasi DCOC (*Digital Chain of Custody*). Dokumentasi *chain of custody* barang bukti digital dilakukan dengan menggunakan skema *entry* dan *update* metadata dalam sebuah skema kasus yang ditangani oleh penegak hukum.

1.8 Struktur Penulisan

Tahapan yang menjelaskan secara umum terkait sistematika penulisan yang berisi penjelasan secara ringkas terhadap kerangka penulisan yang digunakan.

BAB I : PENDAHULUAN

Tahap awal dari penelitian berisi penjelasan terkait dengan latar belakang penelitian, penetapan judul, rumusan masalah, tujuan penelitian, manfaat penelitian, metode serta struktur penulisan yang digunakan. Dalam bagian ini juga dijelaskan mengenai temuan paling relevan dengan penelitian sebelumnya dan kontribusi ilmiah yang diharapkan.

BAB II : KAJIAN PUSTAKA

Tahap ini menjelaskan tentang kajian atas pustaka yang relevan dengan penelitian dan rumusan masalah berupa manajemen dokumentasi bukti digital, *chain of custody* bukti digital, model metadata untuk menentukan rancangan metadata bukti digital serta bahasa pemrograman Java dan XML untuk mendukung penerapan konsep metadata sebagai *chain of custody* bukti digital.

BAB III : METODOLOGI PENELITIAN

Menguraikan metode penelitian yang digunakan untuk memperoleh data dan informasi sesuai dengan topik penelitian. Pada penelitian ini, metodologi yang diguanakan adalah berbasis penelitian desain (*design research*).

BAB IV : ANALISIS DAN PERANCANGAN

Menjelaskan kebutuhan informasi metadata, analisis dan perancangan model informasi metadata yang digunakan serta aplikasi/sistem yang dibangun sebagai wujud implementasi model metadata.

BAB V : IMPLEMENTASI DAN PEMBAHASAN

Menjelaskan penerapan atau implementasi dari rancangan model metadata dan aplikasi yang telah dibuat. Memaparkan hasil analsis dan pembahasan terkait model informasi metadata yang digunakan dan aplikasi/sistem dokumentasi *chain of custody* terhadap proses manajemen bukti digital.

BAB VI : PENUTUP

Berisi simpulan dari hasil penelitian disertai dengan beberapa saran

DAFTAR PUSTAKA

BAB II
KAJIAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian terkait dengan pemodelan metadata telah dilakukan terhadap beberapa objek oleh peneliti. Pada sub-bab ini diberikan kajian terkait penelitian dibidang pemodelan metadata. Kajian dilakukan untuk memetakan penelitian antara penelitian sebelumnya dan penelitian terbaru.

Penelitian pendekatan pemodelan informasi metadata terhadap informasi proses manufaktur / MPIMM (*A Manufacturing Process Information Metamodel*) dilakukan oleh Yang et al. (2017). Menurutnya integrasi informasi dan interoperabilitas diantara perbedaan desain dan sistem manufaktur sangat penting dalam mendukung implementasi *smart manufacturing* dan manajemen *life-cycle* produk. Pada penelitian ini pemodelan informasi dibuat menggunakan *unified Modeling Language* (UML) yang mencakup *object classes, relationship classess* dan menentukan informasi dan relasi antar proses, operasi, sumber daya yang digunakan dan produk/bagian produk hasil manufaktur serta hasil proses perencanaan manufaktur.

Penelitian pemodelan informasi metadata terhadap *scholar output* seperti riset publikasi dilakukan oleh Liu & Qin, (2014). Penelitian ini membuat model metadata *scientific* yang meliputi informasi deskriptif dalam elemen metadata klasik yaitu *Dublin Core* dan inovasi elemen struktural, deskriptif dan referensial (SDR) dimana pemodelan informasi metadata dibuat menggunakan *Ontology Web Language* (OWL). Selain itu eksperimen dilakukan menggunakan platform wiki yang mengijinkan *user* untuk menambah, mengedit dan menghapus informasi metadata.

Untuk mendukung adanya integrasi berbagai sistem manajemen informasi, penelitian pemodelan metadata terhadap sistem manajemen informasi pada institusi dilakukan oleh Zheng, (2015). Pada penelitian ini, peneliti menawarkan solusi dengan membuat model teknikal metadata dan model bisnis metadata. Untuk mendeskripsikan konten dan detail informasi, pemodelan metadata dilakukan dengan menggunakan skema XML.

Shah & Ibrahim, (2014) melakukan penelitian pemodelan informasi metadata terhadap aplikasi android meliputi *activity, service* dan *content provider*. Pemodelan kebutuhan informasi metadata untuk membantu pengembang dalam pemodelan aplikasi Android dibuat menggunakan *Unified Modeling Language* (UML).

Qin, Jin, Dobreski & Brown, (2016) melakukan penelitian pemodelan metadata untuk mendukung manajemen data dan keberlangsungan penelitian. Metadata pada penelitian tersebut digunakan untuk mendokumentasikan *lifecycle* penelitian dan hasil penelitian dengan studi kasus pada *Gravitational Wave (GW) research*. Untuk merancang model metadata yang sesuai, data diperoleh melalui wawancara terhadap para peneliti di GW dimana informasi metadata dan relasinya dideskripsikan dalam blok diagram.

Ge & Rao, (2015) melakukan penelitian pemodelan metadata untuk data transportasi dan logistik. Model metadata pada penelitian ini berupa *business metadata* menggunakan pendekatan *SDMX information model.* Model metadata kemudian diimplementasikan ke dalam skema XML menggunakan sebuah program aplikasi manajemen metadata untuk mengelola metadata teknikal dan bisnis.

Grube et al., (2011) melakukan penelitian pemodelan metadata untuk laboratorium online *the Lybrary of Labs* atau sering disebut LiLa. Lila adalah sebuah portal yang memberikan fasilitas bagi peneliti, pengajar dan siswa untuk saling bertukar konten seperti proyek, materi dan informasi. Metadata digunakan untuk menotasikan konten-konten yang ada pada portal LiLa. Pemodelan informasi metadata dibuat menggunkan struktur ontology dan dinormalisasi menggunakan skema RDF/XML.

Xiankun et al., (2010) melakukan penelitian pemodelan metadata untuk mendeskripsikan *Emergency Information Semantic Metadata* (EISMDM). Pada penelitian ini pemodelan informasi metadata dibuat berdasarkan deskripsi logis dengan pendekatan ontology. Pengujian dilakukan dengan melakukan implementasi pada aplikasi. Hasil dari beberapa percobaan mengindikasikan bahwa *emergency information* dapat diintegrasikan secara semantik menggunkan EISMDM berdasarkan mekanisme *query model* dan *semantic retrieval* yang diperoleh.

The Earth System Curator bersama *Earth System Grid Team* (ESG) mengembangkan pemodelan metadata untuk mendeskripsikan kebutuhan sumber data iklim untuk kepentingan *Curator metadata*. Metadata digunakan untuk menotasikan dataset yang tersimpan dalam portal. Model konseptual relasi dan kebutuhan informasi iklim pada penelitian ini dibuat dengan menggunakan *Unified Modeling Language* (UML) *Class Diagram* dan direpresentasikan menggunakan skema XML. Untuk melakukan validasi model metadata dan prototype portal, Curator bersama ESG melakukan perbandingan 13 inti dinamik atmosfer elemen kunci dari model iklim generasi selanjutnya pada sebuah NCAR *colloquium* serta melakukan 365 simulasi dan 593 *file* data (Dunlap et al., 2008). Penelitian-penelitian tersebut diringkas ke dalam Tabel 2.1.

Tabel 2. 1 Tinjauan Pustaka

Peneliti	Obyek	Model Metadata	Tools	Hasil Penelitian
Yang et al., (2017)	*Manufactur Process Information*	UML	Enterprise Architect (EA)	Metode pemodelan, model metadata dan framework pemodelan informasi proses manufaktur berdasarkan aturan pemodelan metadata yang telah dibuat.
Liu & Qin, (2014)	*Scholarly Output*	SDR (*Structural, Descriptive & Referential*), *Ontology web language format* (OWL)	Protege	Model metadata yang mengintegrasikan metadata struktural untuk level utama, deskriptif dan referensial untuk level publikasi. Prototype implementasi "*ScholarWiki"* berdasarkan model metadata SDR.
Zheng, (2015)	*Institutonal Information Management*	XML	-	Framewok integrasi data antar perangkat lunak menggunakan terminologi metadata
Shah & Ibrahim, (2014)	*Android*	UML	Stereotype	Diagram pemodelan UML untuk platform Android dan UML meta-model untuk mendeskripsikan pemodelan aplikasi android bagi *developer*
Qin, Jin, Dobreski & Brown, (2016)	*Gravitational Wave Research Data*	Block Diagram	-	Model metadata yang disesuaikan dengan kebutuhan *user* (*GW Scientists*). Model metadata masih dalam tahap pengembangan.
(Ge & Rao, 2015)	*Transportation & Logistic Data*	SDMX model, XML	-	Model *business metadata* untuk data transportasi dan logistik menggunakan XML
Xiankun et al., (2010)	*Emergency Information*	Ontology	-	Model semantik metadata *emergency informasi* (EISMDM).
Grube et al., (2011)	*Online Laboratories*	Ontology, RDF/XML	-	Model metadata notasi konten untuk *Online Laboratories* (portal LiLa). Metadata dimodelkan secara langsung menggunakan skema RDF/XML.

Tabel 2. 2 Tinjauan Pustaka Lanjutan

Peneliti	Obyek	Model Metadata	Tools	Hasil Penelitian
Dunlap et al., (2008)	*Climate*	UML, RDF, XML	-	Model kurator metadata untuk data iklim.
Penelitian yang akan dilakukan (Sekarang)	Bukti Digital	Normalisasi, XML	-	Model informasi metadata untuk *chain of custody* bukti digital

2.2 Landasan Teori

2.2.1 Barang Bukti Digital

Penelitian ini memiliki fokus pada perancangan model metadata *chain of custody*. Sedangkan objek utama dari penelitian ini adalah barang bukti digital.

a. Definisi dan Contoh Bukti Digital

Barang bukti pada kejahatan siber (*cyber crime*) dan kejahatan yang melibatkan perangkat elektronik umumnya berupa bukti-bukti digital. Bukti digital adalah obyek digital yang mengandung informasi handal dalam mendukung atau menolak terkait kasus kejahatan dalam proses investigasi (Carrier, 2005). Di Indonesia, pedoman hukum *cyber* yaitu Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) tidak mencantumkan istilah bukti digital. Akan tetapi di dalam UU ITE tersebut dikenal dua istilah alat bukti elektronik yaitu Informasi Elektronik dan dokumen Elektronik. Alat bukti elektronik ialah Informasi Elektronik dan Dokumen Elektronik yang memenuhi persyaratan formil dan materiil yang diatur di dalam Undang-Undang ITE. Sesuai Pasal 5 ayat (1) UU ITE menyatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetakannya merupakan alat bukti (*Digital Evidence*) hukum yang sah.

Sedangkan yang dimaksud dengan Informasi Elektronik dalam Pasal 1 ayat (1) UU ITE, bahwa Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data *interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Yang dimaksud dengan Dokumen Elektronik dalam Pasal 1 ayat (2) UU ITE adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Berikut beberapa contoh barang bukti digital yaitu: *Logical file, Deleted File, Lost File, File slack, Log File, Encrypted File,Steganography file, Office file, Audio File, video File, Image file, Email, User ID* dan *Password, Short Message Service (SMS), Multimedia Message Service (MMS), Call Logs*. Bukti digital juga adalah *file* bukti digital hasil ekstraksi

(*full copy*) bit per bit dari media penyimpanan yaitu *hard drives, flash drives, floppy disk* dan *optical media* yang dikenal dengan istilah *Disk Image*.

b. Karakteristik Bukti Digital

Menurut (Kuntze, Rudolph, Richter, Kuntze, & Rudolph, 2017) untuk dapat diterima di persidangan barang bukti digital harus memenuhi karakteristik bukti digital yaitu Admissible (layak), Authentic (Asli), Complete (Lengkap), Reliable (Dapat dipercaya) dan Believable (terpercaya).

- **Admissible**

  Barang bukri digital harus sesuai dengan fakta dan masalah yang terjadi dan dapat diterima serta digunakan secara hukum mulai dari proses penyidikan sampai ke pengadilan.

- **Authentic**

  Bahwa barang bukti harus mempunyai hubungan keterkaitan yang jelas secara hukum dengan kasus yang diselidiki dan barang bukti bukan hasil rekayasa. Barang bukti adalah masih asli dan tidak pernah diubah-ubah.

- **Complete**

  Barang bukti harus lengkap dan dapat membuktikkan tindakan jahat yang dilakukan pelaku kejahatan. Barang bukti yang dikumpulkan, tidak cukup hanya berdasarkan satu perspektif dari sebuah kejadian yang berlangsung.

- **Reliable**

  Barang bukti yang dikumpulkan harus dapat dipercayai. Pengumpulan barang bukti dan analisis yang dilakukan harus sesuai prosedur dan dilakukan dengan jujur. Selain itu barang bukti tidak boleh meragukan dan benar benar harus dapat dipercayai serta sesuai dengan prosedur yang SOP yang berlaku.

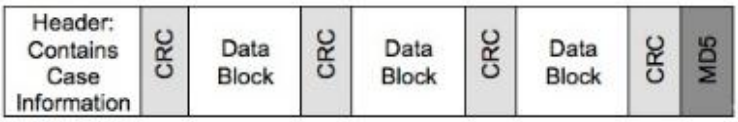
c. Format *File* Bukti Digital (EnCase)

Terdapat beberapa format *file* dalam literatur digital forensik diantaranya AFF, AFF4, *Expert Witness File Format, Logical Evidence File* dan SMART. Namun format *file disk image* yang paling banyak digunakan saat ini adalah format *file* bukti digital hasil akuisisi Encase (sering disebut sebagai *Expert Witness File Format*) dan format *file raw image* (Vandoven, 2014).

Encase /Encase Forensic Imager merupakan salah satu perangkat lunak forensika digital berbasis Windows yang digunakan untuk melakukan akuisisi, mendapatkan,

menerjemahkan, melakukan analisis dan membuat laporan terkait *file* bukti digital. Terdapat dua tipe *file* bukti digital pada Encase yaitu *Encase Evidence File* dan *Logical Evidence File*. Format *file Encase Evidence File* adalah .E01 atau .Ex01 merupakan representasi bit-per-bit dari perangkat fisik atau partisi harddisk. Sedangkan *Logical Evidence File* merupakan format *file* dari hasil akuisisi perangkat ponsel pintar. Tipe *file* untuk *logical File format* adalah .L01 atau .Lx01. (Software, 2013)

Format *file* E01 menyimpan metadata pada *header* dan *footer*. Metadata berisi tipe *drive*, versi EnCase yang digunakan untuk membuat *file image*, sistem operasi, *timestamps* dan nilai hash. selain itu *file* E01 juga memiliki cek nilai integritas *file* yang disebut sebagai *Cyclical Redundancy Check* (CRC) yang berada pada interval 64 KB seluruh *image file.* Nilai CRC digunakan untuk cek integritas pada setiap blok data seperti halnya nilai hash untuk cek integritas keseluruhan *image file*.



Gambar 2. 1 Format *File* Bukti Digital Encase

Gambar 2.1 menunjukkan *layout* atau struktur dari format *file* EnCase. Bagian header *file* berisi informasi metadata image. nilai kriptografi hash oleh Encase dihitung berdasarkan blok data, ditambahkan dan disimpan pada footer atau bagian paling akhir dari *file* (Vandoven, 2014).

2.2.2 *Chain of Custody*

Chain of custody adalah prosedur pencatatan / dokumentasi kronologis barang bukti sejak barang bukti ditemukan, proses duplikasi, penyimpanan barang bukti baik itu secara fisik ataupun digital hingga sampai pada presentasi dan keputusan akhir terhadap barang bukti. *Chain of custody* digunakan untuk memastikan integritas dan orisinalitas dari barang bukti (Prayudi & SN, 2015).

Dokumentasi *chain of custody* selama ini tidak memiliki standar yang baku. Sehingga setiap penegak hukum dapat memiliki form dokumentasi *chain of custody* yang berbeda-beda. Namun untuk dapat diterima di persidangan, sebuah form *chain of custody* setidaknya mencakup informasi "5W dan 1 H" untuk mencatat setiap proses investigasi diantaranya (Cosic, 2017):

a. Siapa yang terlibat dalam penanganan barang bukti

b. Kapan waktu setiap proses penanganan barang bukti dilakukan
c. Bagaimana proses penanganan yang dilakukan terhadap barang barang bukti
d. Kemana saja alur perjalanan proses penanganan barang bukti itu dibawa dan dimana disimpan
e. Mengapa pihak tersebut menanganinya
f. Apa saja barang bukti yang telah dikumpulkan

Dalam melakukan *chain of custody*, ada hal-hal yang harus diperhatikan diantaranya (Leintz, n.d.) :

a. *Security and Trust*

   Proses *chain of custody* seharusnya mampu menjamin keamanan dan tingkat kepercayaan di persidangan. Menciptakan dan memelihara *chain of custody* artinya menjaga *log* detail terkait dimana barang bukti ditemukan dan *log* seluruh aktivitas yang terjadi pada barang bukti.

b. *Documentation*

   Proses *chain of custody* dimulai di Tempat Kejadian Perkara (TKP) yaitu pada saat proses investigasi dan ketika barang bukti pertama kali diperoleh. Dokumentasi yang dilakukan di TKP umumnya dilakukan dengan menggunakan foto-foto TKP dan catatan investigasi awal sampai selesai kasus.

c. *Preventing Contamination*

   Merupakan aspek pencegahan barang bukti dari adanya kontaminasi, perubahan dan kerusakan selama proses penanganan. Hal ini berkaitan dengan nilai integritas dan keaslian dari barang bukti. Pihak-pihak yang berwenang dalam mengakses barang bukti, mendokumentasikan, dan menyerahkan merupakan pihak yang bertanggung jawab. Menurut (Cosic & Baca, 2010b) dalam dunia forensika digital, nilai integritas barang bukti digital adalah memastikan bahwa informasi yang terkandung dalam bukti yang dihadirkan lengkap dan tidak mengalami perubahan oleh pihak yang tidak memiliki wewenang otorisasi mulai pada saat diciptakan, penanganan hingga selesai persidangan. Salah satu metode yang dapat digunakan untuk memastikan integritas bukti digital adalah tidak berubahnya nilai fungsi MD5/hash barang bukti digital. MD5 merupakan fungsi hash yang paling umum digunakan dan merupakan pengembangan dari MD4. Fungsi MD5 memiliki panjang 128 bit. MD5 bekerja dengan membawa setiap pesan yang ada dan menghitung total bit yang terdapatpada pesan dan melakukan *message diggest*

dengan langkah penambahan *padding bit*, penambahan nilai panjang semula, inisialisasi buffer, pengolahan buffer dan pengolahan pesan dalam blok 512 bit .

2.2.3 Aspek Dalam *Chain of Custody*

Proses dokumentasi pengelolaan *chain of custody* barang bukti sangat dipengaruhi oleh beberapa aspek penting yang terlibat secara langsung dengan barang bukti. Beberapa aspek penting yang harus diperhatikan dalam melakukan dokumentasi *chain of custody* diantaranya;

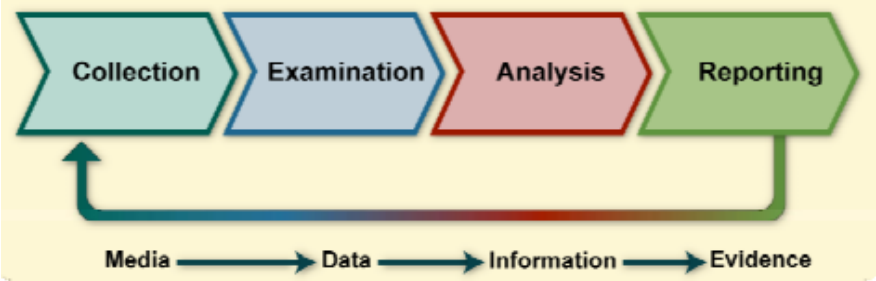
a. Aspek Personel

Dalam penanganan bukti digital, seluruh proses penanganan harus dilakukan oleh personel yang sah di mata hukum. Dengan kata lain, proses mendapatkan bukti digital, investigasi forensik, penuntutan dan pengadilan, manajemen dan dokumentasi. Berikut daftar personel yang dapat melakukan interaksi dengan barang bukti digital (Cosic & Baca, 2010b) :

- *First responder*
- Investigator forensik
- Saksi ahli persidangan
- Penegak hukum
- Petugas kepolisian
- Korban
- Tersangka
- Petugas terkait lainnya

b. Alur Proses Digital Forensik

Dalam *National Institute Standard and Technology* (NIST) oleh (Kent, Chevalier, Grance, & Dang, 2006) secara umum proses forensik dibagi ke dalam empat tahapan, yaitu *collection, examination, analysis* dan *reporting* seperti pada gambar 2.2.



Gambar 2. 2 Proses Digital Forensik

Tahap *Collection* (Pengumpulan Data) meliputi aktivitas identifikasi sumber data yang relevan terkait kasus, pelabelan dan pencatatan. Dalam tahapan ini seluruh prosedur yang dilakukan harus sesuai dengan pedoman dan Standar Operasional Prosedur yang berlaku untuk menjaga integritas barang bukti digital. Termasuk di dalam nya melakukan verifikasi integritas data (Nilai Hash, MD5 atau SHA-1) dari data asli dan hasil akuisisi.

Tahap *Examination* (Pemeriksaan) meliputi aktivitas penggunaan *tools* atau perangkat lunak dan teknik tertentu untuk melakukan identifikasi dan ekstraksi informasi yang relevan. Tahap pemeriksaan dapat menggunakan *tools* otomatis atau melalui proses manual.

Tahap *Analysis* (Analisis) merupakan aktifitas analisis terhadap hasil pemeriksaan untuk mendapatkan informasi yang berguna sehingga diperoleh kesimpulan.

Tahap *Reporting* (Pelaporan) merupakan aktivitas yang memuat tindakan, prsedur, alat yang digunakan dan memberikan rekomendasi perbaikan kebijakan dan petunjuk dalam aspek proses forensik.

c. Prosedur Pengelolaan Barang Bukti

Pengelolaan barang bukti adalah tata cara atau proses penerimaan, penyimpanan, pengamanan, perawatan, pengeluaran dan pemusnahan benda sitaan dari ruang atau tempat khusus penyimpanan barang bukti. Di Indonesia, pedoman dalam melakukan prosedur pengelolaan barang bukti diatur dalam Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 Tahun 2010 dan telah diperbaharui dalam Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 8 Tahun 2014. Terdapat poin yang dirubah, dihapus atau ditambahkan pada Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 8 Tahun 2014. Poin tersebut berkaitan dengan pengemban fungsi pengelolaan barang bukti di tingkat kepolisian pada pasal 9 yang semula bernama PPDB (Petugas Pengelola Barang Bukti). Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 8 Tahun 2014 pasal 9 ayat (1) menyatakan bahwa Pengelolaan barang bukti di lingkungan Polri dilaksanakan oleh Pengemban Fungsi Pengelolaan Barang bukti. Dan pada pasal 9 ayat (2) mengatur bahwa pengemban fungsi pengelolaan barang bukti pada tingkat Polri terdiri dari Bagian Tahanan dan Barang Bukti (Bagtahti) bareskrim Polri, Bagtahti Baharkam Polri, Subbagian Tahanan dan Barang Bukti (Sunnagtahti) Korlantas Polri dan Subbagtahti Densus 88 AT Polri, pada tingkat Polda adalah Direktorat Tahanan dan Barang Bulti (Dittahti) Polda, pada tingkat Polres adalah Satuan Tahanan dan Barang Bukti (Sattahti) Polres dan pada tingkat Polsek adalah Urusan Tahanan dan Barang Bukti (Urtahti) Polsek

Dokumen administrasi pengelolaan barang bukti terdapat pada Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 8 Tahun 2014 pasal 27. Dokumen tersebut terdiri dari :

- Berita acara.
- Surat tanda penerimaan barang bukti
- Surat penerimaan barang bukti
- Buku register daftar barang bukti
- Buku kontrol barang bukti
- Laporan bulanan, dan
- Laporan semester dan tahunan

Sedangkan aktivitas pengelolaan barang bukti tertuang dalam Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 Tahun 10 pasal 12 sampai pasal 21 sebagaimana dijabarkan di dalam Tabel 2.3.

Tabel 2. 3 Aktivitas Pengelolaan Barang Bukti Menurut Perkap No 10 Tahun 2010

Prosedur	Pasal	Aktivitas
Penerimaan dan Penyimpanan	12	- Meneliti Surat Perintah Penyitaan dan Berita Acara Penyerahan Barang bukti - Mengecek dan mencocokan jumlah dan jenis barang bukti yang diterima - Memeriksa dan meneliti jenis baik berdasarkan sifat, wujud, dan/atau kualitas barang bukti - Mencatat barang bukti yang diterima ke dalam buku register daftar barang bukti - Melakukan pemotretan terhadap barang bukti sebagai bahan dokumentasi - Men*core*t dari buku register, barang bukti yang sudah dimusnahkan atau yang sudah diserahkan ke JPU - Melaporkan tindakan yang telah dilakukan kepada penyidik dan Kasatker
	13 & 14	- Pemeriksaan dan penelitian barang bukti
Pengamanan dan Perawatan	15	- Melakukan pemeriksaan dan pengawasan berkala - Mengawasi jenis-jenis barang bukti tertentu yang berbahaya, berharga dan/atau memerlukan pengawetan - Menjaga dan mencegah agar barang bukti tidak terjadi pencurian, kebakaran ataupun kebanjiran - Mengarahkan dan mengatur pembagian tugas bawahannya - Mencatat dan melaporkan bila terjadi kerusakan dan penyusutan serta kebakaran dan pencurian terhadap barang bukti yang disimpan - Menindak PPBB yang lalai dalam melaksanakan tugas sesuai peraturan perundang-undangan
Pengeluaran dan Pemusnahan	17, 18, 19 dan 20	- Memeriksa dan meneliti surat permintaan pengeluaran barang bukti - Memeriksa dan meneliti surat perintah dan atau surat penetapan pengembalian barang bukti - Memeriksa dan meneliti surat perintah dan/atau penetapan penjualan lelang terhadap barang bukti - Membuat berita acara serah terima dan menyampaikan tembusannya kepada atasan penyidik - Mencatat lama peminjaman barang bukti dalam buku mutasi atau register yang tersedia - Menerima, memeriksa, meneliti dan menyimpan kembali barang bukti yang telah dipinjam - Mencatat dan men*core*t barang bukti tersebut yang telah dikembalikan, dilelang atau dimusnahkan dari daftar yang tersedia

2.2.4 Metadata

(NISO, 2004) Metadata sering disebut sebagai data atau informasi tentang data atau informasi. Metadata adalah informasi terstruktur yang mendeskripsikan, menjelaskan, menempatkan atau memberikan kemudahan untuk mengambil, menggunakan atau mengelola sumber informasi. Di dalam terminologi lingkungan perpustakaan, umumnya metadata digunakan untuk berbagai skema formal deskripsi sumber, diterapkan pada berbagai tipe obyek baik digital maupun non-digital. Terdapat tiga tipe metadata diantaranya :

a. *Descriptive Metadata*

menggambarkan sumber daya untuk tujuan seperti penemuan dan identifikasi. Mencakup unsur-unsur seperti judul, abstrak, penulis, dan kata kunci

b. *Structural Metadata*

Menunjukkan bagaimana kumpulan obyek disusun secara bersama-sama menjadi satu, semisal bagaimana halaman-halaman ditata untuk membentuk suatu bab.

c. *Administrative Metadata*

Menyediakan informasi untuk membantu mengelola suatu obyek, seperti kapan dan bagaimana obyek dibuat, tipe *file* dan informasi teknikal lainnya, serta siapa yang bisa mengaksesnya. Dan salah satu bagian dari *administrative metadata* adalah *preservation metadata* yang mendeskripsikan informasi yang dibutuhkan untuk keperluan arsip dan penyimpanan suatu obyek.

Secara teknis, implementasi metadata dapat menempel secara langsung pada obyek digital atau dapat disimpan secara terpisah. Metadata yang menempel umumnya disimpan dalam *file header* untuk memastikan bahwa metadata tidak akan hilang, *file* dan metadata terhubung serta *file* dan metadata diperbaharui secara bersamaan. Sedangkan metadata yang terpisah dengan obyek dapat menyederhanakan pengelolaan metadata dan mendukung fasilitas pencarian dan pengambilan informasi.

Skema metadata adalah set elemen metadata yang dirancang untuk tujuan tertentu, seperti mendeskripsikan jenis informasi tertentu pada sebuah obyek. Skema metadata dapat dibuat menggunakan SGML (*Standard Generalized Mark-up Language*) atau XML (*Extensible Mark-up Language*). Beberapa skema metadata yang telah dikembangkan diantaranya *Dublin Core, The Text Encoding Initiative* (TEI), *Metadata Encoding and Transmission Standard* (METS), *Metadata Object Description Schema* (MODS), *The Encoded Archival Description* (EAD), *Learning Object Metadata* dan lain-lain.

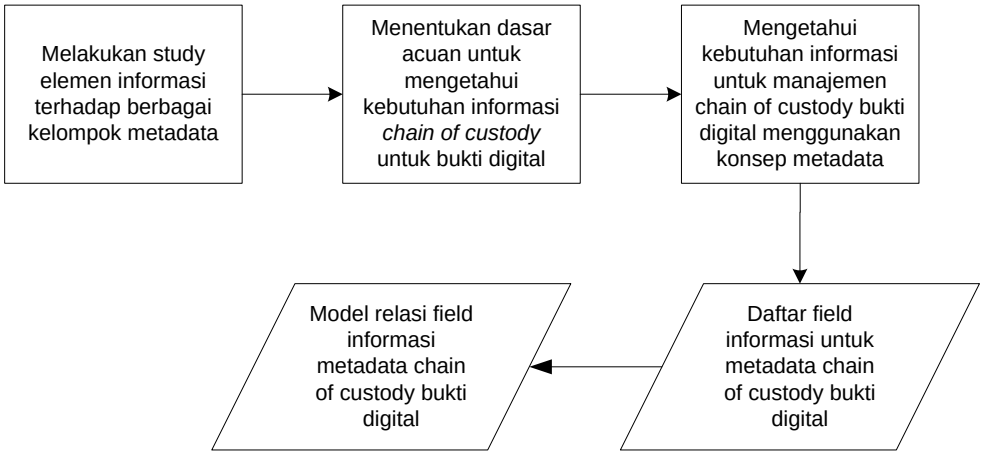
BAB III
METODOLOGI PENELITIAN

3.1 Studi Pustaka

Data yang digunakan pada penelitian ini diperoleh dari berbagai studi pustaka yang relevan terkait dengan bukti digital, manajemen *chain of custody* bukti digital, metadata, pemodelan metadata, bahasa pemrograman Java, skema XML dan referensi terkait lainnya.

3.2 Analisis Kebutuhan Metadata *Chain of Custody*

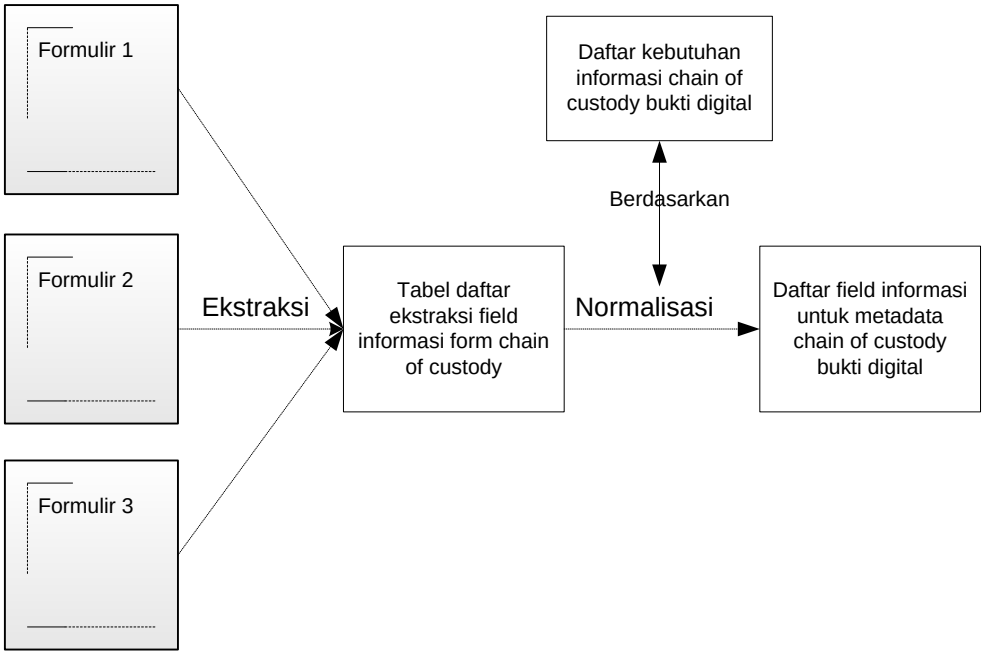
Penelitian ini akan melakukan pemodelan informasi metadata (*meta modeling*) untuk mendukung proses manajemen *chain of custody* bukti digital. Untuk dapat memodelkan informasi metadata, tahapan penting yang harus dilakukan adalah analisis kebutuhan informasi yang digunakan dalam dokumentasi *chain of custody* untuk bukti digital. Tahapan untuk melakukan analisis kebutuhan informasi metadata dapat ditunjukkan pada gambar 3.1.



Gambar 3. 1 Tahapan Analisis Kebutuhan Informasi Metadata

Tahap pertama dari penelitian ini adalah studi elemen informasi terhadap berbagai kelompok metadata. Studi dilakukan untuk mengetahui elemen informasi standar yang biasa ada di dalam sebuah metadata. Tahap kedua adalah menentukan dasar yang digunakan sebagai acuan untuk identifikasi kebutuhan informasi *chain of custody* untuk bukti digital. Tahap selanjutnya adalah identifikasi *field* informasi untuk manajemen *chain of custody* bukti digital berdasarkan acuan yang telah ditentukan. Dasar acuan dan daftar kebutuhan informasi untuk *chain of custody* bukti digital dapat diperoleh dari beberapa sumber diantaranya; referensi penelitian terdahulu dan standar operasional prosedur atau aturan resmi yang telah ada yang mengatur tentang mekanisme pelaksanaan *chain of custody*.

Dokumen tersebut seperti dalam NIST, NIJ, Perkap dan dokumen formulir *chain of custody*. Daftar kebutuhan informasi ini nantinya akan digunakan untuk membantu dalam identifikasi *field* informasi untuk metadata *chain of custody* bukti digital. Proses identifikasi kebutuhan *field* informasi *chain of custody* dapat ditunjukkan pada gambar 3.2.



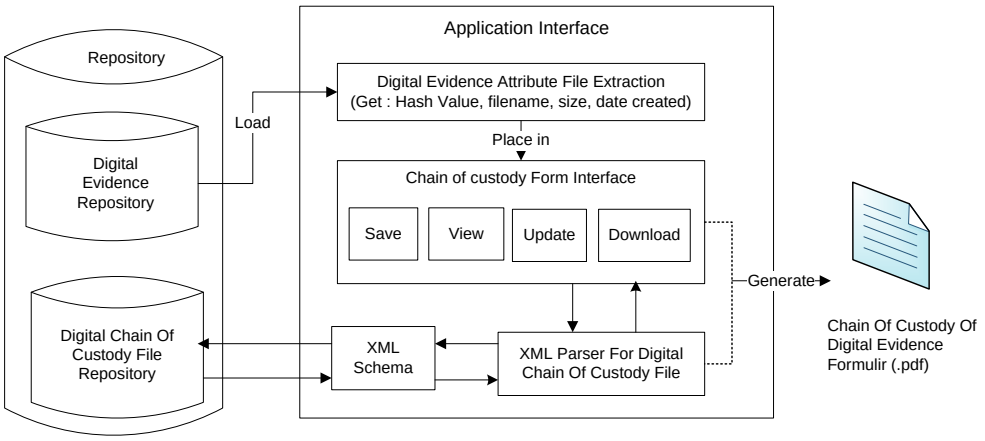
Gambar 3.2 Proses Identifikasi Kebutuhan *Field* Informasi

Proses identifikasi *field* infornasi dilakukan dengan ekstraksi terhadap formulir *chain of custody* yang memiliki keterkaitan dengan manajemen bukti digital. Selanjutnya *field* informasi yang diperoleh tersebut dilakukan normalisasi dan disesuaikan dengan kebutuhan informasi *chain of custody* yang telah dijabarkan pada tahap sebelumnya. Penelitian ini juga akan memodelkan relasi antar *field* informasi metadata *chain of custody* untuk mengetahui hubungan setiap *field* informasi terhadap kebutuhan informasi *chain of custody* dan bukti digital. *Output* atau hasil yang diharapkan dari serangkaiam tahap tersebut adalah berupa daftar *field* informasi beserta relasi yang dimiliki yang akan digunakan dalam konsep metadata *chain of cuatody* bukti digital.

3.3 Implementasi Model Metadata

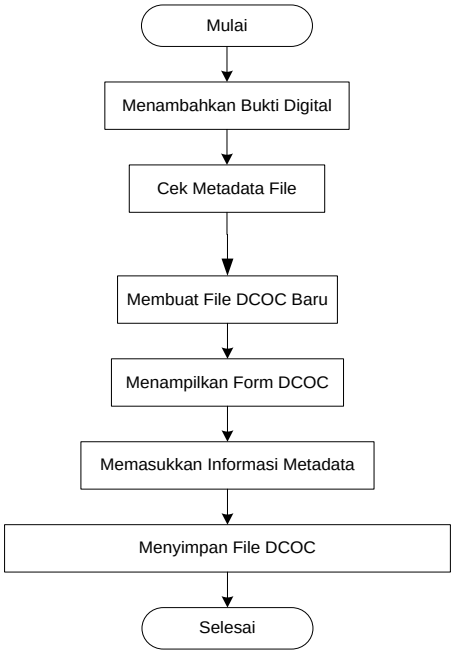
Implementasi model metadata pada penelitian ini adalah dengan menerjemahkan model metadata *chain of custody* bukti digital yang telah dibuat ke dalam skema XML (*Extensible Markup Language*). Selanjutnya, untuk melakukan penerapan skema XML (*Extensible Markup Language*) metadata *chain of custody* diperlukan sebuah program

aplikasi. Program aplikasi pada penelitian ini akan dibuat dalam lingkungan bahasa pemrograman JAVA yaitu menggunakan *tools* IDE Netbeans. Fungsi utama program aplikasi yaitu membaca informasi metadata *file* bukti digital, membuat *file* dokumentasi, memodifikasi informasi dokumentasi dan menyimpan *file* dokumentasi pada aplikasi. Hal tersebut seperti terlihat pada bagan rancangan aplikasi DCOC (*Digital Chain of Custody*) yang ditunjukkan pada gambar 3.3.



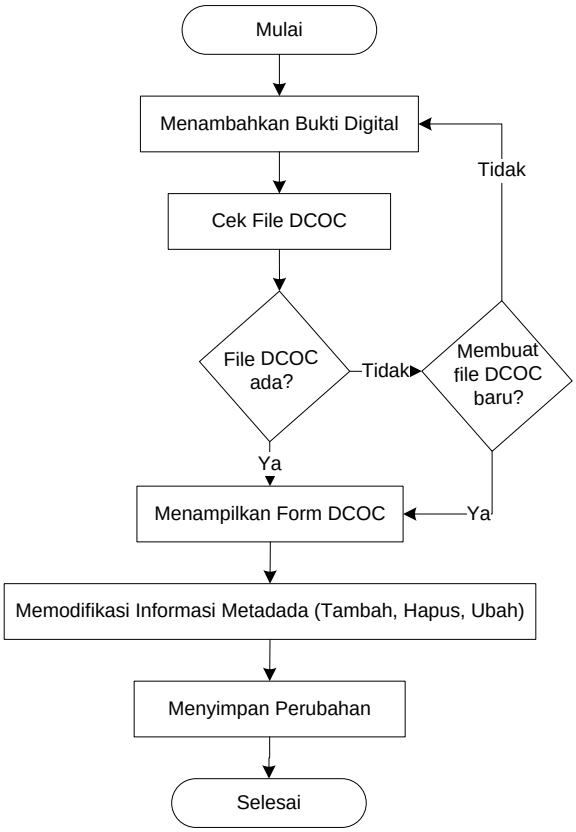
Gambar 3. 3 Bagan Rancangan Aplikasi DCOC (*Digital Chain of Custody*)

Untuk melakukan aktivitas membuat *file* dokumentasi *Chain of Custody* pada program aplikasi DCOC (*Digital Chain of Custody*) dapat dilakukan sesuai dengan alur yang ditunjukkan pada Gambar 3.4.



Gambar 3.4 Alur Aktivitas Membuat *File* Dokumentasi *Chain of Custody*

Sedangkan untuk melakukan aktivitas modifikasi (menambah, mengubah dan menghapus) informasi metadata *file* dokumentasi *Chain of Custody* pada program aplikasi DCOC (*Digital Chain of Custody*) dapat dilakukan sesuai dengan alur yang ditunjukkan pada gambar 3.5.



Gambar 3.5 Alur Aktivitas Modifikasi *File* Dokumentasi *Chain of Custody*

3.4 Pengujian Model Metadata

Untuk mengetahui apakah model metadata yang telah dibuat dapat digunakan untuk mendukung dokumentasi *chain of custody* bukti digital maka perlu dilakukan pengujian. Pengujian model informasi metadata dilakukan menggunakan dua jenis pengujian yaitu pengujian secara konseptual dan pengujian secara fungsional. Pengujian secara konseptual dilakukan untuk mengetahui kualitas dan kuantitas informasi dokumentasi *chain of custody*. Mekanisme yang digunakan dalam pengujian secara konseptual adalah dengan memetakan informasi terhadap kebutuhan informasi *chain of custody* dalam dokumen ISO/IEC 27037. Dokumen ISO/IEC 27037 sendiri merupakan dokumen standar nasional yang digunakan sebagai pedoman dalam melakukan identifikasi, pengumpulan, akuisisi dan preservasi bukti digital. Di dalam dokumen SNI ISO/IEC 27037 terdapat panduan standar minimum

informasi dalam melakukan dokumentasi *chain of custody* barang bukti diantaranya tentang identitas barang bukti, siapa yang mengakses, kapan dan dimana diambilnya barang bukti, mengapa barang bukti perlu diakses, informasi bukti yang dapat menunjukkan bahwa bukti tidak berubah/rusak, informasi *lifetime* dan pihak-pihak yang bertanggung jawab terhadap barang bukti.

Pengujian secara fungsional adalah dengan melakukan percobaan menggunakan program aplikasi dokumentasi DCOC (*Digital Chain of Custody*) yang telah dibuat. Pengujian secara fungsional ini bertujuan untuk mengetahui apakah model metadata yang dibuat dapat secara fungsional diterapkan. Pengujian akan menggunakan data berupa *file* digital dari beberapa sumber elektronik dan metode akuisisi. Setelah melakukan pengujian ini, diharapkan model metadata yang dibuat dalam format *file* .XML dapat digunakan untuk mengelola informasi dokumentasi bukti digital. Dokumentasi yang dilakukan menggunakan konsep metadata diharapkan tidak merubah nilai *hash file* bukti digital karena berkaitan dengan nilai integritas barang bukti. Aspek-aspek pengujian informasi dokumentasi *chain of custody* dapat ditunjukkan dalam Tabel 3.1 dan Tabel 3.2.

Tabel 3. 1 Pengujian Konseptual Model Informasi Metadata

No	Acuan ISO 27037:2014	Pemetaan Informasi	
		Statis	Dinamis
1	Penanda/pengenal yang bersifat unik dari barang bukti		
2	Siapa yang mendapatkan dan mengakses barang bukti, kapan waktu nya dan dimana lokasi nya		
3	Siapa yang memeriksa masuk dan keluar nya barang bukti dari fasilitas penyimpanan dan kapan aktivitas tersebut terjadi		
4	Mengapa barang bukti dikeluarkan dari fasilitas penyimpanan (kondisi dan tujuan) serta pihak yang memiliki hak/otoritas.		

Tabel 3. 2 Pengujian Konseptual Model Informasi Metadata Lanjutan

No	Acuan ISO 27037:2014	Pemetaan Informasi	
		Statis	Dinamis
5	Informasi yang dapat menunjukkan bahwa barang bukti telah atau tidak mengalami perubahan		
6	*Lifetime of the evidence*		
7	Pihak yang bertanggungjawab dalam menangani barang bukti digital		

Tabel 3. 3 Pengujian Fungsional Model Metadata

No	**Skenario Pengujian**	**Test Case**	**Hasil Yang diharapkan**	**Hasil**
1.	Membuat Metadata	a. ..... b. ..... c.	a. ..... b. ..... c.	Sesuai Harapan
2.	Mengubah Metadata	a. ..... b. ..... c.	a. ..... b. ..... c.	Sesuai Harapan
3.	Menampilkan Metadata	a. ..... b. ..... c.	a. ..... b. ..... c.	Sesuai Harapan

3.5 Perangkat Pendukung Penelitian

3.5.1 Perangkat Keras

Perangkat keras merupakan spesifikasi komputer yang digunakan dalam mendukung melakukan penelitian. Adapun perangkat keras yang digunakan adalah:

- Processor Intel *Core*(TM) i3-2370
- Memory (RAM) 4,00 GB
- Kapasitas Harddisk 320 GB

3.5.2 Perangkat Lunak

Perangkat lunak merupakan aplikasi komputer yang digunakan dalam mendukung penelitian. Adapun perangkat lunak yang digunakan adalah :

- Sistem Operasi : Micros*o*ft Windows 7 Ultimate
- Pengolah Kata : Micros*o*ft *Of*fice Word 2013
- Bahasa Pemrograman : Java Netbeans, XML
- Desain sistem : Micros*o*ft *Of*fice Visio

BAB IV
ANALISIS DAN PERANCANGAN

4.1 Analisis Kebutuhan Informasi Metadata *Chain of Custody*

Analisis kebutuhan informasi metadata *chain of custody* dilakukan dengan beberapa tahapan diantaranya; melakukan studi terkait standar informasi dalam metadata, menentukan dasar acuan *chain of custody* dan melakukan identifikasi kebutuhan informasi *chain of custody* dari beberapa studi literatur, *guidance*, formulir *chain of custody* dan artikel yang memiliki relevansi dengan *chain of custody*.

4.1.1 Standar Informasi Dalam Metadata

Penelitian ini memiliki tujuan untuk membuat mekanisme *chain of custody* bukti digital yang relevan seperti formulir fisik namun menggunakan pendekatan metadata. Metadata yang digunakan sebagai media untuk merncatat aktivitas *chain of custody* akan disimpan dalam bentuk *file* XML. Konsep metadata digunakan sebagai media yang dapat ditawarkan menjadi salah satu solusi pengelolaan *chain of custody* barang bukti berbasis digital. Dalam merumuskan formula metadata, pendekatan standar metadata yang digunakan dalam penelitian ini adalah standar metadata *Dublin Core*. Terdapat banyak standar umum dalam metadata diataranya adalah BIB Frame, DDWA, DDI, Exif, Ead, OWL, Mods, Premis dan lain-lain. Namun standar metadata *dublin core* dipilih karena merupakan standar metadata yang paling sederhana, mudah dipahami dan mudah untuk diadopsi dan disesuaikan dengan kebutuhan (Riley, 2017).

Pada Tabel 4.1 merupakan tabel pemetaan elemen informasi yang dapat menunjukkan standar informasi atau informasi apa saja yang biasa ada dalam sebuah metadata. Beberapa kelompok metadata telah diidentifikasi berdasarkan elemen informasi yang ada pada standar metadata *Dublin Core*. Terdapat 15 elemen informasi dalam standar metadata *dublin core* diantaranya *specific information, title / name of file, creator, description, publisher, contributor, date/time, type, format, identifier, source, language, relation, coverage* dan *right*. Beberapa kelompok metadata yang didapatkan dari beberapa sumber pustaka yaitu *descriptive metadata, administratif metadata, structure metadata, pseudo metadata, application metadata, technical metadata, file system metadata, use metadata* dan *preservation metadata.*

Dari seluruh referensi yang ada, dapat diketahui bahwa mayoritas kelompok metadata memiliki satu atau beberapa informasi yang terdapat di dalam standar metadata *dublin core*. Seperti pada NISO, (2004), metadata dari sebuah *file* digital ternyata paling tidak memuat informasi mengenai *Tittle/Name of File*, *Creator*, *Abstract, Keyword, Format*, *Contributor* dan *Date/Time*. Menurut Tanner, Shook, Hardy, & Bacon, (2011), metadata paling tidak dapat memuat informasi *Abstract, Keyboard* dan *Specific Information*. Menurut Raghavan, (2014), metadata *file* digital paling tidak memuat informasi tentang *Specific Information* dan *Tittle/Name of File*. Menurit Baca, (2008), metadata paling tidak dapat memuat informasi Lokasi *File*, *Description*, *How to access it, Date/time, Format* dan *Righ*t. Menurut Riley, (2017), sebuah metadata memuat informasi *Tittle*, *Creator, Subject, Publisher, Date/Time, Type Format, Size, Relation* dan *Right*. Dan menurur Gartner, (2016), metadata setidaknya memuat informasi *Size of file, How to access it, Keyboard, Tittle/Name of a file*, *Creator, Subject, Publisher, Date/Time, Identifier, Format* dan *Righ*t.

Tabel 4.1 Pemetaan Elemen Informasi Kelompok Metadata Menggunakan *Dublin Core*

NO	Referensi	Kelompok Metadata	Penjelasan							DUBLIN CORE														
				File Location	*How to Access it*	*Size of file*	*Comment*	*Abstract*	*Keyword*	*Specifi Information*	*Title / Name of File*	*Creator*	*Subject*	*Description*	*Publisher*	*Contributor*	*Date / Time*	*Type*	*Format*	*Identifier*	*Source*	*Languange*	*Relation*	*Coverage*	*Right*
1	NISO, (2004)	*Metadata Deskriptif* (Metadata Deskriptif)	Mendeskripsikan sebuah sumber dengan tujuan agar sumber daya mudah untuk ditemukan dan diidentifikasi. Elemen yang termasuk diantaranya *title, abstract, author, and keywords*.					■	■		■	■							■						
		Structural Metadata (Metadata Struktural)	Untuk dapat mengindikasikan / mengetahui bagaumana sebuah objek dapat terbentuk dari sekumpulan objek. Misalnya sebuah buku dapat terbentuk dari beberapa *chapter*.																					
		Administrative Metadata (Metadata Administratif)	Menyediakan informasu yang dapat membantu mengelola sumber daya seperti kapan dan bagaimana sumber daya dibuat, tipe *file*, siapa yang dapat mengaksesnya dan informasi teknis lainnya.														■	■							

Tabel 4. 2 Pemetaan Elemen Informasi Kelompok Metadata Menggunakan *Dublin Core* Lanjutan

NO	Referensi	Kelompok Metadata	Penjelasan							*DUBLIN CORE*															
				File Location	***How to Access it***	***Size of file***	***Comment***	***Abstract***	***Keyword***	***Specifi Information***	***Title / Name of File***	***Creator***	***Subject***	***Description***	***Publisher***	***Contributor***	***Date / Time***	***Type***	***Format***	***Identifier***	***Source***	***Languange***	***Relation***	***Coverage***	***Right***
	Tanner et al., (2011)	*Pseudo metadata* atau *hidden metadata*	Merupakan metadata yang melekat langsung dan tersimpan pada objek *file*nya, misalnya adalah komentar yang dibuat pada sebuah dokumen word/pdf																						
		Application Metadata (Metadata Aplikasi)	Merupakan metadata yang dihasilkan dari aplikasi yang digunakan dalam menghasilkan/mengolah *file*nya. Setiap aplikasi memiliki standar tersendiri dalam menghasilkan metadatanyanya, misalnya aplikasi dengan ektensi JPG akan menghasilkan metadata yang berbeda dengan aplikasi yang menghasilkan PDF																						

Tabel 4. 3 Pemetaan Elemen Informasi Kelompok Metadata Menggunakan *Dublin Core* Lanjutan

NO	Referensi	Kelompok Metadata	Penjelasan							DUBLIN CORE															
				File Location	*How to Access it*	*Size of file*	*Comment*	*Abstract*	*Keyword*	*Specifi Information*	*Title / Name of File*	*Creator*	*Subject*	*Description*	*Publisher*	*Contributor*	*Date / Time*	*Type*	*Format*	*Identifier*	*Source*	*Languange*	*Relation*	*Coverage*	*Right*
		Filesystem Metadata	Adalah metadata standar yang langsung dapat dilihat dari menu properties *file*nya, misalnya adalah data seputar nama dan pemilik *file* serta MAC dari *file* tsb																						
3	Raghavan, (2014)	*file system metadata*	Metadata yang dihasilkan oleh *file* system							■															
		Application metadata (Metadata Aplikasi)	metadata yang dihasilkan secara khusus oleh aplikasi tertentu								■														
4	Baca, (2008)	*Administrative metadata* (Metadata Administratif)	Metadata yang memuat informasi administrattif pengelolaan objek dan informasi objek	■																					
		Descriptive Metadata (Metadata Deskriptif)	Metadata untuk mengidentifikasi dan menggambarkan koleksi dan informasi objek terkait.											■											

Tabel 4. 4 Pemetaan Elemen Informasi Kelompok Metadata Menggunakan *Dublin Core* Lanjutan

NO	Referensi	Kelompok Metadata	Penjelasan							DUBLIN CORE															
				File Location	*How to Access it*	*Size of file*	*Comment*	*Abstract*	*Keyword*	*Specifi Information*	*Title / Name of File*	*Creator*	*Subject*	*Description*	*Publisher*	*Contributor*	*Date / Time*	*Type*	*Format*	*Identifier*	*Source*	*Languange*	*Relation*	*Coverage*	*Right*
		Preservation Metadata	Metadata digunakan untuk keperluan dokumentasi yaitu metadata yang berkaitan dengan manajemen penyimpanan koleksi dan informasi objek																						
		Technical Metadata (Metadata Teknikal)	Metadata yang berkaitan dengan perilaku teknis dan bagaimana sistem dapat berfungsi		■												■		■						
		Use Metadata	Metadata yang memuat informasi level akses dan penggunaan terhadap koleksi dan informasi objek seperti mencatat tindakan yang telah dilakukan oleh pengguna terhadap objek.																						■
5	Riley, (2017)	*Descriptive Metadata* (Metadata Deskriptif)	Metadata yang digunakan untuk kepentingan memahami dan menemukan obyek (sumber daya)								■	■	■		■		■		■						

Tabel 4. 5 Pemetaan Elemen Informasi Kelompok Metadata Menggunakan *Dublin Core* Lanjutan

NO	Referensi	Kelompok Metadata	Penjelasan																							
				File Location	***How to Access it***	***Size of file***	***Comment***	***Abstract***	***Keyword***	***DUBLIN CORE***																
										Specifi Information	***Title / Name of File***	***Creator***	***Subject***	***Description***	***Publisher***	***Contributor***	***Date / Time***	***Type***	***Format***	***Identifier***	***Source***	***Languange***	***Relation***	***Coverage***	***Right***
		Administrative Metadata (Metadata Administratif)	Metadata memuat informasi yang dibutuhkan dalam mengelola sumber daya terkait dengan informasi penciptaan sumber daya tersebut. Terdiri dari ***technical metadata*** (*decoding* dan *rendering file* seperti *file type*), ***preservation metadata*** (manajemen kelangsungan *file* seperti nilai *hash*) dan ***right metadata*** (*intelectual property content*)			■											■	■							■
		Structural Metadata (Metadata Struktural)	Metadata memuat informasi hubungan atau relasi antara obyek (sumber daya) satu dengan obyek lainnya																			■		
6	Gartner, (2016)	*Descriptive Metadata* (Metadata Deskriptif)	Metadata yang digunakan untuk membantu pencarian objek. Fungsinya seperti informasi pada katalog.						■		■	■	■		■		■			■					

Tabel 4. 6 Pemetaan Elemen Informasi Kelompok Metadata Menggunakan *Dublin Core* Lanjutan

NO	Referensi	Kelompok Metadata	Penjelasan							DUBLIN CORE															
				File Location	*How to Access it*	*Size of file*	*Comment*	*Abstract*	*Keyword*	*Specifi Information*	*Title / Name of File*	*Creator*	*Subject*	*Description*	*Publisher*	*Contributor*	*Date / Time*	*Type*	*Format*	*Identifier*	*Source*	*Languange*	*Relation*	*Coverage*	*Right*
		Administrative metadata (Metadata Administratif)	Menyediakan informasi bahwa data dapat disimpan, dikelola dan diakses kapanpun ketika dibutuhkan. Seperti informasi teknis, *right* dan *preservation*. Informasi teknis misalnya pada *digital image* yaitu *size*, *file* format in px dan *compression*. Informasi *right* memuat intelektual properti yaitu *grant access*. dan informasi penyimpanan untuk memastikan bahwa objek dapat diakses dan digunakan di masa yang akan datang.																						
		Metadata Structural (Metadata Struktural)	Untuk mengetahui struktur yang dapat membentuk sebuah komponen sederhana menjadi sebuah komponen yang lebih besar dan memiliki arti yang luas bagi pengguna.																						

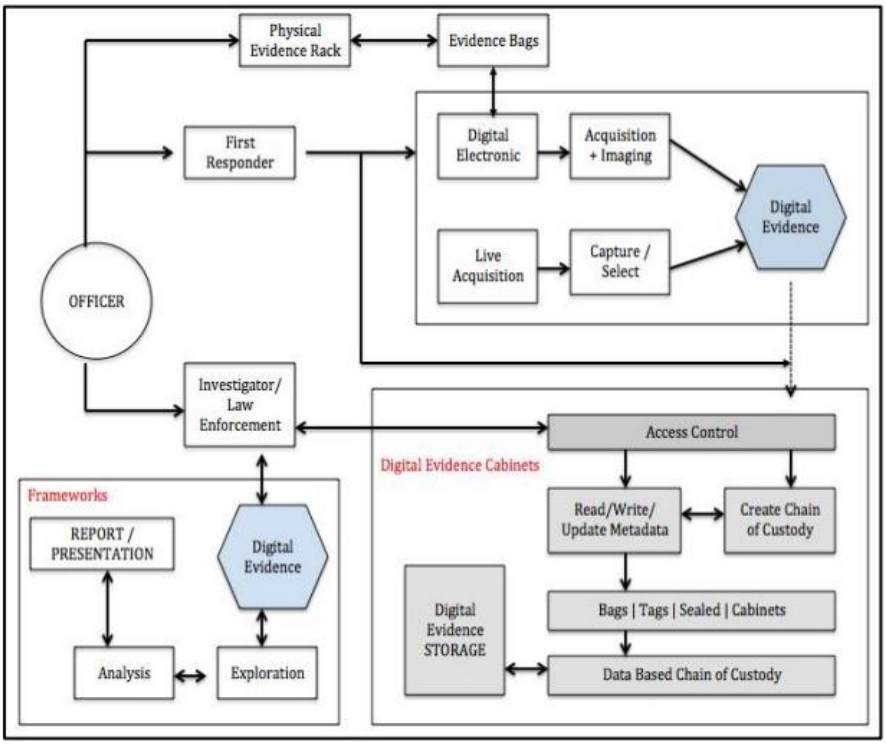
4.1.2 Dasar Acuan Identifikasi Kebutuhan Informasi

Dalam menentukan kebutuhan *field* informasi yang sesuai untuk pengelolaan *chain of custody* bukti digital diperlukan sebuah acuan. Acuan tersebut merupakan dasar dalam berfikir agar informasi yang terkandung di dalam metadata tidak berlebihan namun tetap memenuhi tujuan awal dari pengelolaan *chain of custody* untuk bukti digital. Formula informasi metadata akan ditentukan menggunakan bantuan dari standar metadata *dublin core* dan dikombinasikan dengan tiga poin penting dalam *chain of custody.* Ketiga poin tersebut diantaranya; kebutuhan fungsional, model bisnis dan *legal standard*.

Terkait dengan ketiga poin tersebut, penelitian ini menetapkan ketentuan diantaranya; bahwa kebutuhan fungsional *chain of custody* barang bukti digital adalah dokumen *chain of custody* hanya akan berubah apabila terjadi interaksi dengan barang bukti, model bisnis *chain of custody* adalah berkaitan dengan pendekatan manajemen *chain of custody* dan individu yang bertanggung jawab di dalam manajemen *chain of custody* tersebut sedangkan *legal standard* adalah berkaitan dengan aspek hukum yang menjadi landasan dalam melakukan aktivitas *chain of custody*. Dalam hal ini aktivitas manajemen *chain of custody* adalah sesuai dengan Peraturan Kepala Kepolisian Republik Indonesia No 10 Tahun 2010 tentang tata cara pengelolaan barang bukti. Oleh karena itu, ketiga aspek tersebut akan menjadi acuan utama dalam menentukan kebutuhan *field* informasi metadata *chain of custody* bukti digital.

Berkaitan dengan model bisnis *chain of custody* untuk bukti digital, penelitian ini mengadaptasi dari penelitian Prayudi, Ashari, & Priyambodo, (2015) yaitu pendekatan model bisnis digital forensik seperti pada Gambar 4.1 Pendekatan model tersebut menggunakan konsep metadata sebagai media untuk menyimpan informasi manajemen *chain of custody* bukti digital. Selain itu, petugas yang bertanggung jawab terhadap *chain of custody* barang bukti adalah *First Responder*, investigator, dan petugas pengelola yang bertanggung jawab penuh terhadap akses dan pengelolaan barang bukti. Sedangkan untuk penyimpanan bukti digital sendiri pada penelitian ini menggunakan pendekatan dari *framework digital evidence cabinet* oleh Prayudi, Ashari, et al., (2014). Dimana pada pendekatan *digital evidence cabinet* bukti digital disimpan dalam suatu rak khusus pada sebuah *server*. Bukti digital tersebut akan dapat diakses oleh *user* setelah mendapatkan *approve* (hak akses) dari pihak pengelola (*administrator*). Secara fungsional, informasi manajemen *chain of custody* dimulai dari barang bukti elektronik, kemudian dilakukan proses akuisisi oleh *First Responder* dan menyimpan hasil akuisisi ke dalam ruang penyimpanan (*storage*) yaitu menggunakan konsep *Digital Evidence Cabinet*. Petugas yang

bertanggung jawab terhadap informasi metadata *chain of custody* yang mencatat keluar dan masuknya barang bukti dari ruang penyimpanan adalah petugas pengelola (*officer*). Informasi metadata manajemen *chain of custody* barang bukti digital tersebut hanya akan berubah atau diperbaharui apabila terjadi interaksi barang bukti dari dan ke ruang penyimpanan (*Digital Evidence Cabinet*). Sedangkan hal-hal terkait dengan proses analisis, eksplorasi dan *report*ing barang bukti digital berada di luar model bisnis *chain of custody* dan menjadi tanggung jawab seorang ahli dalam hal ini sesuai dengan Standar Operasional Prosedur yang berlaku.



Gambar 4.1 Model Manajemen *Chain of Custody* Bukti Digital
(Sumber : Prayudi, Ashari, & Priyambodo, (2015))

Terkait dengan apa saja aktivitas yang terdapat pada *chain of custody* dalam manajemen barang bukti, di Indonesia telah diatur di dalam Peraturan Kepala Kepolisian Republik Indonesia No 10 Tahun 2010 tentang tata cara pengelolaan barang bukti di lingkungan kepolisian. Aktivitas pengelolaan barang bukti sesuai dengan tercantum di dalam Bab V dalam Perkap meliputi; penerimaan dan penyimpanan barang bukti, pengamanan dan perawatan barang bukti, serta pengeluaran barang bukti baik untuk keperluan pemeriksaan, peminjaman, pemusnahan dan lain-lain dari ruang penyimpanan khusus barang bukti. Seluruh aktivitas pengelolaan barang bukti tersebut dicatat dan didokumentasikan oleh petugas PPBB (Petugas Pengelola Barang Bukti).

Berdasarkan uraian tersebut, maka penelitian ini menggunakan pendekatan model manajemen *chain of custody* pada Gambar 4.1 dan Peraturan Kepala Kepolisian Republik Indonesia No 10 Tahun 2010 sebagai dasar acuan untuk melakukan identifikasi dan menentukan kebutuhan informasi *chain of custody*.

4.1.3 Kebutuhan Informasi *Chain of Custody*

Di beberapa organisasi dan institusi, *chain of custody* pada prakteknya dilakukan berbasis kertas (*paper based*) yaitu menggunakan formulir *chain of custody*. Formulir *Chain of Custody* berisi *field* catatan informasi mengenai barang bukti dan perjalanan barang bukti. Informasi yang terdapat di dalam formulir tersebut merupakan informasi penting yang diperlukan di dalam persidangan. Selama ini belum terdapat regulasi atau aturan baku yang menjadi acuan utama bagi organisasi dalam melakukan aktivitas dan menentukan kebutuhan informasi *chain of custody* untuk barang bukti. Hal ini menyebabkan masing-masing organisasi memiliki aturan tersendiri dan mekanisme pelaksanaan *chain of custody* menjadi berbeda-beda sesuai dengan peraturan dan kebutuhan dari setiap organisasi.

Pada saat ini, panduan atau standart operasional yang membahas tentang kebutuhan informasi di dalam dokumen *chain of custody* barang bukti terutama untuk barang bukti digital masih sangat sedikit. Namun terdapat beberapa studi yang membahas mengenai kebutuhan umum informasi manajemen *chain of custudy*. Menurut Ashcr*o*ft et al., (2004) dalam laporan *National Institute of Justice* dokumentasi *chain of custody* setidaknya dapat merekam informasi terkait segala tindakan, tahapan atau aktivitas maupun perpindahan barang bukti serta subyek/personel/organisasi yang terlibat dengan aktivitas tersebut. Pernyataan ini sejalan dengan pernyataan dari Dahiya & Sangwan, (2014), Thomson, (2011), Gayed, Lounis, & Bari, (2012), Woods, Chassan*o*ff, & Lee, (2013), Giova, (2011), Ryder, (2002), ENISA & Andreson, (2014), Cosic et al., (2011), Graves, (2013) dan Coons, (2015). Selanjutnya Ashcr*o*ft et al., (2004), Dahiya & Sangwan, (2014), Woods et al., (2013), Giova, (2011), ENISA & Andreson, (2014), dan Graves, (2013) juga menyatakan bahwa detail tanggal/waktu dari setiap aktivitas terhadap barang bukti tersebut juga perlu diperhatikan. Selain informasi tersebut, terkait dengan kemanan barang bukti Ashcr*o*ft et al., (2004), Dahiya & Sangwan, (2014), Thomson, (2011), ENISA & Andreson, (2014), Ryder, (2002), Cosic et al., (2011) dan Graves, (2013) menyebutkan bahwa *chain of custody* seharusnya juga dapat memberikan informasi tentang bagaimana barang bukti disimpan dan dianalisa. Informasi yang berkaitan dengan penyimpanan barang bukti meliputi deskripsi lokasi penyimpanan beserta nilai MD5/SHA-1 apabila barang bukti tersebut adalah barang bukti

digital. Sedangkan untuk informasi yang berkaitan dengan analisa barang bukti meliputi metode dan tools atau perangkat yang digunakan selama proses analisa. Informasi penting lain yang seharusnya ada di dalam dokumen *chain of custody* adalah berkaitan dengan informasi bagaimana barang bukti tersebut didapatkan (*collection*). Hal ini disebutkan oleh Ashcr*o*ft et al., (2004), Dahiya & Sangwan, (2014), Thomson, (2011), Gayed et al., (2012), ENISA & Andreson, (2014), Cosic et al., (2011) dan Coons, (2015). Selain itu Ashcr*o*ft et al., (2004), Dahiya & Sangwan, (2014), Thomson, (2011), Gayed et al., (2012) dan Coons, (2015) menambahkan bahwa informasi kasus juga diperlukan dalam dokumen *chain of custody*. Salah satu informasi penting lainnya untuk *chain of custody* menurut Ashcr*o*ft et al., (2004) adalah berkaitan dengan *role of evidence*. *Role of evidence* ini merupakan informasi yang menjadi motivasi mengapa barang bukti dipilih sebagai barang bukti untuk membantu dalam penyelesaian kasus dan informasi-informasi apa saja yang diharapkan dapat ditemukan dari barang barang bukti yang memiliki potensi kuat terhadap penyelesaian kasus (*potensial sought*).

Secara garis besar informasi *chain of custody* seharusnya dapat menjawab pertanyaan tentang 5W+1H (Cosic et al., 2011). *Chain of custody* minimal dapat memberikan informasi yang berkaitan dengan aktivitas barang bukti dan subyek yang terlibat di dalamnya. Namun dokumen *chain of custody* yang baik adalah dokumen yang memiliki informasi lengkap. Semakin detail dan lengkap informasi yang dicatat maka semakin baik *chain of custody* (Coons, 2015). Pada prinsipnya, informasi pada formulir *chain of custody* untuk barang bukti digital seharusnya memiliki kebutuhan yang hampir sama dengan formulir *chain of custody* untuk barang bukti fisik. Namun karena barang bukti digital memiliki karakteristik yang berbeda dengan barang bukti fisik, maka perlu beberapa informasi pada formulir *chain of custody* yang harus disesuaikan. Untuk lebih mudah mengetahui kebutuhan informasi *chain of custody* dan sesuai dasar acuan identifikasi pada Gambar 4.1, Tabel 4.7 dapat menunjukkan pemetaan kebutuhan informasi *chain of custody* dari beberapa sumber.

Tabel 4.7 Ekstraksi Kebutuhan Informasi *Chain of Custody* Barang Bukti

No	Kebutuhan Informasi CoC	Penjelasan	Ashcroft et al., (2004)	Dahiya & Sangwan, (2014)	Thomson, (2011)	Woods et al., (2013)	Gayed et al., (2012)	Giova, (2011)	ENISA & Andreson, (2014)	Ryder, (2002)	Cosic et al., (2011)	Graves, (2013)	Coons, (2015)
1	Bukti elektronik	Deskripsi perangkat atau spesifikasi temuan barang bukti elektronik, seperti model, manufaktur, tipe, kapasitas, kondisi pada saat ditemukan dan perangkat yang tersambung.	✔	✔	✔	✔	✔	✘	✘	✔	✘	✘	✘
2	Personel yang terlibat	Petugas atau individu yang melakukan interaksi atau terlibat secara langsung dengan barang bukti	✔	✔	✘	✔	✘	✔	✔	✔	✔	✔	✔
3	Lokasi penyimpanan barang bukti	Tempat atau ruang dimana barang bukti disimpan	✔	✔	✔	✘	✘	✔	✔	✔	✔	✔	✘
4	Kondisi lokasi penyimpanan barang bukti	Kondisi keamanan tempat penyimpanan barang bukti	✔	✔	✔	✘	✘	✘	✔	✔	✔	✔	✘
5	Bukti digital	Deskripsi *file* image hasil akuisisi seperti; nama *file*, ukuran dan format	✔	✔	✘	✔	✘	✔	✘	✘	✘	✘	✘

Tabel 4. 8 Ekstraksi Kebutuhan Informasi *Chain of Custody* Barang Bukti Lanjutan

No	Kebutuhan Informasi CoC	Penjelasan	Ashcroft et al., (2004)	Dahiya & Sangwan, (2014)	Thomson, (2011)	Woods et al., (2013)	Gayed et al., (2012)	Giova, (2011)	ENISA & Andreson, (2014)	Ryder, (2002)	Cosic et al., (2011)	Graves, (2013)	Coons, (2015)
6	Proses mendapatkan barang bukti elektronik	Deskripsi aktivitas koleksi (*collection*) oleh petugas. Disebut juga sebagai proses olah Tempat Kejadian Perkara	✔	✔	✔	✘	✔	✘	✔	✔	✔	✔	✔
7	Proses Akuisisi bukti elektronik	Deskripsi aktivitas ekstraksi atau *imaging* bukti elektronik untuk mendapatkan *file* digital di dalamnya	✔	✔	✘	✘	✔	✘	✔	✔	✔	✔	✔
8	Nilai *Hash*/MD5/SHA-1	Nilai hashing *file* hasil ekstraksi atau *imaging*	✔	✔	✘	✔	✔	✔	✔	✘	✔	✔	✔
9	Tanggal/Waktu	Informasi waktu terjadinya aktivitas forensik, interaksi dan perpindahan barang bukti	✔	✔	✘	✔	✘	✔	✘	✘	✔	✔	✔
10	Lokasi ditemukan bukti elektronik	Alamat dimana barang bukti diperoleh	✔	✔	✘	✘	✘	✔	✘	✘	✔	✘	✔
11	Kasus	Deskripsi tentang kasus kejahatan yang melibatkan barang bukti	✔	✔	✔	✘	✔	✘	✘	✘	✘	✘	✔

Tabel 4. 9 Ekstraksi Kebutuhan Informasi *Chain of Custody* Barang Bukti Lanjutan

No	Kebutuhan Informasi CoC	Penjelasan	Ashcroft et al., (2004)	Dahiya & Sangwan, (2014)	Thomson, (2011)	Woods et al., (2013)	Gayed et al., (2012)	Giova, (2011)	ENISA & Andreson, (2014)	Ryder, (2002)	Cosic et al., (2011)	Graves, (2013)	Coons, (2015)
12	Korban dan pelaku	Nama lengkap dari pelaku dan korban kejahatan	✔	✔	✘	✘	✘	✘	✘	✘	✘	✘	✘
13	Interaksi dan perpindahan	Catatan interaksi dan perpindahan seperti peminjaman dan pengeluaran barang bukti dari ruang penyimpanan	✔	✔	✔	✔	✘	✔	✘	✘	✔	✔	✘
14	*Role of evidence*	Alasan mengapa barang bukti dipilih sebagai barang bukti di dalam sebuah kasus dan catatan informasi yang diharapkan (*potensial sought*) sebagai bukti pendukung dalam mengungkap kasus	✔	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘
15	Akses	Individu yang melakukan interaksi dengan barang bukti adalah individu yang memiliki hak akses atau diberikan hak akses kepadanya	✘	✔	✘	✘	✘	✔	✘	✔	✔	✘	✘
16	Perangkat yang digunakan	Nama perangkat yang digunakan selama proses mendapatkan barang bukti	✘	✘	✘	✘	✘	✘	✔	✘	✘	✘	✔

Berdasarkan pemetaan pada Tabel 4.7, Tabel 4.8 dan Tabel 4. 9, kebutuhan informasi *chain of custody* untuk barang bukti digital dapat disederhanakan menjadi beberapa kelompok informasi diantaranya :

1. Informasi kasus (*Case Information*), dapat memberikan informasi terkait identitas kasus yang dimiliki dari setiap barang bukti digital.
2. Informasi mendapatkan bukti elektronik (*Collection Information*), dapat memberikan informasi penting selama proses mendapatkan barang bukti elektronik dari tempat kejadian perkara.
3. Informasi mendapatkan bukti digital (*Acquisition Information*), dapat memberikan informasi proses akuisisi untuk mendapatkan *file* digital dari barang bukti elektronik.
4. Informasi deskripsi bukti Elektronik (*Electronic Evidence Description*), memuat informasi deskripsi baik secara fisik maupun spesifik dari barang bukti elektronik.
5. Informasi hasil akuisisi (*Image Description*), dapat memberikan informasi tentang deskripsi dari *file* image barang bukti termasuk nilai hash atau MD5/SHA-1 dari *file* image bukti digital setelah didapatkan dari barang bukti elektronik.
6. Informasi lokasi penyimpanan (*Storage Information*), dapat memberikan informasi lokasi dan kondisi penyimpanan barang bukti digital.
7. Informasi personel yang terlibat (*Personel Information*), dapat memberikan informasi mengenai siapa saja subyek / individu yang memiliki keterlibatan dengan barang bukti digital. Subyek tersebut dapat meliputi *first responder*, investigator forensik, saksi ahli, penegak hukum, petugas yang menangani manajemen barang bukti, dan pihak-pihak yang dapat terlibat dengan barang bukti apabila diberikan hak akses.
8. *Role of evidence*, dapat memberikan informasi mengenai alasan mengapa bukti elektronik dipilih sebagai barang bukti dalam kasus dan informasi apa saja yang diharapkan dapat diperoleh dari barang bukti tersebut
9. Interaksi dan perpindahan *(Chain of custody),* dapat memberikan informasi mengenai apapun aktivitas / tindakan yang dikenakan terhadap barang bukti, kapan dan alasan mengapa aktivitas tersebut perlu dilakukan.

4.2 Identifikasi Field Informasi *Chain of Custody*

Pada tahap ini, identifikasi *field* informasi untuk metadata *chain of custody* adalah dengan melakukan ekstraksi dari beberapa model formulir *chain of custody* barang bukti yang ada di internet. Selanjutnya, *field* informasi hasil dari identifikasi yang telah dilakukan

akan digunakan di dalam formulir usulan *chain of custody* serta menentukan definisi dan relasi dari masing-masing *field* informasi.

4.2.1 Ekstraksi Model Informasi Formulir *Chain of Custody*

Field informasi untuk metadata *chain of custody* didapatkan dengan melakukan ekstraksi *field* informasi dari beberapa contoh formulir *chain of custody* yang sudah ada. Formulir yang digunakan dalam ekstraksi adalah formulir *chain of custody* barang bukti untuk kasus *computer crime*. Meskipun memiliki tujuan yang sama, namun formulir ini memiliki karakteristik dan perbedaan. Perbedaan dapat terlihat dari jenis barang bukti dan jumlah item barang bukti yang dapat diakomodasi dalam satu formulir *chain of custody*, informasi yang disimpan dan jumlah *field* informasi yang disediakan di dalam formulir. Diantara formulir yang digunakan untuk melakukan ekstraksi *field* informasi adalah formulir *chain of custody* dari University *of* Pennsylvenia, Audit West, NIST (National Institute *of* Standards and Technology), Digital Forensic Lab dan PVL Forensics.

Tabel 4.10, Tabel 4.11, Tabel 4.12, Tabel 4.13 dan Tabel 4.14 merupakan tabel Ekstraksi *field* informasi dari kelima formulir *chain of custody* diatas. Dan berikut dapat dijabarkan perbedaan dari masing-masing formulir *chain of custody* yang digunakan :

1. Formulir *chain of custody* dari University *of* Pennsylvenia

   Merupakan formulir yang dapat digunakan untuk menyimpan catatan informasi barang bukti digital. Selain itu, formulir ini hanya dapat digunakan untuk mencatat satu item barang bukti yaitu satu formulir *chain of custody* adalah untuk satu item barang bukti digital. Di dalam formulir ini memuat beberapa kelompok informasi diantaranya; informasi bukti dan kasus, deskripsi barang bukti digital, histori *copy* dan histori transfer barang bukti.
2. Formulir *chain of custody* dari Audit West

   Merupakan formulir yang digunakan untuk menyimpan catatan *chain of custody* untuk barang bukti komputer elektronik. Dalam satu formulir ini hanya dapat digunakan untuk mencatat satu item barang bukti. Untuk informasi yang dicatat di dalam formulir ini adalah informasi deskripsi barang bukti, informasi penyitaan barang bukti dan informasi *chain of custody*.
3. Formulir *chain of custody* dari Digital Forensics Lab

   Merupakan formulir yang dapat digunakan untuk menyimpan catatan informasi barang bukti fisik/elektronik dan *file* digital hasil akuisisi dari bukti elektronik tersebut. Satu

formulir *chain of custody* Digital Forensics Lab digunakan untuk mencatat satu item bukti fisik dan satu item bukti digital. Di dalam formulir ini, informasi yang dicatat adalah; nomor kasus dan nomor barang bukti, informasi proses mendapatkan barang bukti, detail informasi barang bukti elektronik, detail informasi barang bukti digital, *remarks*, informasi disposal penyerahan barang bukti dan tabel *chain of custody*.

4. Formulir *chain of custody* dari NIST (*National Institute of Standards and Technology*)
   Merupakan formulir yang dapat digunakan untuk mencatat informasi lebih dari satu barang bukti elektronik dalam satu kasus kejahatan yang ditangani. Informasi di dalam formulir ini diantaranya; nomor kasus, petugas, nama korban, nama pelaku dan informasi penyitaan, deskripsi barang bukti, tabel *chain of custody* dan tabel *final disposal* untuk informasi penyerahan atau pemusnahan barang bukti.
5. Formulir *chain of custody* dari PVL Forensics
   Merupakan formulir yang juga dapat digunakan untuk menyimpan catatan informasi lebih dari satu barang bukti. Informasi barang bukti yang dicatat di dalam formulir ini adalah untuk barang bukti digital, diantaranya; nama kasus dan nomor kasus, deskripsi barang bukti digital dan transfer *chain of custody* dari barang bukti digital.

Tabel 4.10 Ekstraksi Model Informasi Formulir *Chain of Custody*

No	Kelompok Informasi	University *of* Pennsilvenia	Audit West	Digital Evidence Lab	NIST	PVL Forensics	Form Usulan
1	Deskripsi bukti elektronik		*Items No*	*Evidence No*	*Item No*		*Model*
			Make	*Device Type*	*Quantity*		*Serial Number*
			Model	*Manufacturer*	*Description*		*Type*
			S/N	*Capacity*			*Manufacturer*
			Date/Time Computer	*Model*			*Electronic Evidence No*
			Attached Devices	*Serial Number*			*Owner*
			Notes	*Additional Info*			***Spesifications***
			Name (Discovered Evidence)	*Digital image taken?*			***Physical Description***
			Name (Seized Evidence)				
			Name (Forensic Activity)				
2	Lokasi penyimpanan	*Storage Location*		*Date/Time Stored*			*Storage Location*
		Storage Condition		*Evidence Storage Location*			*Time Stored*
				Image Storage Location			***Cabinet Structure***
							Validator
3	Deskripsi bukti digital	*Evidence Description*		*Filename*		*Evidence No*	*File Name & Format*
		Software to open		*Size*		*Image Format*	*Size*
		Items number		*Additional Info*			MD5
				MD5 Sum			SHA-1

Tabel 4. 11 Ekstraksi Model Informasi Formulir *Chain of Custody* Lanjutan

No	Kelompok Informasi	University *of* Pennsilvenia	Audit West	Digital Evidence Lab	NIST	PVL Forensics	Form Usulan
				SHA-1 Sum			SHA-256
							Digital Evidence No
							Status
4	(Collection) Mendapatkan bukti elektronik	*Collection Method*	*Date*	*Date/Time Collected*	*Date/Time*		*Tools*
		Date/Time Collected	*Time*	*Site Address*	*Location*		*Date/Time*
		Date of Collector Signature	*Description*				*Address*
			Location				
5	Personel yang terlibat (First Responder)	*Collector Name*		*Collected by*	*Officer Name/ID*		*First Responder Name*
		Collector Signature					***Position***
							Agency
6	Akuisisi bukti elektronik			*Date/Time Imaged*		*Date/Time*	*Acquisition Time*
				Imaged by		*Creator*	*Acquisition Tools*
						Method	*Acquisition Date*
						Device Acquisition	*Acquisition Officer*
						Notes	*Device*
7	Identitas Kasus	*Case Name*	*Case No*	*Case No*	*Case No*	*Case Name*	*Offense*
			Page		*Offense*	*Case Number*	*Suspect*

Tabel 4. 12 Ekstraksi Model Informasi Formulir *Chain of Custody* Lanjutan

No	Kelompok Informasi	University *of* Pennsilvenia	Audit West	Digital Evidence Lab	NIST	PVL Forensics	Form Usulan
			Of		*Victim*		*Victim*
					Suspect		*Case No*
8	*Handover / Disposal*			*Date/Time*	*Item No (disposal)*		
				Submitted by	*Suspect (disposal)*		
				Signature	*Method (disposal)*		
				Received by	*Officer (disposal)*		
				Signature	*Date (disposal)*		
				Witnessed by	*Signature (disposal)*		
				Signature	*Item No (Destructionl)*		
				Remarks	*Custodian (Destructionl)*		
					ID (Destructionl)		
					Date (Destructionl)		
					Wittness (Destructionl)		
					Signature (Destructionl)		
					Date Sign (Destructionl)		
					Item No (Release)		
					Custodian (Release)		
					ID (Release)		

Tabel 4. 13 Ekstraksi Model Informasi Formulir *Chain of Custody* Lanjutan

No	Kelompok Informasi	University *of* Pennsilvenia	Audit West	Digital Evidence Lab	NIST	PVL Forensics	Form Usulan
					To Name (Release)		
					Address		
					City		
					State		
					Zip Code		
					Phone No		
					Signature owner		
					Date Sign (Release)		
					Copy attached?		
9	informasi interaksi dan perpindahan	*Date*	*Registered Mail*	*Case No*	*Item No*	*Evidence No*	*Autorized by*
		Copied By	*Date*	*Evidence No*	*Date/Time*	*Date*	*Received by*
		Copy Method	*Time*	*Page No*	*Released Id*	*Time*	*Action*
		Disposition of original and all copy	*Released by*	*Submitter Name*	*Received by*	*From*	***Request time***
		Transfered From	*Signature*	*Signature*	*Comments/Location*	*Signature*	***Approve time***
		Transfered To	*Received by*	*Receiver Name*		*To*	***Received time***
		Storage Location Now	*Signature*	*Signature*		*Signature*	
		Security Evidence Condition	*Reason*	*Date/Time Submit*		*Description/Reason*	
				Date/Time Receive			
				Evidence Modified			

Tabel 4. 14 Ekstraksi Model Informasi Formulir *Chain of Custody* Lanjutan

No	Kelompok Informasi	University *of* Pennsilvenia	Audit West	Digital Evidence Lab	NIST	PVL Forensics	Form Usulan
10	*Role of evidence*						***Reason For Foreclose***
							Potential Information
11	*Other*					*Form Dscription*	
						Notes	
Jumlah *Field* Informasi		**19**	**23**	**40**	**40**	**20**	**42**

4.2.2 Identifikasi *Field* Informasi Formulir *Chain of Custody*

Ekstraksi pada Tabel 4.10, Tabel 4.11, Tabel 4.12, Tabel 4.13 dan Tabel 4.14 telah dikelompokkan berdasarkan kelompok kebutuhan informasi *chain of custody* bukti digital yang telah dijabarkan pada pembahasan sebelumnya. Pengelompokan *field* informasi tersebut diantaranya "informasi kasus", "informasi mendapatkan buki elektronik", "informasi mendapatkan bukti digital", "deskripsi bukti elektronik", "deskripsi bukti digital", "informasi lokasi penyimpangan", "informasi personel", "*role of evidence*" serta "interaksi dan perpindahan". Terdapat juga dua kelompok informasi tambahan yaitu "lain-lain" dan "*final disposal* dan penyerahan" yang tidak termasuk dalam kebutuhan informasi namun informasi tersebut terdapat di dalam formulir *chain of custody*.

Pada penelitian ini pengelompokan informasi yang dilakukan tidak berdasarkan konsep pendekatan tertentu seperti *ontology* yang sering dipakai peneliti di dalam domain *chain of custody*. Penelitian ini mengelompokkan informasi berdasarkan kesesuaiannya terhadap kelompok informasi yang sebelumnya telah diidentifikasi. Selain itu, untuk memperoleh usulan *field* informasi untuk metadata *chain of custody* bukti digital adalah dengan cara normalisasi dari *field* informasi pada kelima formulir yang ada. Normalisasi dilakukan dengan menghapus beberapa *field* yang kurang sesuai dan menambahkan beberapa *field* yang dibutuhkan pada *field* informasi formulir usulan agar tujuan dan kebutuhan informasi *chain of custody* bukti digital dapat tercapai.

Dari proses normalisai *field* informasi pada formulir diperoleh sebanyak 42 *field* informasi untuk formulir usulan. Beberapa *field* informasi dipilih dari formulir yang telah ada dan beberapa lainnya merupakan *field* informasi tambahan, diantaranya;

- Kelompok informasi **"Deskripsi bukti elektronik"** terdiri dari *field* informasi *model, serial number, type, manufacturer, electronic evidence no, owner, spesifikation* dan *physical description*.
- Kelompok informasi **"Lokasi penyimpanan"** terdiri dari *field* informasi *storage location, cabinet structure, time stored* dan *validator*.
- Kelompok informasi **"Deskripsi bukti digital"** terdiri dari *field* informasi *file name, size,* MD5, SHA-1, SHA-256, *digital evidence no* dan *status*.
- Kelompok informasi **"Mendapatkan bukti elektronik"** terdiri dari *field* informasi *tools, date/time* dan *address*.
- Kelompok informasi **"Perosnel yang terlibat"** terdiri dari *field* informasi *first responder name, position* dan *status* serta *agency*.

- Kelompok informasi **"Akuisisi bukti elektronik"** terdiri dari *field informasi acquisition time, acquisition tools, acquisition date, device* dan *acquisition officer*.
- Kelompok informasi **"Identitas kasus"** terdiri dari *field* informasi *case no, offense, suspect* dan *victim*.
- Kelompok informasi **"Interaksi dan perpindahan"** terdiri dari *field informasi autorized by, received by, request time, approve time, received time* dan *action*.
- Kelompok informasi **"Role *of* evidence"** merupakan kelompok informasi tambahan yang sebelumnya tidak terdapat di dalam formulir. Informasi ini terdiri dari *field reason for foreclose* dan *potential information*.
- Sedangkan kelompok informasi **"lain-lain"** serta **"final disposal dan penyerahan"** barang bukti tidak digunakan atau dihilangkan di dalam formulir usulan.

Setiap *field* informasi pada formulir usulan merepresentasikan informasi tertentu pada formulir *chain of custody* bukti digital. Berikut merupakan deskripsi dari masing-masing *field* informasi;

Tabel 4.15 *Field* Informasi Formulir Usulan *Chain of Custody*

***Field* Informasi**

No	Nama *Field*	Keterangan
1	*Case No*	Field informasi yang merepresentasikan nomor kasus dari barang bukti digital
2	*Offense*	*Field* informasi yang merepresentasikan tipe kasus dari tindak kejahatan. Misalnya tipe kejahatan sosial media, pelanggaran UU ITE dan lain-lain.
3	*Suspect*	*Field* informasi yang merepresentasikan nama tersangka/pelaku kasus kejahatan
4	*Victim*	*Field* informasi yang merepresentasikan nama dari korban tindakan kejahatan
5	*First Responder Name*	*Field* informasi yang merepresentasikan nama dari Petugas yang melakukan olah TKP barang bukti
6	*Position*	*Field* informasi yang merepresentasikan jabatan dan status dari petugas yang melakukan olah TKP barang bukti
7	*Agency*	*Field* informasi yang merepresentasikan organisasi / instansi yang menaungi petugas olah TKP

Tabel 4. 16 *Field* Informasi Formulir Usulan *Chain of Custody* Lanjutan

No	Nama *Field*	Keterangan
8	*Tools*	*Field* informasi yang merepresentasikan nama perangkat yang digunakan dalam melakukan proses olah TKP BB
9	*Date/Time*	*Field* informasi yang merepresentasikan tanggal dan waktu dilakukan proses olah TKP
10	*Address*	*Field* informasi yang merepresentasikan tempat/alamat olah TKP dilakukan
11	*Electronic Evidence No*	*Field* informasi yang merepresentasikan no register atau no daftar yang diberikan pada bukti elektronik
12	*Model*	*Field* informasi yang merepresentasikan model/seri dari bukti elektronik
13	*Serial Number*	*Field* informasi yang merepresentasikan nomor serial bukti elektronik
14	*Type*	*Field* informasi yang merepresentasikan tipe bukti elektronik. Misalnya komputer atau laptop
15	*Manufacturer*	*Field* informasi yang merepresentasikan manufaktur bukti elektronik
16	*Spesifikation*	*Field* informasi yang merepresentasikan spesifikasi yang dimilikioleh bukti elektronik seperti kapasistas penyimpan, processor, RAM dan lain-lain
17	*Physical Description*	*Field* informasi yang mendeskripsikan bukti elektronik secara fisik, seperti warna, bentuk, berat dan ukuran
18	*Owner*	*Field* informasi yang merepresentasikan nama dari pemilik barang bukti elektronik
19	*Acquisition Time*	*Field* informasi yang merepresentasikan waktu dilakukan proses mendapatkan bukti digital dari bukti elektronik
20	*Acquisition Tools*	*Field* informasi yang merepresentasikan perangkat lunak yang digunakan untuk mendapatkan bukti digital
21	*Device*	*Field* informasi yang merepresentasikan perangkat keras yang digunakan untuk mendapatkan bukti digital
22	*Acquisition Date*	*Field* informasi yang merepresentasikan tanggal dilakukan proses akuisisi bukti elektronik

Tabel 4. 17 *Field* Informasi Formulir Usulan *Chain of Custody* Lanjutan

No	Nama *Field*	Keterangan
23	*Acquisition Officer*	*Field* informasi yang merepresentasikan nama petugas yang melakukan akuisisi
24	*File Name*	*Field* informasi yang merepresentasikan nama dan format dari *file* bukti digital hasil proses akuisisi
25	*Size*	*Field* informasi yang merepresentasikan ukuran dari *file* bukti digital
26	MD5	*Field* informasi yang merepresentasikan nilai MD5 yang dimiliki oleh *file* bukti digital
27	SHA-1	*Field* informasi yang merepresentasikan nilai SHA-1 yang dimiliki oleh *file* bukti digital
28	SHA-256	*Field* informasi yang merepresentasikan nilai SHA-256 yang dimiliki oleh *file* bukti digital
29	*Digital Evidence No*	*Field* informasi yang merepresentasikan nomor register penyimpanan dari barang bukti digital
30	*Status*	*Field* informasi yang merepresentasikan status bukti digital. Terdapat 2 macam status yaitu open dan close. Open menunjukkan bahwa bukti digital masih dapat di akses dan masih digunakan untuk keperluan pengadilan. Close menunjukkan bahwa bukti digital telah selesai digunakan.
31	*Storage Location*	*Field* informasi yang merepresentasikan lokasi (path) tempat dimana *file* bukti digital disimpan
32	*Cabinet Structure*	*Field* informasi yang merepresentasikan struktur kabinet dari lokasi penyimpanan bukti digital
33	*Time Stored*	*Field* informasi yang merepresentasikan tanggal/waktu bukti digital disimpan di dalam lokasi penyimpanan
34	*Validator*	*Field* informasi yang merepresentasikan nama petugas validasi terhadap informasi *chain of custody*
35	*Reason For Foreclose*	*Field* informasi yang merepresentasikan alasan mengapa BE ini dipilih sebagai BB dalam kasus, kaitannya dengan suspect dan victim

Tabel 4. 18 *Field* Informasi Formulir Usulan *Chain of Custody* Lanjutan

No	Nama *Field*	Keterangan
36	*Potential Information*	*Field* informasi yang merepresentasikan informasi apa yang diharapkan didapat dari BB ini yang akan mendukung proses investigasi
37	*Autorized by*	*Field* informasi yang merepresentasikan nama dari petugas pengelola yang memberikan akses terhadap bukti digital
38	*Received by*	*Field* informasi yang merepresentasikan nama dari petugas/individu/organisasi yang menerima akses bukti digital
39	*Request time*	*Field* informasi yang merepresentasikan tanggal dan waktu terjadinya permintaan akses terhadap bukti digital
40	*Approve time*	*Field* informasi yang merepresentasikan tanggal dan waktu disetujuinya permintaan akses terhadap bukti digital
41	*Received time*	*Field* informasi yang merepresentasikan tanggal dan waktu bukti digital telah diterima atau selesai di *download*
42	*Action*	*Field* informasi yang merepresentasikan alasan atau tindakan yang dilakukan terhadap bukti digital selama interaksi berlangsung

4.2.3 Pemetaan dan Spesifikasi *Field* Informasi

Dokumentasi *chain of custody* setidaknya dapat memuat informasi perihal pertanyaan 5W+1H yaitu *What, Who, Where, When, Why* dan *Ho*w tentang barang bukti di persidangan (Cosic et al., 2011). Berdasarkan rangkaian informasi pada formulir *chain of custody* yang telah diusulkan, maka dapat dipetakan bagaimana konstruksi informasi dari konten metadata formulir usulan terhadap 5W+1H, sebagai berikut;

1. *Who* : *First Responder, Suspect, Victim, Examiner, Officer, Law Enforcement*
2. *What* : Spesifikasi dari Bukti Elektronik dan Bukti Digital yang didapat
3. *Where* : Lokasi olah TKP Bukti Elektronik dan lokasi Bukti Digital
4. *When* : Tanggal dan waktu olah TKP Bukti Elektronik, Akuisisi Bukti Elektronik dan Bukti Digital, Akses terhadap Bukti Digital

5. *Why* : *Role of Evidence,* Mengapa Bukti Elektronik dan Bukti Digital ini dipilih dalam kasus ini serta mengapa melakukan interaksi Bukti Digital

6 *How* : Bagaimana proses akuisisi dan imaging Bukti Digital, *tools* dan alatnya, dan bagaimana kondisi lokasi penyimpanan Bukti Elektronik dan Bukti Digital

Setelah menentukan *field* informasi dari metadata, langkah selanjutnya adalah menentukan bagaimana secara teknis *field* informasi metadata tersebut dihasilkan serta tipe data dan berapa *space* (ukuran) yang dibutuhkan dari masing-masing *field* informasi. Di dalam konsep metadata, sebuah konten informasi metadata dapat dihasilkan melalui dua cara yaitu automatis (didapatkan langsung dari sistem atau aplikasi) dan manual (ditambahkan secara manual oleh *user*). Selain itu terdapat dua istilah lain di dalam konten metadata yaitu metadata statis dan metadata dinamis. Metadata statis adalah metadata yang apabila telah dibuat tidak dapat diubah, contohnya *date created* dari suatu *file*. Sedangkan metadata dinamis adalah metadata yang dapat berubah sesuai dengan kondisi, aktivitas dan keperluan dari suatu *file* misalnya untuk keperluan dokumantasi. Sebagai contoh metadata dinamis dari suatu *file* adalah *date modified* (Baca, 2008).

Di dalam konteks penelitian ini, digunakan dua istilah berdasarkan sifat dari metadata yaitu metadata statis dan metadata dinamis. *Field* informasi yang termasuk di dalam metadata statis adalah *field* informasi metadata yang dihasilkan secara langsung oleh sistem dengan mengambil informasi dari metadata *file* image bukti digital seperti *filename, size, date created, time created* dan *hash value*. Informasi metadata statis tersebut didasarkan pada informasi metadata *Dublin Core*. Sedangkan *field* informasi yang termasuk di dalam metadata dinamis adalah *field* informasi yang ditambahkan secara manual oleh *user*. Selain itu di dalam informasi interaksi atau *chain of custody record*, *field* informasi di dalamnya juga di dapat secara otomatis dari sistem. *Field* informasi metadata dinamis tersebut kemudian disimpan sebagai metadata baru (*New XML Tag*) sebagai contoh *field* informasi *case no, offense, suspect, victim* dan lain-lain.

Untuk lebih jelasnya, pemetaan *field* informasi formulir usulan *chain of custody* berdasarkan kelompok informasi, konten informasi (*What, Where, When, Who, Why* dan *How*), sifat (metadata statis dan metadata dinamis) serta spek teknis (tipe data dan ukuran) dapat ditunjukan pada Tabel 4.19, Tabel 4.20 dan Tabel 4.21.

Tabel 4.19 Pemetaan *Field* Informasi Metadata Untuk Formulir Usulan

No	Kelompok Informasi	*Field* Informasi	*Who*	*When*	*Where*	*What*	*Why*	*How*	Sifat		Spek Teknis
									Statis (*Dublin Core*)	Dinamis (New XML Tag)	
1	Kasus (*Case*)	*Case No*				■				■	Char (15)
		Offense				■					Char (24)
		Suspect	■								Char (24)
		Victim	■								Char (24)
2	*First Responder*	*First Responder Name*	■							■	Char (24)
		Position	■								Char (24)
		Agency	■								Char (24)
3	Olah TKP Bukti Elektronik (*Collection*)	*Tools*				■				■	Char (15)
		Date/Time		■							Date/Time
		Address			■						Char (50)
4	Bukti elektronik (*Electronic Evidence*)	*Model*				■				■	Char (24)
		Serial Number				■					Char (15)
		Type				■					Char (15)
		Manufacturer				■					Char (24)

Tabel 4. 20 Pemetaan *Field* Informasi Metadata Untuk Formulir Usulan Lanjutan

No	Kelompok Informasi	*Field* Informasi	*Who*	*When*	*Where*	*What*	*Why*	*How*	Sifat		Spek Teknis
									Statis (*Dublin Core*)	Dinamis (New XML Tag)	
		Spesification									Char (150)
		Electronic Evidence No									Char (!5)
		Owner									Char (24)
		Physical Description									Char (150)
5	Proses Akuisisi	*Acquisition Time*									Time
		Acquisition Tools									Char (15)
		Acquisition Date									Date
		Acquisition Officer									Char (24)
		Device									Char (50)
6	Hasil Imaging BE (*ImageFile / Digital Evidence*)	*File name*									Char (24)
		Size									Char (10)
		MD5									Char (30)
		Digital Evidence No									Char (15)
		SHA-1									Char (30)
		SHA-256									Char (30)

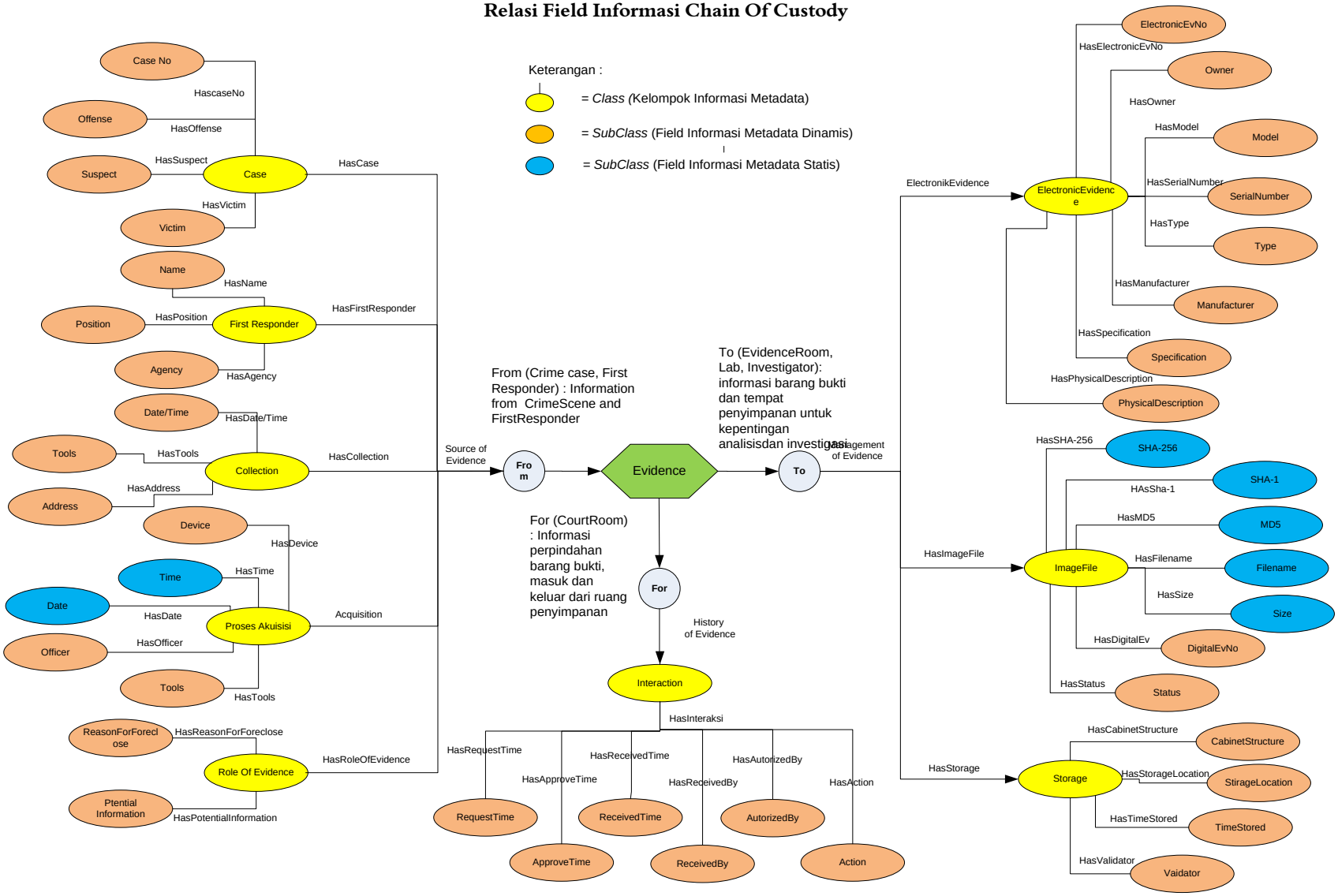
Tabel 4. 21 Pemetaan *Field* Informasi Metadata Formulir Untuk Usulan Lanjutan

No	Kelompok Informasi	*Field* Informasi	*Who*	*When*	*Where*	*What*	*Why*	*How*	Sifat		No
									Statis (*Dublin Core*)	Dinamis (New XML Tag)	
		Status									Char (5)
7	Lokasi Penyimpanan BD (*Storage*)	*Storage Location*									Char (100)
		Cabinet structure									Char (100)
		Time Stored									Date/Time
		Validator									Char (24)
8	*Role of Evidence*	*Reason For Foreclose*									Char (150)
		Potential Information									Char (150)
9	Interaksi Para Pihak (*Interactions*)	*Autorized by*									Char (24)
		Received by									Char (24)
		Request time									Date/Time
		Approve time									Date/Time
		Received time									Date/Time
		Action									Char (150)

4.2.4 Relasi *Field* Informasi *Chain of Custody*

Relasi *field* informasi *Chain Of Custody* dapat ditunjukkan pada Gambar 4.2. Di dalam bagan relasi *chain of custody* pada Gambar 4.2, barang bukti memiliki 3 relasi utama yaitu "*from*", "*for*" dan "*to*". Relasi "from" menunjukkan sumber barang bukti yaitu dari mana, bagaimana, oleh siapa dan mengapa barang bukti tersebut ditemukan dan digunakan sebagai barang bukti. Relasi "*to*" menunjukkan tujuan dari barang bukti setelah ditemukan yaitu untuk disimpan di ruang penyimpanan dan untuk keperluan analisa laboratorium forensik. Informasi pada relasi "*to*" adalah informasi yang berkaitan dengan deskripsi barang bukti, lokasi dan kondisi penyimpanan. Relasi "*for*" menunjukkan bahwa selama barang bukti berada di ruang penyimpanan, seluruh interaksi yang terjadi terhadap barang bukti dilakukan oleh individu atau organisai yang memiliki hak dan sesuai dengan prosedur. Hal ini berkaitan dengan informasi histori perpindahan barang bukti baik masuk dan keluar dari ruang penyimpanan. Ketiga relasi barang bukti dalam *chain of custody* tersebut dapat menunjukkan informasi barang bukti untuk keperluan di dalam persidangan. Informasi barang bukti yang dapat direkam dimulai dari proses mendapatkan barang bukti elektronik, proses mendapatkan barang bukti digital sampai pada tempat penyimpanan dan interaksi barang bukti yang dilakukan oleh para pihak.

Pada Gambar 4.2 dapat diketahui pula kardinalitas dari masing-masing *class* dan *subclass* informasi. Relasi "*From*" memiliki 5 *class* diantaranya "*Case*", "*FirstResponder*", "*Collection*", "*Acquisition*" dan "*RoleOfEvidence*". *Class* "Case" memiliki *Subclass* yaitu "*CaseNo*", "*Offense*", "*Suspect*" dan "*Victim*". *Class* "*FirstResponder*" memiliki *subclass* diantara "*Name*", "*Position*" dan " *Agency*". *Class* "*Collection*" memiliki *subclass* "*Tools*", "*Address*" dan "*Date/Time*". *Class* "*Acquisition*" memiliki *subclass* "*Time*", "*Date*", "*Officer*", "*Tools*" dan "*Device*". Serta *class* "*RoleOfEvidence*" memiliki *subclass* diantaranya "*ReasonForclose*" dan "*PotentialInfo*". Relasi "*To*" memiliki 3 *class* yang terhubung yaitu "*ElectronicEvidence*", "*ImageFile*" dan "*Storage*". *Class* "*ElectronicEvidence*" memiliki *subclass* yaitu "*ElectronicEvNo*", "*Owner*", "*Model*", "*SerialNumber*", "*Type*", "*Manufacturer*", "*Spesification*" dan "*PhysicalDescription*". *Class* "*ImageFile*" memiliki *subclass* yaitu "*DigitalEvNo*", "*Hash*", "*File*name" dan "*size*". Dan *class* "*Storage*" memiliki *subclass* "*CabinetStructure*", "*TimeStored*", "*Validator*" dan "*StorageLocation*". Sedangkan relasi "*For*" memiliki *class* "*Interactions*" dengan *subclass* "*Action*", "*RequestTime*", "*ApproveTime*", "*ReceivedTime*", "*Receivedby*" dan "*Autorizedby*".



Gambar 4. 2 Bagan Relasi *Field* Informasi *Chain Of Custody*

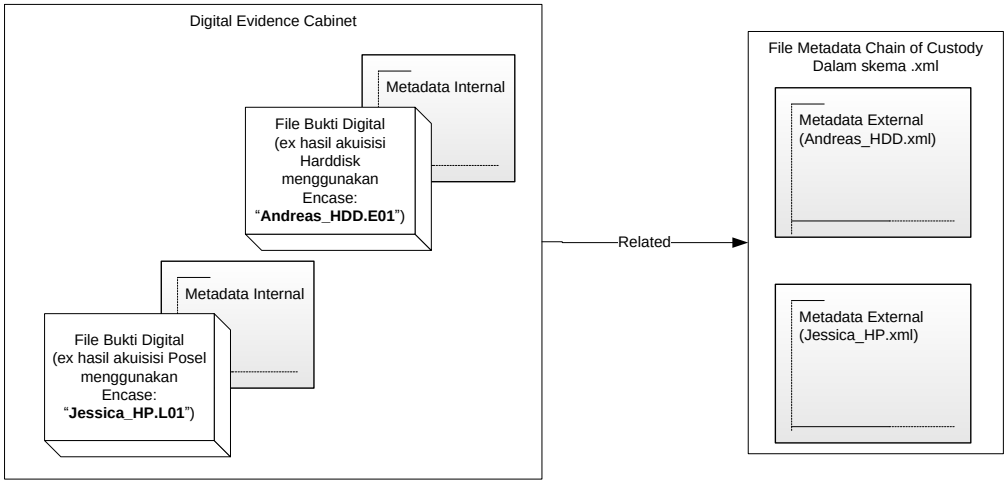
BAB V
IMPLEMENTASI DAN PEMBAHASAN

5.1 Implementasi Model Informasi Metadata

Pada penelitian ini, implementasi dilakukan dengan membuat sebuah aplikasi yang diberi nama *Digital Chain Of Custody* (DCOC). Aplikasi DCOC digunakan untuk membantu melakukan simulai aktivitas manajemen *chain of custody* untuk bukti digital dengan menerapkan konsep model informasi metadata *chain of custody* yang telah dibuat.

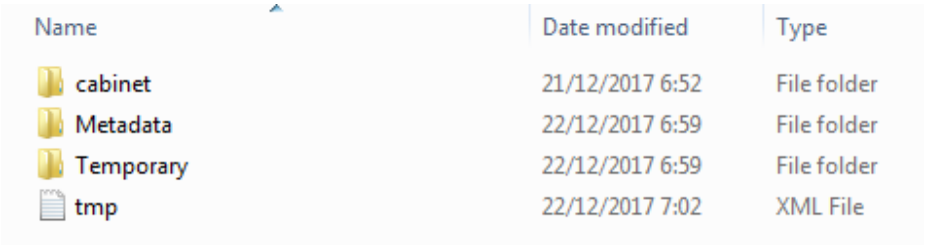
5.1.1 Model Penyimpanan Metadata *Chain Of Custody*

Model informasi metadata yang telah dibuat diimplementasikan dengan menggunakan skema XML. Skema XML dalam hal ini merupakan sebuah *file* dengan ekstensi .XML yang menyimpan informasi *chain of custody* untuk bukti digital sebagai metadata eksternal dari sebuah *file* bukti digital. Konsep penyimpanan *file chain of custody* sebagai metadata eksternal adalah *file* metadata *chain of custody* disimpan terpisah dengan *file* bukti digital dengan nama *file* hasil dokumentasi *chain of custody* akan secara otomatis disesuaikan dengan nama *file* bukti digitalnya. Alasan mengapa menggunakan konsep metadata eksternal untuk menyimpan informasi *chain of custody* adalah karena perubahan pada metadata eksternal tidak merubah nilai integritas (*hash*) dari barang bukti digital. Sebuah aplikasi *Digital Chain Of Custody* (DCOC) juga telah dibuat untuk membantu dalam menunjukkan implementasi model informasi *chain of custody* tersebut. Pada Gambar 5. ***1*** dapat menunjukkan bagaimana implementasi penyimpanan *file* metadata eksternal *chain of custody* terhadap *file* bukti digital yang asli.

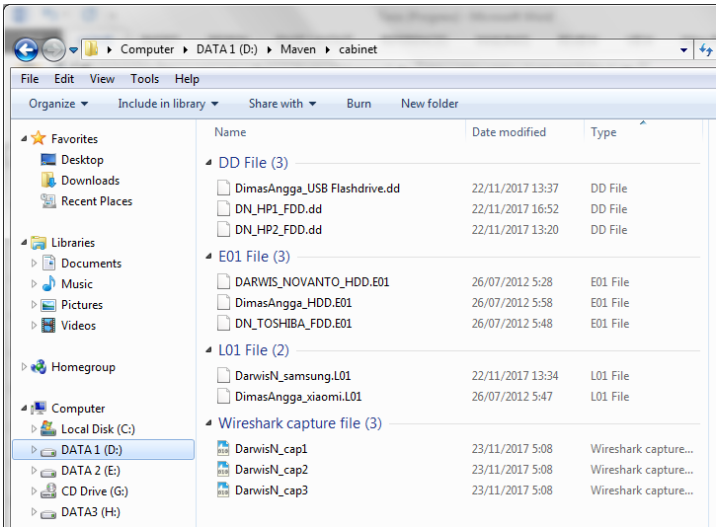


Gambar 5. 1 Implementasi Penyimpanan Metadata *Chain Of Custody*

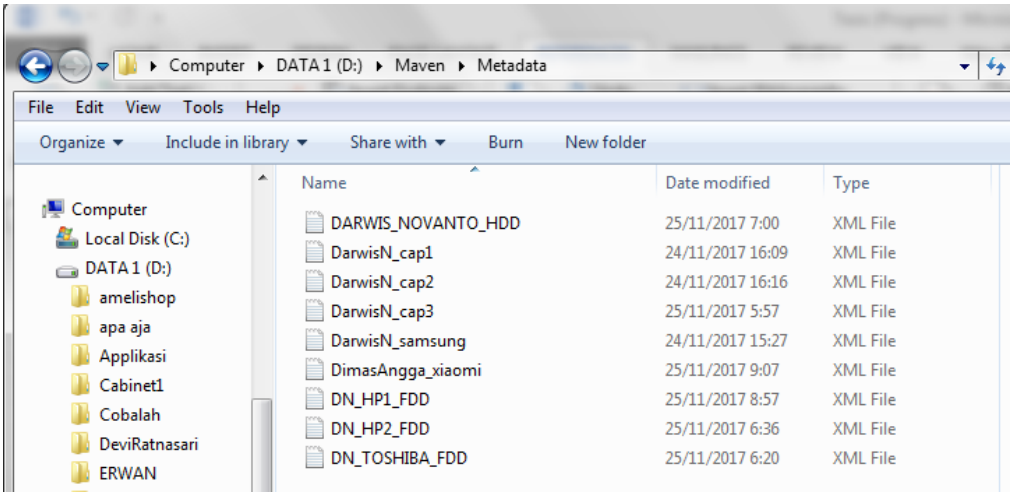
Pada Gambar 5. ***2***, Gambar 5. ***3*** dan Gambar 5. ***4*** menunjukkan realisasi hasil implementasi penyimpanan *file* bukti digital dan *file* hasil entry *chain of custody* di dalam aplikasi *Digital Chain Of Custody* (DCOC). Terdapat tiga direktori yaitu "*Cabinet*" untuk menyimpan *file* bukti digital, direktori "Metadata" untuk menyimpan *file chain of custody* bukti digital dan direktori "Temporary" untuk menyimpan *file temporary chain of custody* serta satu *file* "tmp.xml".



Gambar 5. 2 Penyimpanan *File* Bukti Digital Di Dalam *Cabinet*



Gambar 5. 3 Implementasi Penyimpanan Metadata Aplikasi Digital *Chain Of Custody*



Gambar 5. 4 Pemyimpanan *File* Metadata *Chain Of Custody*

5.1.2 Implementasi dan Simulasi Aplikasi *Digital Chain Of Custody*

Aplikasi *Digital Chain Of Custody* dibuat sesuai dengan dasar acuan yang telah ditetapkan. Dalam aplikasi ini, *user* dibedakan menjadi dua yaitu *user* sebagai *first responder* dan *user* sebagai pengelola (*administrator*). Masing-masing *user* memiliki hak akses yang berbeda-beda. Untuk dapat masuk dan mengakses serta mengelola bukti digital *user* terlebih dahulu harus terdaftar dan melakukan *log in* pada sistem.

Berikut adalah implementasi dari simulasi studi kasus yang dilakukan dalam manajemen *chain of custody* untuk sebuah *file* bukti digital.

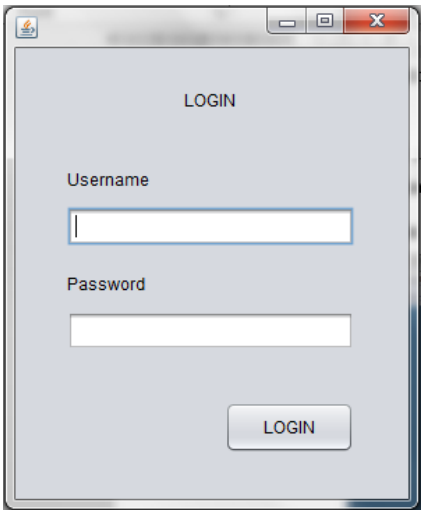
❖ Tampilan Awal Aplikasi *Digital Chain Of Custody*

Gambar 5. 5 Halaman Utama Aplikasi DCOC

Merupakan tampilan halaman awal ketika aplikasi di jalankan. Di dalam aplikasi terdapat 3 menu utama yaitu "*file*", "*manage*" dan "*view* DCOC". Untuk dapat menggunakan menu tersebut terlebih dahulu *user* harus melakukan login ke dalam aplikasi DCOC dengan memasukkan *username* dan *password*.

❖ Tampilan Halaman Login *User*

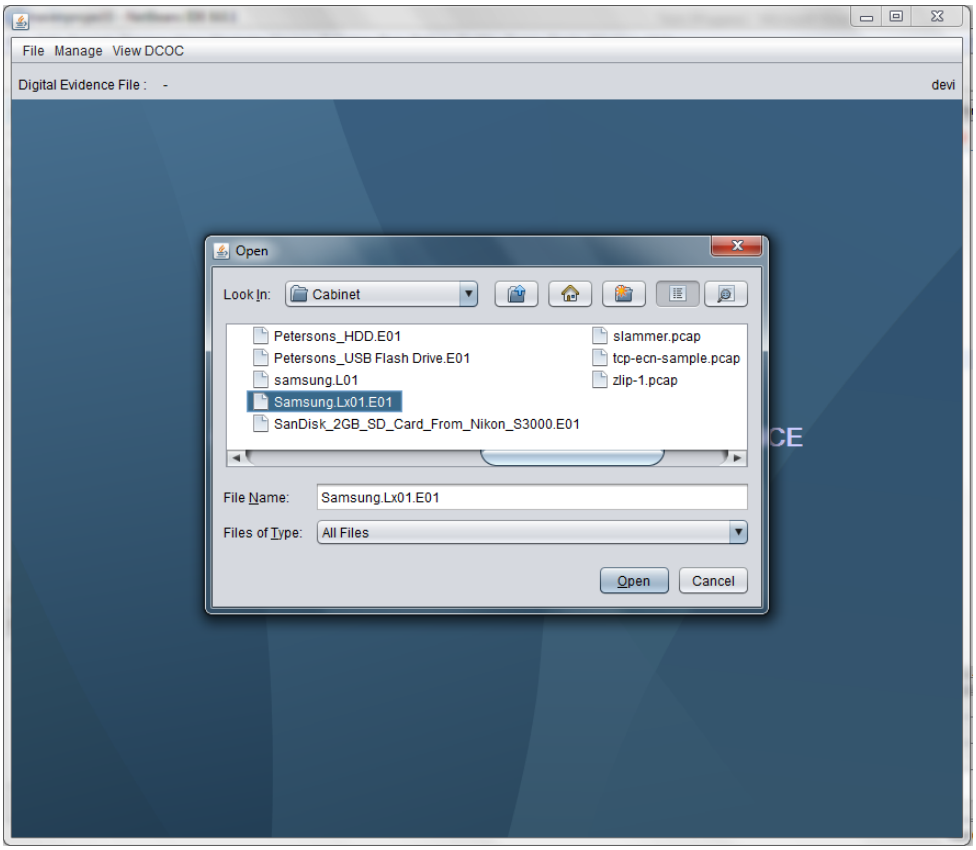
Merupakan halaman yang digunakan oleh *user* untuk memasukkan *user*name dan *password*.



Gambar 5. 6 Halaman Login Aplikasi DCOC

❖ Tampilan Memuat *File* Bukti Digital

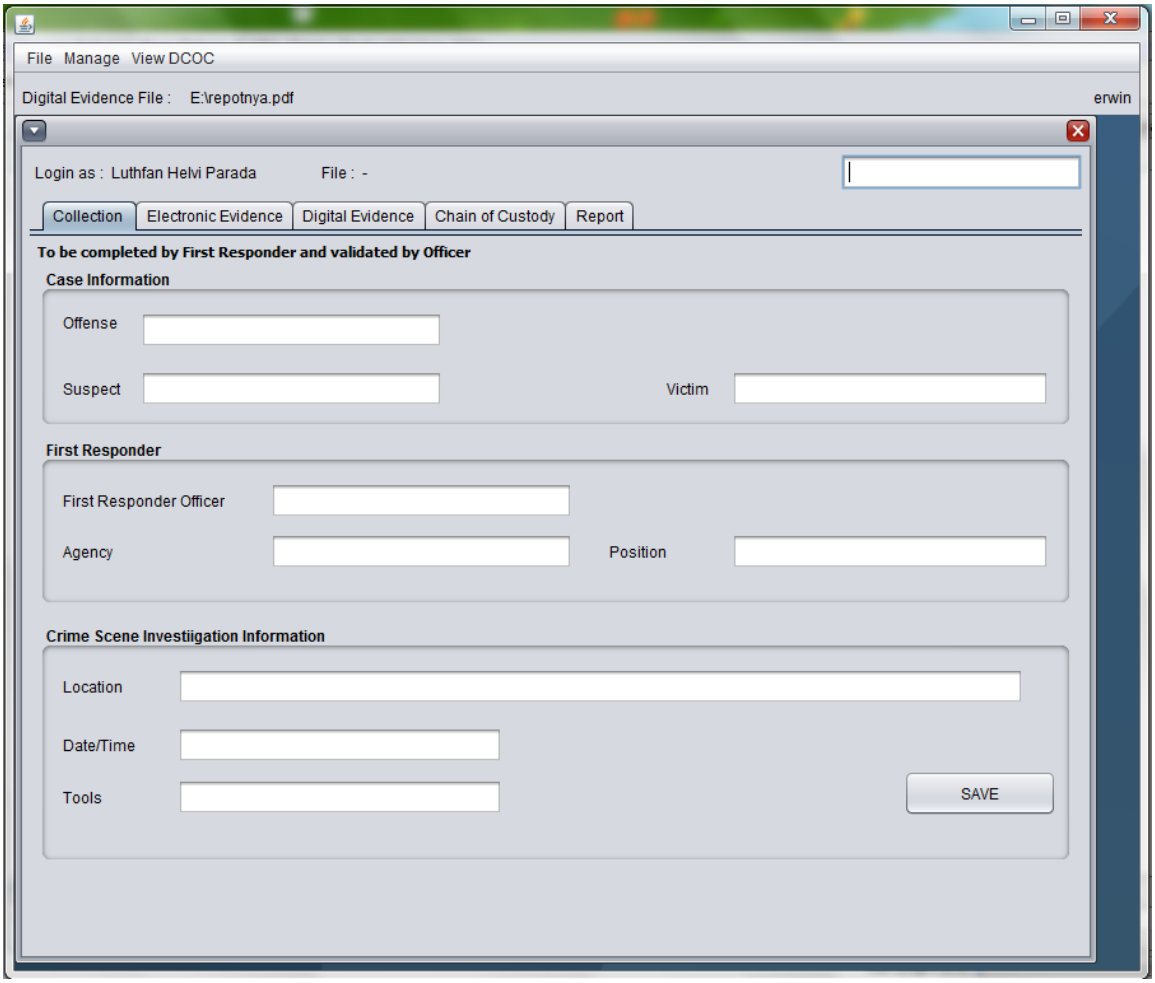
Merupakan tampilan jendela ketika *user* memuat *file* bukti digital dari tempat penyimpanan (*cabinet*) ke dalam aplikasi DCOC. Untuk memuat *file*, *user* harus memilih menu *file*→*open*.



Gambar 5. 7 Halaman Memuat *File* Bukti Digital

❖ Tampilan Manajemen *Field* Informasi Metadata *Chain Of Custody* (Informasi Olah TKP)

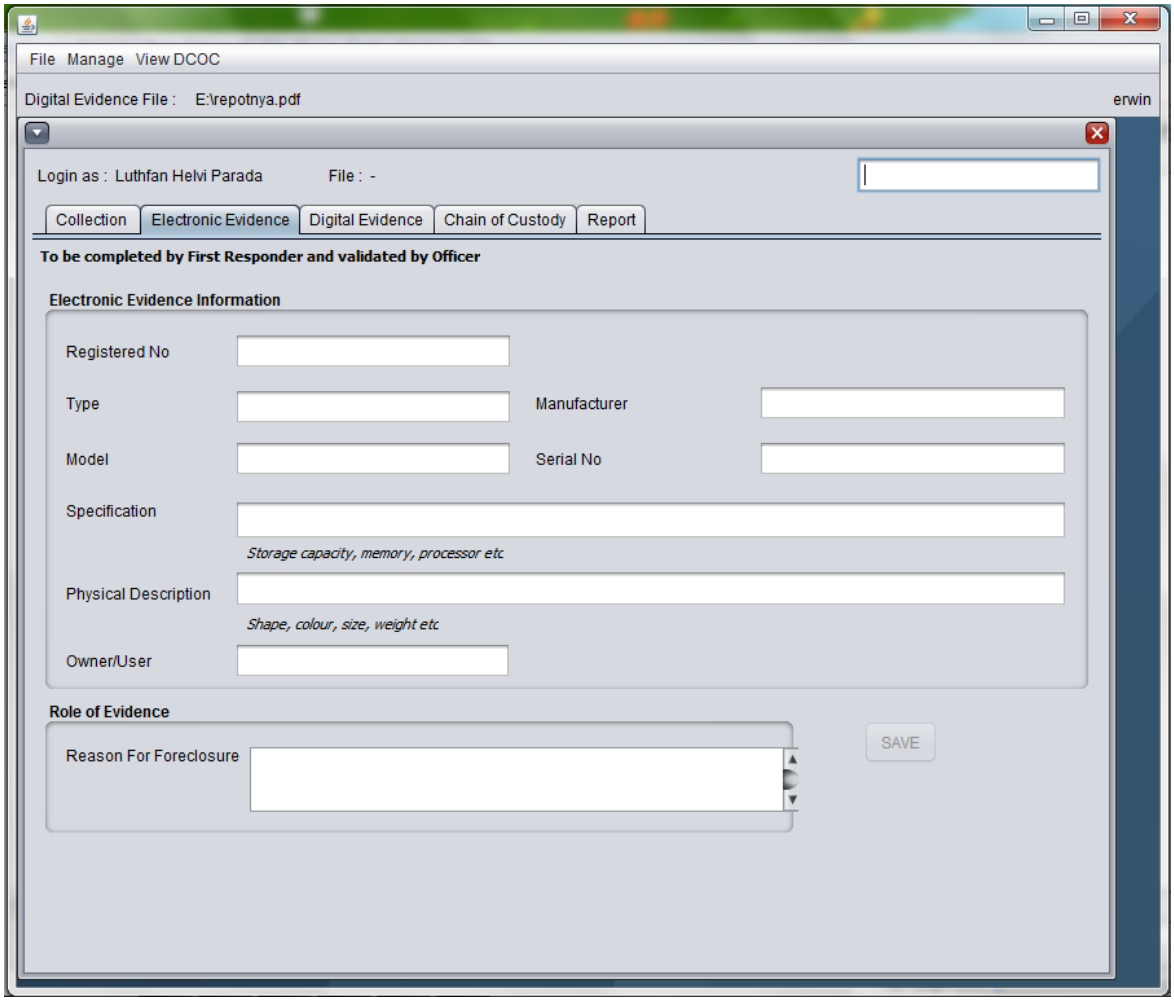
Merupakan halaman yang muncul setelah *file* bukti digital dimuat ke dalam aplikasi DCOC. Di halaman ini tab yang terbuka adalah tab untuk informasi Olah TKP. *User* dapat memasukkan dan menyimpan informasi *chain of custody* untuk informasi Olah TKP, informasi kasus dan informasi *first responder* melaui *field* yang telah ada. Pada Gambar 5. 8 merupakan tampilan manajemen *chain of custody* untuk *user* sebagai "*first responder*". Dimana tab yang ada adalah *Collection*, *Electronic Evidence*, *Digital Evidence*, *Download* dan *Report*.



Gambar 5. 8 Halaman Manajemen COC Informasi Olah TKP

❖ Tampilan Manajemen *Field* Informasi Metadata *Chain Of Custody* (Informasi Bukti Elektronik)

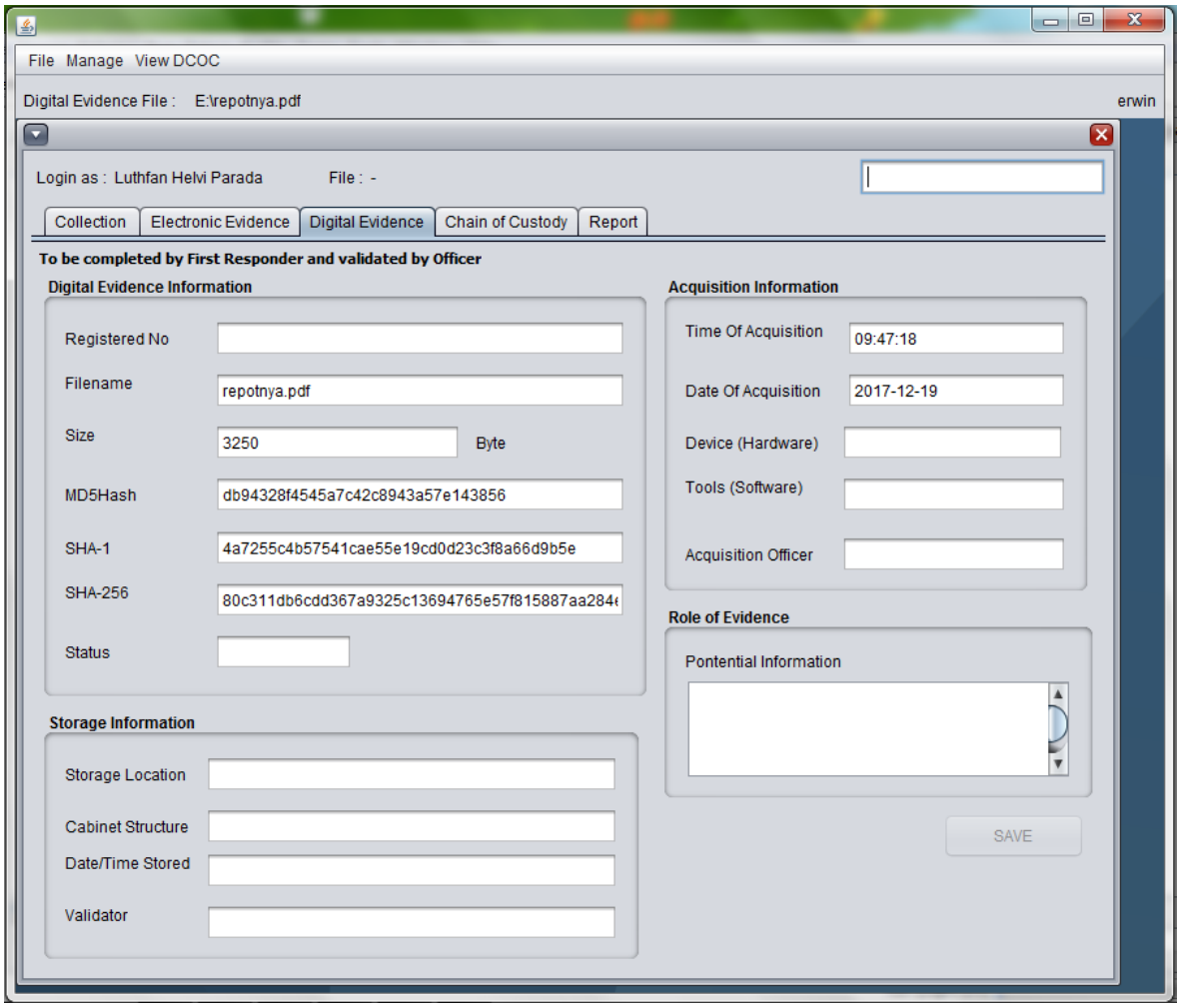
Merupakan tampilan halaman manajemen *chain of custody* bukti digital untuk memasukkan dan menyimpan informasi bukti elektronik dan *role of evidence*.



Gambar 5. 9 Halaman Manajemen COC Informasi Bukti Elektronik

❖ Tampilan Manajemen *Field* Informasi Metadata *Chain Of Custody* (Informasi Bukti Digital)

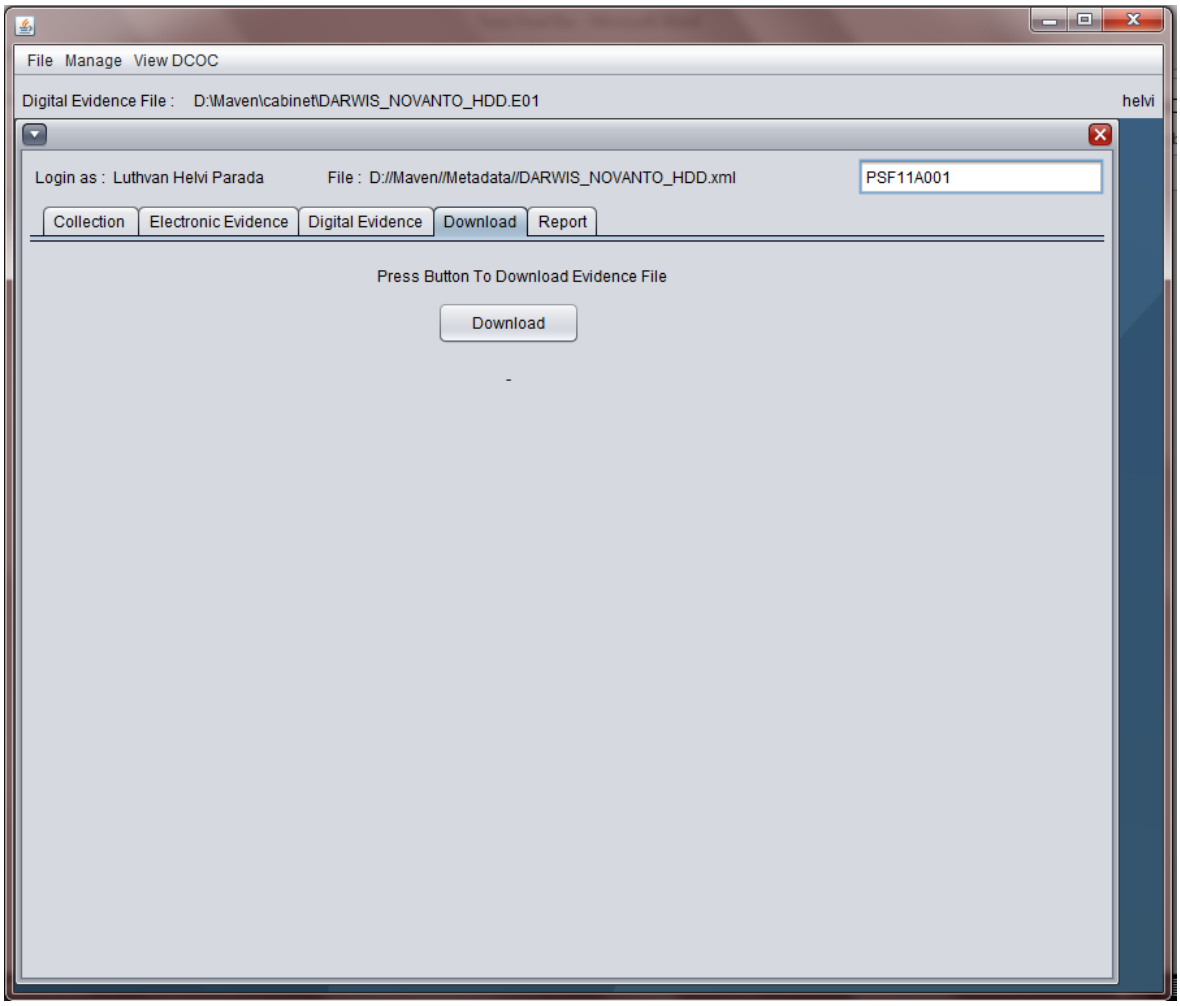
Merupakan tampilan halaman manajemen *chain of custody* bukti digital untuk memasukkan dan menyimpan informasi bukti digital, informasi akuisisi, penyimpanan dan *role of evince*. Beberapa *field* informasi secara otomatis akan mengambil dari informasi *file* bukti digital dan tidak dapat diubah yaitu *field filename*, *size*, *hash value* dan *date created file*.



Gambar 5. 10 Halaman Manajemen COC Informasi Bukti Digital

❖ Tampilan Manajemen *Field* Informasi Metadata *Chain Of Custody* (*Download File* Digital)

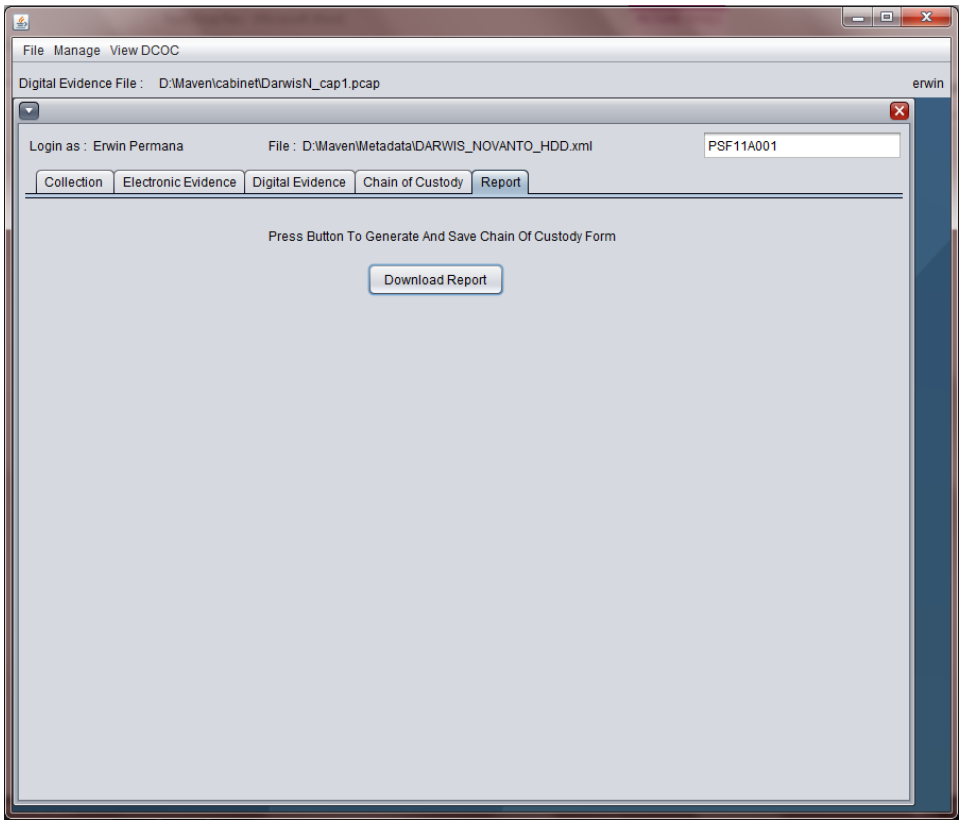
Merupakan tampilan halaman untuk *first responder* apabila ingin mengunduh *file* bukti digital. Sebelum mengunduh *file* bukti digital, *first responder* harus melakukan *request download* kepada *administrator* atau pihak pengelola untuk mendapatkan akses terhadap sebuah *file* bukti digtal.



Gambar 5. 11 Halaman *Download File* Bukti Digital

❖ Tampilan Manajemen *Field* Informasi Metadata *Chain Of Custody* (Informasi Bukti Digital)

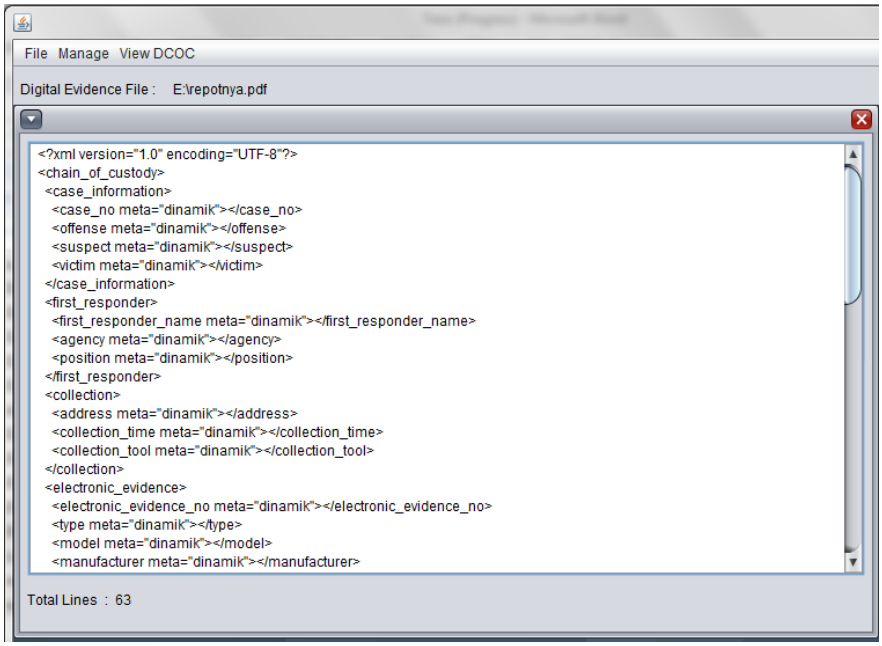
Merupakan tampilan halaman untuk mencetak laporan (*report*) *chain of custody file* bukti digital. Laporan yang dicetak adalah berupa formulir dengan ekstentensi .pdf.



Gambar 5. 12 Halaman *Download Report* Formulir *Chain Of Custody*

❖ Tampilan Halaman *View* XML *File*

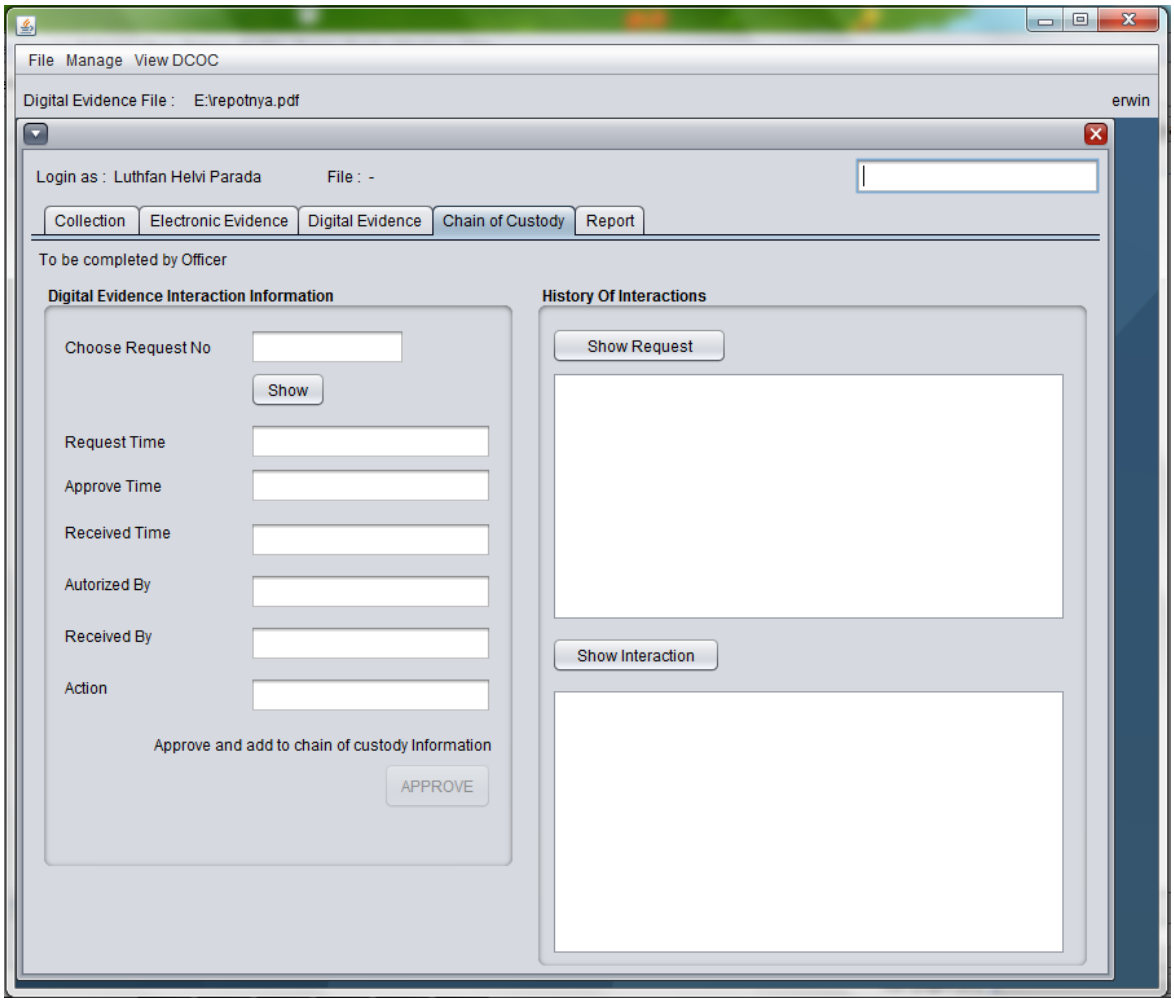
Merupakan halaman yang menampilkan isi dari suatu *file* metadata *chain of custody* struktur XML



Gambar 5. 13 Halaman *View* Metadata *Chain Of Custody*

❖ Tampilan Halaman *Chain Of Custody*

Halaman *Chain Of Custody* merupakan halaman yang akan muncul apabila *user* login adalah sebagai petugas pengelola (*administrator*). Pada halaman ini akan ditampilkan permintaan *download* dari *first responder*. Admin akan melakukan *approve* terhadap permintaan tersebut dan nilai *field approve time* dan *received time* akan secara otomatis berubah berdasarkan waktu dari sistem. Secara ilustrasi *first responder* telah mengunduh *file* bukti digital dan telah di dokumentasikan di dalam interaksi *file* metadata *chain of custody*.



Gambar 5. 14 Tampilan Halaman *Chain Of Custody*

❖ Struktur Informasi *File* Metadata *Chain Of Custody*

Berikut merupakan isi/konten *file* metadata *chain of custody* dari hasil percobaan yang dilakukan pada sebuah *file* bukti digital menggunakan aplikasi DCOC.

Tabel 5. 1 Hasil *File* Dokumentasi Manajemen *Chain Of Custody*

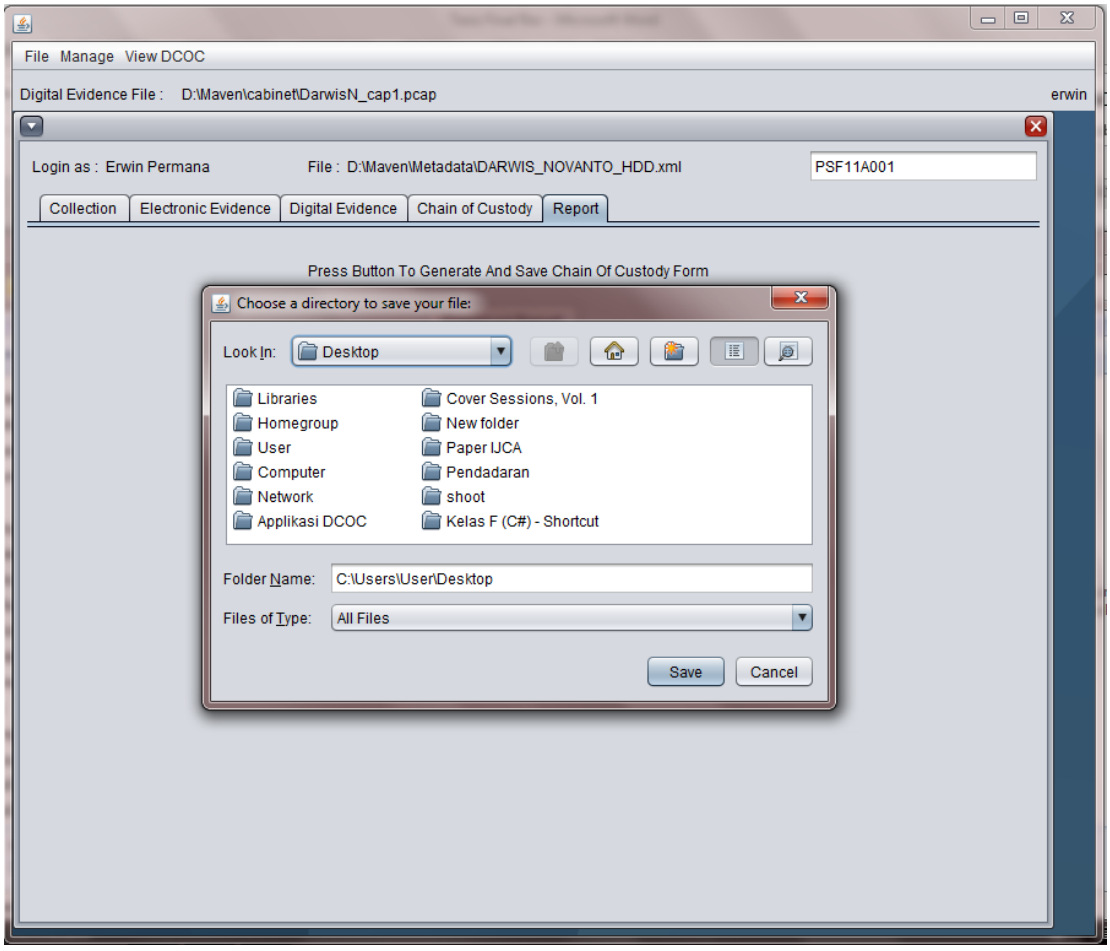
```
1. <?xml version="1.0" encoding="UTF-8"?>
2. <chain_of_custody>
3. <case_information>
4. <case_no meta="dinamik"></case_no>
5. <offense meta="dinamik"></offense>
6. <suspect meta="dinamik"></suspect>
7. <victim meta="dinamik"></victim>
8. </case_information>
9. <first_responder>
10.      <first_responder_name meta="dinamik"></first_responder_name>
11.      <agency meta="dinamik"></agency>
12.      <position meta="dinamik"></position>
13.      </first_responder>
14.      <collection>
15.      <address meta="dinamik"></address>
16.      <collection_time meta="dinamik"></collection_time>
17.      <collection_tool meta="dinamik"></collection_tool>
18.      </collection>
19.      <electronic_evidence>
20.      <electronic_evidence_no
   meta="dinamik"></electronic_evidence_no>
21.      <type meta="dinamik"></type>
22.      <model meta="dinamik"></model>
23.      <manufacturer meta="dinamik"></manufacturer>
24.      <serial_no meta="dinamik"></serial_no>
25.      <spesification meta="dinamik"></spesification>
26.      <physical_description meta="dinamik"></physical_description>
27.      <owner meta="dinamik"></owner>
28.      </electronic_evidence>
29.      <role_of_evidence>
30.      <reason_for_foreclose meta="dinamik"></reason_for_foreclose>
31.      <potential_information
   meta="dinamik"></potential_information>
32.      </role_of_evidence>
33.      <digital_evidence>
34.      <digital_evidence_no meta="dinamik"></digital_evidence_no>
35.      <filename meta="statik"></filename>
36.      <size meta="statik"></size>
37.      <md5 meta="statik"></md5>
38.      <sha1 meta="statik"></sha1>
39.      <sha256 meta="statik"></sha256>
40.      <status meta="dinamik"></status>
41.      </digital_evidence>
42.      <acquisition>
43.      <acquisition_time meta="statik"></acquisition_time>
44.      <acquisition_date meta="statik"></acquisition_date>
45.      <device meta="dinamik"></device>
46.      <acquisition_tool meta="dinamik"></acquisition_tool>
47.      <acquisition_officer meta="dinamik"></acquisition_officer>
48.      </acquisition>
49.      <storage>
50.      <storage_location meta="dinamik"></storage_location>
51.      <cabinet_structure meta="dinamik"></cabinet_structure>
```

Tabel 5. 2 Hasil *File* Dokumentasi Manajemen *Chain Of Custody* Lanjutan

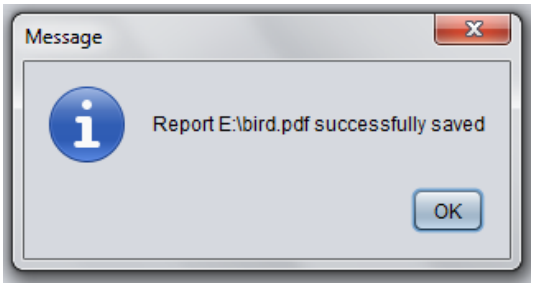
```
52.       <time_stored meta="dinamik"></time_stored>
53.       <validator meta="dinamik"></validator>
54.       </storage>
55.       <chain_of_interactions>
56.       <request_time meta="dinamik"></request_time>
57.       <approve_time meta="dinamik"></approve_time>
58.       <received_time meta="dinamik"></received_time>
59.       <autorized_by meta="dinamik"></autorized_by>
60.       <received_by meta="dinamik"></received_by>
61.       <action meta="dinamik"></action>
62. </chain_of_interactions>
```

❖ Tampilan Halaman *Report*

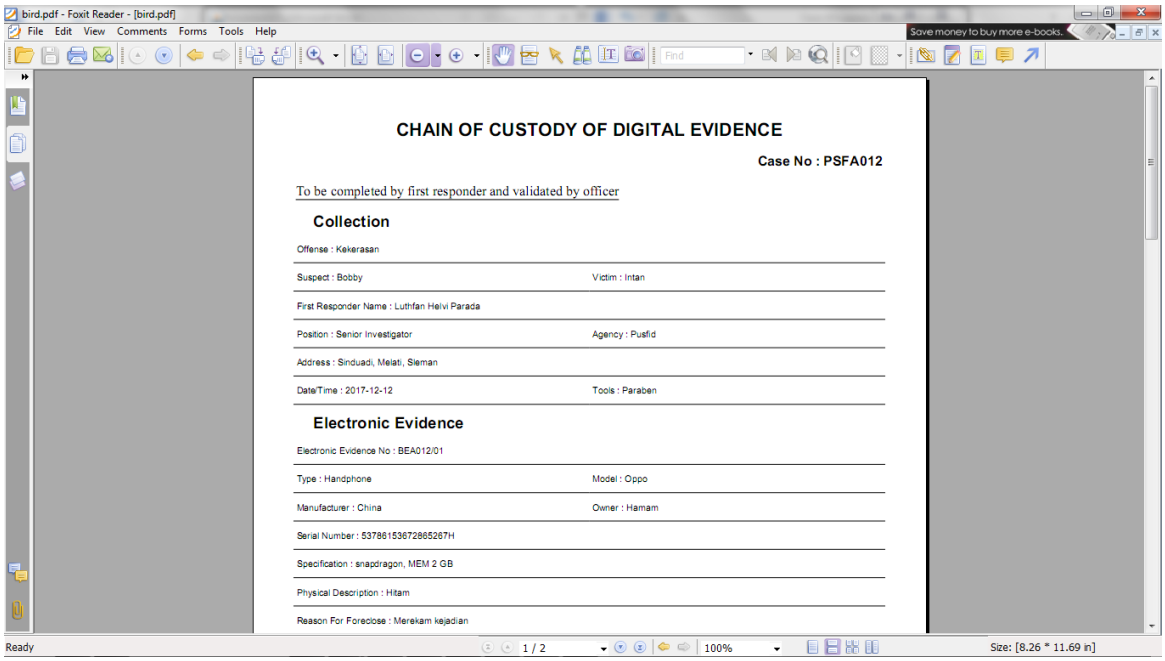
Halaman *report* merupakan halaman yang akan muncul pada saat *user* memilih Tab *Report*. Untuk mengunduh *report*/laporan formulir *chain of custody* bukti digital yang bersangkutan, *user* terlebih dahulu menekan tombol "*Download Report*", selanjutnya *user* diminta untuk memilih lokasi penyimpanan dan nama *file report* tersebut. Dengan menekan tombol "*Save*" maka secara otomatis sistem akan malakukan *generate* laporan formulir *chain of custody* dalam format .pdf seperti pada Gambar 5. 17.



Gambar 5. 15 Tanpilan Halaman *Report*



Gambar 5. 16 Tampilan Konfirmasi Penyimpanan *Report*



Gambar 5. 17 Tampilan Hasil *Download Report*

5.2 Pengujian Model Informasi Metadata

Pemodelan informasi metadata *chain of custody* untuk bukti digital menggunakan dua pengujian diantaranya pengujian secara konseptual dan pengujian secara fungsional.

5.2.1 Pengujian Konseptual Model Informasi Metadata

Pengujian secara konseptual bertujuan untuk mengetahui apakah kualitas dan kuantitas informasi metadata dokumentasi *chain of custody* telah memenuhi kriteria informasi sesuai dengan kebutuhan *chain of custody* untuk bukti digital dan dapat mudah dipahami.

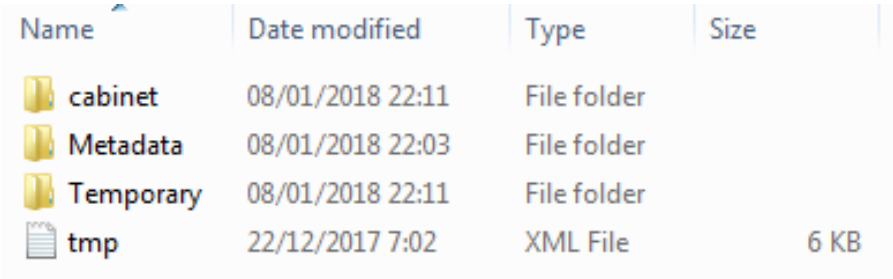
Dalam penerapannya, salah satu skenario yang digunakan adalah misalnya terdapat sebuah kasus kejahatan komputer (*Cybercrime*) dengan hasil olah TKP ditemukan 4 barang bukti elektronik diantaranya laptop, USB *flashdrive*, ponsel dan desktop serta 2 *file* bukti

langsung yang dilaporkan kepada petugas. Proses akuisisi yang dilakukan dan *entry* data ke dalam sistem DCOC adalah sebagaimana pada Tabel 5.3:

Tabel 5.3 Barang Bukti Kasus Kejahatan Komputer (*Cybercrime*)

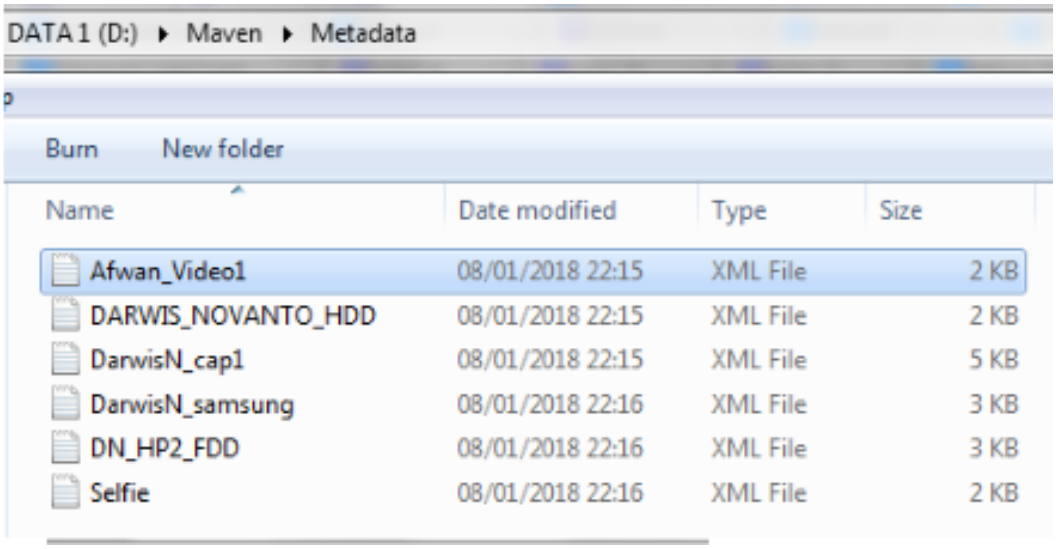
No	**Electronic Evidence**	**Acquisition and Disk Imaging**	**Tools**	**Digital Evidence**	**Integrity MD5**	**Digital *Chain of Custody***
1	Laptop Asus	*Offline*	Encase	DARWIS_NOVANTO_HDD.E01	d03544bada024056a521a41298b4051d	DARWIS_NOVANTO_HDD.xml
2	USB	*Offline*	FTK	DN_HP2_FDD.dd	5f800f3cf7660885fccb1cf012a6b29f	DN_HP2_FDD.xml
3	Ponsel	*Offline*	XRY	DarwisN_samsung.xry	2e6a6dac2195eab1e1ed2e8fc957dfbe	DarwisN_samsung.xml
4	Desktop	*Online*	Wireshark	DarwisN_cap1.pcap	40e7e81ae206f291b531c9252132d7ab	DarwisN_cap1.xml
5		-	-	Selfie.jpg	195d5e069d225ebb7adf565a0cefd18a	Selfie.xml
6		-	-	Afwan_Video1.mp4	df6133f4b68a12ebf3a88db51a679abe	Afwan_Video1.xml

Capture dari folder untuk letak penyimpanan bukti digital dan *file* digital dokumentasi *chain of custody* sebagai mana pada Tabel No dapat dilihat pada Gambar 5. 18 dan Gambar 5. 19.



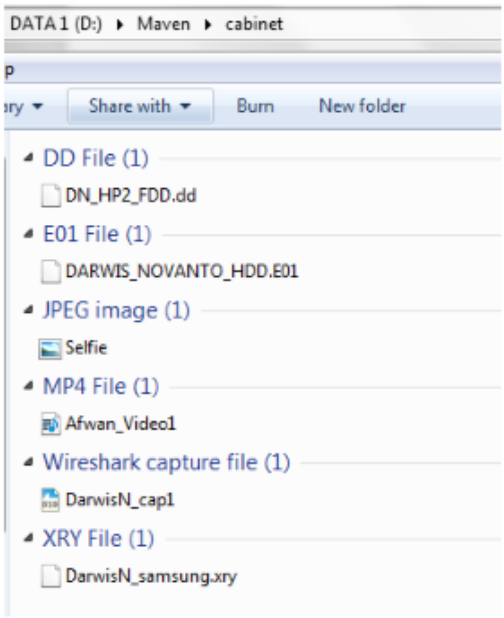
Gambar 5. 18 Susunan Direktori Penyimpanan Aplikasi Digital *Chain Of Custody*

Pada Gambar 5.18 menunjukkan susunan penyimpanan aplikasi yang terdiri dari tiga direktori yaitu "*Cabinet*", "Metadata" dan "Temporary" serta satu *file* "tmp.xml". Direktori "*Cabinet*" berisi seluruh *file* bukti digital. Direktori "Metadata" berisi seluruh *file chain of custody* dari *file* bukti digital yang telah di-*approve* oleh *officer*. Direktori "Temporary" berisi seluruh *file chain of custody* yang di-*entry* oleh *first responder* dan belum di-*approve* oleh *officer*. Sedangkan *file* tmp.xml berisi *tag* XML yang menyimpan riwayat interaksi (*download*) barang bukti.



Gambar 5. 19 Penyimpanan *File* Bukti Digital

Gambar 5.19 merupakan isi dari direktori "Metadata". Direktori ini berisi enam *file chain of custody* dengan format .xml. Seluruh *file chain of custody* merupakan dokumentasi dari *file* bukti bukti digital yang digunakan di dalam kasus ini. Nama *file chain of custody* diambil dari nama *file* bukti digital. Satu *file chain of custody* menunjukkan dokumentasi dari satu *file* bukti digital.



Gambar 5. 20 Penyimpanan *File Chain Of Custody*

Gambar 5.20 menunjukkan isi dari direktori "*Cabinet*". Direktori ini berisi seluruh *file* bukti digital yang digunakan di dalam kasus. Terdapat enam *file* bukti digital dengan format *file* yang berbeda-beda seperti .dd, .E01, .jpeg, .mp4, .pcap dan .xry sesuai dengan sknerario kasus yang digunakan.

Untuk mengetahui apakah pemetaan informasi telah sesuai dengan kebutuhan informasi untuk *digital chain of custody*, maka salah satu mekanisme yang dapat digunakan adalah pencocokan dengan kebutuhan informasi *chain of custody* sebagaimana yang terdapat pada dokumen ISO/IEC 27037. Dokumen ISO/IEC 27037 tersebut dipilih karena merupakan dokumen standar nasional sebagai pedoman dalam melakukan identifikasi, pengumpulan, akuisisi dan preservasi bukti digital.

Hasil pemetaan yang dilakukan dari 42 informasi *chain of custody* terhadap kebutuhan informasi *chain of custody* pada ISO/IEC 27037 adalah sebagaimana pada Tabel 5.4. Tidak semua informasi yang telah diidentifikasi termasuk ke dalam salah satu dari ketujuh kategori pada acuan. Informasi yang tidak termasuk di dalam tabel pemetaan ISO/IEC 27037 merupakan informasi sebagai pengayaan *field* informasi untuk dokumentasi *chain of custody*. *Field* informasi yang tidak termasuk di dalam tabel pemetaan *diantaranya offense, suspect, victim, model, type, manufacturer, spesification, physical description, owner, reason for foreclose, potential information, cabinet structure, acquisition tools* dan *acquisition device*.

Tabel 5.4 Pemetaan Informasi Berdasarkan SNI 27037

No	**Acuan ISO 27037:2014**	**Pemetaan Informasi**	
		Statis	**Dinamis**
1	Penanda/pengenal yang bersifat unik dari barang bukti	*Filename*	*Case No, Electronic Evidence No, Digital Evidence No* *Serial Number*
2	Siapa yang mendapatkan dan mengakses barang bukti, kapan waktu nya dan dimana lokasi nya		*First Responder Name, Position, Agency*
			Date/Time (Collection) Address, Tools
3	Siapa yang memeriksa masuk dan keluar nya barang bukti dari fasilitas penyimpanan dan kapan aktivitas tersebut terjadi		*Validator, Autorized By*
			Time Strored, Request Time, Approve Time, Received Time
			Storage Location
4	Mengapa barang bukti dikeluarkan dari fasilitas penyimpanan (kondisi dan tujuan) serta pihak yang memiliki hak/otoritas.		*Action, Received By*
5	Informasi yang dapat menunjukkan bahwa barang bukti telah atau tidak mengalami perubahan	*Size*, MD5, SHA1, SHA256	
6	*Lifetime of the evidence*	*Acquisition Time, Date Acquisition*	*Status*
7	Pihak yang bertanggungjawab dalam menangani barang bukti digital		*Acquisition Officer*

Metode lain yang dapat digunakan untuk mengukur kualitas dari pengelompokan informasi dan desain formulir *chain of custody* adalah dengan penilaian responden menggunakan angket/kuesioner. Pengukuran menggunakan angket/kuesioner diharapkan dapat menunjukkan respon dari calon pengguna terhadap hasil penelitian yang dilakukan. Penelitian ini memilih menggunkan skala likert untuk membantu dalam menyusun pertanyaan/pernyataan dan memperoleh jawaban dari responden. Responden diminta untuk memilih salah satu dari lima pilihan jawaban dengan jenjang (skala 1 sampai 5) yang tersusun sebagai berikut :

- Sangat tidak setuju (1)
- Tidak setuju (2)
- Antara setuju/Tidak setuju/Netral (3)
- Setuju (4)
- Sangat setuju (5)

Responden harus menilai apakah setuju atau tidak setuju terhadap beberapa pertanyan/pernyataan tentang informasi di dalam formulir dan pengelompokan informasi di dalamnya. Susunan pertanyaan/pernyataan tersebut digunakan untuk mengetahui apakah informasi yang telah diidentifikasi dari penelitian telah memenuhi kebutuhan informasi untuk dokumentasi *chain of custody* untuk bukti digital apabila diterapkan secara nyata. Kuesioner ini mutlak sesuai dengan ilmu pengetahuan responden dan tidak ada paksaan atau sejenisnya.

Kuisoner diterapkan secara online dengan pelaksanaan dimulai pada bulan Desember 2017 sampai bulan januari 2018. Terdapat sebanyak 10 responden yang ikut berpartisipasi dari berbagai bidang pekerjaan dan memiliki latar belakang ilmu dibidang digital forensik. Tabel 5.5 merupakan daftar responden yang turut berpartisipasi dalam penelitian ini.

Tabel 5. 5 Daftar Responden

No	Nama	Latar Belakang Pekerjaan
1	Pratomo Djati Nugroho	Dosen
2	Afiyati	Dosen
3	M. Ibrahim Adha	Pengacara
4	Hudi	Kepala Seksi
5	Mirza Rahadian	Staf bidang Digital Forensik
6	Yolly Rinaldi	Junior Manager IT Security
7	Mukhlis Prasetyo Aji	Dosen
8	Ardiyansyah	Pelaksana
9	Tri Widodo	Dosen
10	Andritona Munaf	Konsultan

Obyek yang menjadi penilaian di dalam kuesioner adalah kelompok informasi dan formulir *chain of custody* sebagaiamana output dari penelitian yang dilakukan. Tabel 5. 6 merupakan hasil penilaian responden terhadap sepuluh poin pernyataan/pertanyaan yang diajukan. Poin-poin pernyataan yang ada mewakili kriteria dari kelompok informasi maupun formulir dan menunjukkan bagaimana responden menilai kualitas informasi sesuai dengan pengalaman dan pengetahuan dari responden. Hasil yang diperoleh dari penerapan kuesioner yang telah disebarkan ternyata rata-rata responden menjawab setuju terhadap pertanyaan/pernyataan yang dihadirkan. Hal tersebut dapat dibuktikan oleh Tabel 5. 6 yang menunjukkan persentase dari setiap pertanyaan/pernyataan pada kuesioner tersebut. Dari pernyataan dan makna dari setiap angka pada tabel tersebut adalah 1 = sangat tidak setuju, 2 = tidak setuju, 3 = netral/tidak berpendapat, 4 = setuju dan 5 = sangat setuju.

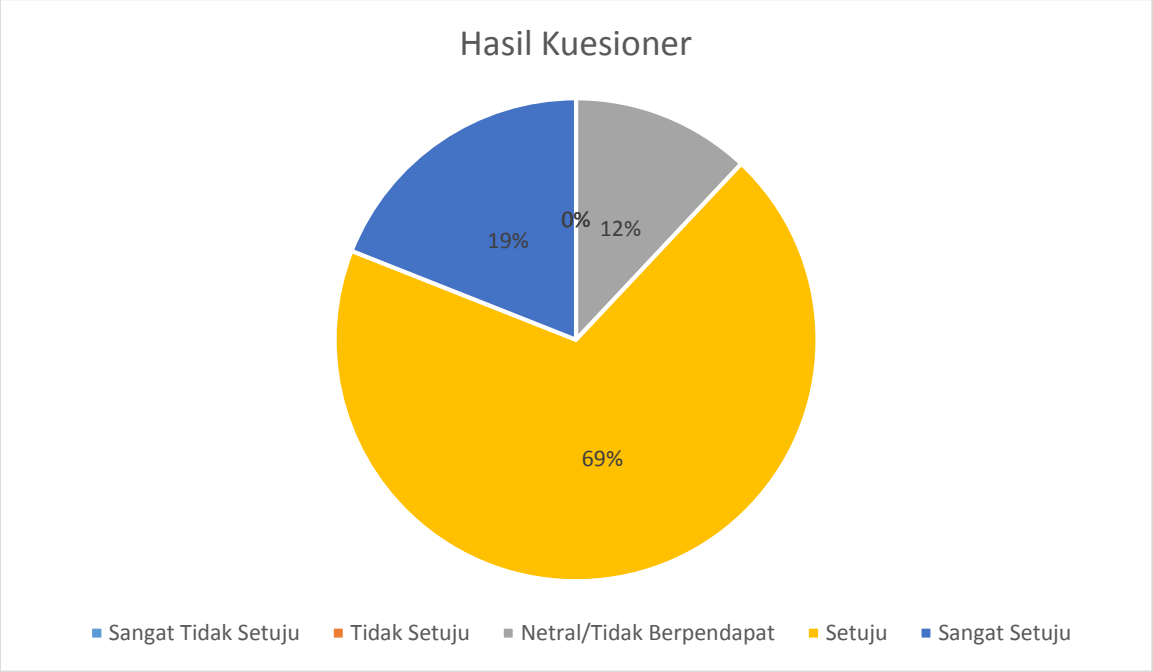
Tabel 5. 6 Hasil Penilaian Menggunakan Kuesioner

No	**Pertanyaan / Pernyataan**	**Skala Penilaian**				
		1	**2**	**3**	**4**	**5**
1	Kelompok informasi yang terdapat di dalam gambar tersebut sudah cukup memenuhi kebutuhan informasi *chain of custody* bukti digital	0%	0%	10%	70%	20%
2	Informasi yang ada pada formulir sudah cukup lengkap dalam mendokumentasikan tahapan *chain of custody* bukti digital	0%	0%	10%	80%	10%
3	Informasi yang ada pada formulir tersebut sudah cukup baik dalam mendokumentasikan interaksi terhadap barang bukti digital	0%	0%	10%	70%	20%
4	Informasi yang ada pada formulir sudah cukup lengkap dalam mendokumentasikan individu yang terlibat dengan bukti digital	0%	0%	20%	70%	10%
5	Informasi yang ada pada formulir sudah cukup baik dalam mendokumentasikan nilai integritas dan keamanan bukti digital	0%	0%	30%	50%	20%
6	Informasi yang ada pada formulir sudah mencakup informasi 5W+1H yaitu apa, siapa, mengapa, dimana, kapan dan bagaiamana terkait dengan barang bukti digital digital	0%	0%	0%	70%	30%

Tabel 5. 7 Hasil Penilaian Menggunakan Kuesioner Lanjutan

No	Pertanyaan / Pernyataan	Skala Penilaian				
		1	2	3	4	5
7	Kelompok informasi yang ada pada Gambar tersebut sudah memuat elemen informasi yang sesuai	0%	0%	10%	70%	20%
8	Informasi yang dimuat di dalam formulir dapat dengan mudah dipahami	0%	0%	20%	50%	30%
9	Pengelompokan informasi pada Gambar sudah mendeskripsikan bukti digital dengan baik dan mudah dipahami	0%	0%	10%	70%	20%
10	Formulir tersebut dapat diimplementasikan untuk mendokumentasikan *chain of custody* bukti digital	0%	0%	0%	90%	10%

Apabila hasil penilaian pada Tabel 5. ***6*** dan Tabel 5.7 diambil nilai rata-rata dari sepuluh poin pernyataan yang ada maka diperoleh nilai rata-rata nya adalah 0% responden menilai sangat tidak setuju dan tidak setuju, 12% responden netral/tidak memberikan pendapat serta 69% responden menilai setuju dan 19% responden menilai sangat setuju. Dengan hasil tersebut menunjukkan bahwa 88% responden setuju dan sangat setuju terhadap output/hasil dari penelitian. Nilai rata-rata hasil kuesioner/angket dapat ditunjukkan dalam grafik pada Gambar 5.21.



Gambar 5. 21 Grafik Hasil Pengujian Kuesioner

5.2.2 Pengujian Fungsional Model Informasi Metadata

Pengujian secara fungsional dilakukan untuk mengetahui bahwa model informasi metadata untuk *chain of custody* yang telah dibuat dapat diterapkan secara fungsional ke dalam sebuah aplikasi *Digital Chain Of Custody*. Di dalam model informasi metadata yang telah dibuat, dokumentasi informasi penyimpanan barang bukti adalah menggunakan pendekatan framework *Digital Evidence Cabinet.* Penelitian ini mengimplementasikan model informasi metadata menggunakan aplikasi berbasis Desktop. Sehingga *Digital Evidence Cabinet* diasumsikan sebagai sebuah *drive* penyimpanan yang memiliki *space* untuk menyimpan *file* bukti digital (*cabinet*) dan *file* metadata (*container of metadata*) secara terpisah.

5.3 Analisis & Pembahasan

❖ **Kebutuhan Informasi Dalam Manajemen *Chain Of Custody***

Dalam melakukan manajemen *chain of custody,* kebutuhan informasi untuk formulir dokumentasi bukti digital memiliki kesamaan dengan kebutuhan informasi untuk dokumentasi bukti elektronik. Kebutuhan informasi yang harus terpenuhi tersebut harus dapat menjawab pertanyaan 5W+1H yaitu apa, siapa, kapan, dimana, mengapa dan bagaimana terkait dengan barang bukti. Penelitian ini telah menjabarkan ketentuan dasar yang digunakan sebagai acuan untuk dapat mendekomuentasikan kebutuhan 5W+1H serta agar informasi yang dihasilkan dapat relevan dengan kebutuhan *chain of custody* untuk bukti digital. Diantara dasar acuan yang digunakan adalah kebutuhan fungsional *chain of custody*, model bisnis *chain of custody* dan *legal standard* manajemen *chain of custody*. Kebutuhan fungsional *chain of custody* adalah bahwa dokumentasi *chain of custody* hanya akan berubah apabila terjadi interaksi dengan barang bukti digital. Pendekatan model bisnis *chain of custody* yang digunakan adalah menggunakan konsep metadata dan *digital evidence cabinet* seperti pada Gambar 4.1. Sedangkan untuk *legal standard* disesuaikan dengan aturan hukum yang berlaku di Indonesia yang mengatur tentang prosedur pengelolaan barang bukti di lingkugan kepolisian yaitu Perkap No 10 Tahun 2010. Selain itu, untuk memudahkan dalam melakukan identifikasi kebutuhan informasi metadata, penelitian ini juga melakukan studi terhadap berbagai literatur yang membahas tentang kebutuhan umum informasi *chain of custody* baik untuk barang bukti digital maupun untuk barang bukti elektronik. Hasil dari aktivitas studi literatur kebutuhan informasi *chain of custody* tersebut telah dipetakan ke dalam Tabel 4.7, Tabel 4. 8 dan Tabel 4. 9 dimana terdapat enam belas kebutuhan informasi

chain of custody. Dari seluruh kebutuhan informasi yang ada kemudian disederhanakan menjadi sembilan kebutuhan informasi *chain of custody* barang bukti diantaranya *case information, collection information, acquisition, electronic evidence description, image description, storage information, personel information, role of evidence* dan *interaction*.

Pada penelitian ini, identifikasi *field* informasi *chain of custody* di dapatkan dengan melakukan ekstraksi terhadap *field* informasi yang ada pada lima formulir *chain of custody.* Formulir tersebut diperoleh dari sumber internet. Dari kelima formulir tersebut diantaranya adalah formulir dari University *of* Pennsylvenia, Audit West, NIST (*National Institute of Standards and Technology*), Digital Forensics Lab dan PVL Forensics. Untuk hasil ekstraksi *field* informasi kelima formulir tersebut telah dipetakan berdasarkan sembilan kelompok kebutuhan informasi pada Tabel 4.10, Tabel 4. 11, Tabel 4. 12 dan Tabel 4. 13. Selain itu untuk menentukan *field* informasi yang relevan dengan kebutuhan informasi *chain of custody* untuk bukti digital, penelitian ini melakukan normalisasi terhadap *field* informasi yang diperoleh dari tahap ekstraksi. Proses normalisasi yang dilakukan adalah dengan menggunakan *field* informasi yang dianggap sesuai, mengeliminasi *field* informasi yang dianggap tidak sesuai dan menambahkan beberapa *field* informasi yang dianggap masih kurang untuk mendokumentasikan informasi *chain of csutody* untuk bukti digital. Dari hasil ekstraksi dan normalisasi yang dilakukan dihasilkan total 42 *field* informasi yang dibutuhkan untuk dokumentasi *chain of custody* untuk bukti digital seperti pada Tabel 4.19, Tabel 4.20 dan Tabel 4.21

Dari keseluruhan *field* informasi yang berhasil diidentifikasi sudah mencakup kebutuhan informasi untuk manajemen *chain of custody* sebagaimana yang terdapat di dalam dokumen ISO/IEC 27037. Hal tersebut sesuai dengan pemetaan pada Tabel 5.4. Terdapat 7 poin kebutuhan informasi menurut ISO 27037 diantaranya tentang identitas barang bukti, siapa yang mengakses, kapan dan dimana diambilnya barang bukti, mengapa barang bukti perlu diakses, nilai integritas bukti yang dapat menunjukkan bahwa bukti tidak berubah/rusak, informasi *lifetime* bukti dan pihak-pihak yang bertanggung jawab terhadap barang bukti. Dari seluruh kebutuhan informasi yang ada telah dipetakan *field* informasinya ke dalam informasi statis dan informasi dinamis berdasarkan acuan tersebut.

Pengujian menggunakan kusesioner pada Tabel 5.6 dan Tabel 5. *7* menunjukkan bahwa bahwa rata-rata persentase respon yang diperoleh adalah hampir 69% responden menyatakan setuju terhadap pernyataan yang diajukan, 19% sangat setuju dan 12% tidak berpendapat/netral. Sementara tidak ada responden yang menyatakan tidak setuju atau

sangat tidak setuju. Pada poin pernyataan 1 sebanyak 70% menyatakan setuju dan 20% menyatakan sangat setuju bahwa kelompok informasi yang telah diidentifikasi sudah cukup memenuhi kebutuhan dokumentasi *chain of custody* bukti digital. Pada poin pernyataan 2 sampai 6 rata-rata lebih dari 80% responden menyatakan setuju atau sangat setuju dan sisanya tidak berpendapat dan sebanyak 0% menyatakan tidak setuju. Poin 2 sampai 6 tersebut menunjukkan bahwa kelompok informasi yang telah diidentifikasi sudah cukup lengkap dalam mendokumentasikan informasi tahapan *chain of custody*, informasi interaksi, informasi individu yang terlibat, informasi integritas dan informasi 5W+1H terkait barang bukti.

❖ **Model informasi metadata *Chain Of Custody***

Model informasi metadata untuk mendukung *chain of custody* bukti digital dirancang menggunakan *field* informasi pada Tabel 4.15, Tabel 4. ***16***, Tabel 4. ***17*** dan Tabel 4. ***18***. Model informasi metadata pada penelitian ini diterapkan menggunakan konsep layaknya formulir *chain of custody* untuk barang bukti. Konsep tersebut adalah bahwa setiap elemen *field* informasi dipetakan ke dalam kelompok informasi yang relevan. Kelompok informasi tersebut merupakan sembilan kelompok informasi yang telah didentifikasi pada tahap sebelumnya diantaranya; *case information*, *collection information*, *acquisition, electronic evidence description, image description, storage information, personel information, role of evidence* dan *interaction*. Hasil dari pengelompokan *field* informasi metadata terhadap kelompok kebutuhan informasi metadata juga telah dipetakan pada Tabel 4.19, Tabel 4. ***20*** dan Tabel 4.21. Sedangkan untuk model informasi metadata beserta relasi dari masing-masing *field* informasi terhadap kelompok informasi telah digambarkan pada Gambar 4.2. Gambar 4.2 tersebut juga dapat mengidentifikasi *field* informasi berdasarkan sumber (*from*), tujuan (*to*) dan keperluan (*for*) sebagaimana model bisnis *chain of custody* yang digunakan yaitu pada Gambar 4.1. Selain itu, pada poin 7 Tabel 5. 6 sebanyak 70% menyatakan setuju dan 20% sangat setuju bahwa pengelompokan informasi yang dilakukan telah memiliki elemen-lemen informasi yang tepat atau sesuai pada setiap kelompoknya. Sebanyak 10% tidak berpendapat dan sisanya yaitu 0% tidak setuju. Pada poin pernyataan 8 dan 9 rata-rata hampir 80% setuju dan sangat setuju bila pengelompokan informasi dan formulir *chain of custody* dapat mendeskripsikan informasi dengan cukup baik dan mudah dipahami. Pada poin terakhir dari kuesioner diperoleh penilaian mencapai 90% setuju dan 10% sangat setuju apabila formulir *chain of custody* digunakan untuk mendokumentasikan *chain of custody*

bukti digital. Dari hasil rata-rata kuesioner ini menunjukkan bahwa bagi responden pengelompokan informasi dan formulir yang telah dibuat sudah cukup memenuhi kebutuhan untuk dokumentasi *chain of custody* bukti digital serta informasinya mudah untuk dipahami.

- **Bentuk implementasi model informasi metadata untuk mendukung *Chain Of Custody***

Implementasi model informasi metadata sesuai pada Gambar 4.1 adalah dengan menerjemahkan model informasi tersebut ke dalam skema *file chain of custody* .xml. Skema *file* .xml digunakan untuk menyimpan informasi dokmentasi *chain of custody* untuk satu *file* bukti digital. Skema *file* metadata .xml diterapkan menggunakan konsep metadata eksternal. Dimana *file* metadata *chain of custody* .xml tersebut merupakan *file* yang terpisah dengan *file* bukti digital namun memiliki keterkaitan. Informasi *chain of custody* yang dimuat dalam skema .xml terbagi menjadi dua kelompok informasi metadata yaitu informasi metadata statis dan informasi metadata dinamis. Informasi metadata statis merupakan informasi metadata yang diekstrak/diperoleh secara otomatis dari *file* bukti digital. Sedangkan informasi metadata dinamis merupakan informasi yang dientry secara manual oleh *user* atau diambil dari sistem. Pengelompokan informasi metadata statik dan metadata dinamik dari model informasi metadata *chain of custody* untuk bukti digital dilakukan sesuai dengan Tabel 4.19, Tabel 4. 20 dan Tabel 4.21 Selain itu, terdapat kolom yang menunjukkan spek teknis dari masing-masing *field* informasi. Spek teknis tersebut tidak digunakan dikarenakan semua data yang dimuat di dalam *file* .xml dibaca sebagai String. Spek teknis akan bermanfaat apabila model informasi yang ada diterapkan sebagai standar metadata.

Implementasi dari konsep penyimpanan *file* bukti digital dan *file* metadata eksternal *chain of custody* .XML yaitu dengan menggunakan direkrori/folder yang terpisah di dalam *drive* penyimpanan. *File-file* bukti digital disimpan di dalam satu folder tersendiri (*cabinet*) dan *file-file* dokumentasi *chain of custody* disimpan di dalam satu folder tersendiri (metadata) terpisah dengan *file* bukti digital seperti pada Gambar 5.1 dan Gambar 5.2. Sedangkan konsep penamaan *file* dokumentasi *chain of custody* .xml adalah menggunakan nama dari *file* bukti digital sesuai pada Gambar 5.3 dan Gambar 5.4.

Selanjutnya implementasi aplikasi dari model informasi metadata *chain of custody* adalah menggunakan aplikasi berbasis Desktop. Terdapat dua jenis *user* yaitu *first responder* dan *officer*. Masing-masing *user* memiliki hak akses yang berbeda sesuai pada Gambar 4.1 dimana kontrol penuh terhadap manajemen *chain of custody* dimiliki oleh *officer,* sedangkan

first responder hanya dapat melakukan entry informasi tetapi tidak termasuk pada informasi interaksi barang bukti digital seperti pada Gambar 5.7, Gambar 5.8, Gambar 5.9 dan Gambar 5.10. Selain itu, untuk dapat men*download file* bukti digital *first responder* harus mengirimkan *request download access* kepada *officer* untuk disetujui seperti pada Gambar 5.11 dan 5.14. Sedangkan *first responder* dan *officer* memiliki akses untuk melihat struktur dan informasi *file* .xml seperti pada Gambar 5.12 dan Gambar 5.13.

Pengujian model informasi metadata secara fungsional dilakukan dengan menggunakan sebuah skenario kasus berdasarkan *test case* tertentu dari aktivitas manajemen *chain of custody*. Dari hasil percobaan dan pengujian yang dilakukan menunjukkan bahwa implementasi model informasi metadata menggunakan konsep alur aplikasi *Digital Chain Of Custody* sudah sesuai dengan harapan yang ingin dicapai. Konsep ini ternyata juga tidak merubah nilai *hash file* digital yang merupakan nilai integritas barang bukti. Oleh karena itu berdasarkan analisis percobaan dan pengujian yang telah dilakukan, maka model informasi metadata *chain of custody* dengan menggunkan konsep metadata eksternal yang ditawarkan dapat menjadi salah satu solusi yang relevan untuk diterapkan dalam manajemen dokumentasi *chain of custody* bukti digital.

BAB VI
Kesimpulan & Saran

6.1 Kesimpulan

Berdasarkan analisa, implementasi aplikasi dan pengujian model informasi metadata *chain of custody* untuk mendukung manajemen *chain of custody* untuk bukti digital, maka diperoleh kesimpulan sebagai berikut :

1. Dalam melakukan manajemen *chain of custody,* terdapat 42 *field* informasi yang terbagi ke dalam sembilan kelompok kebutuhan informasi. Sembilan kelompok kebutuhan informasi tersebut diantaranya *case information, collection information, acquisition, electronic evidence description, image description, storage information, personel information, role of evidence* dan *interactions*.
2. Model informasi yang dapat digunakan di dalam metadata untuk mendukung *chain of custody* bukti digital adalah dengan merancang 42 *field* informasi yang telah diidentifikasi dan dipetakan ke dalam formulir digital berdasarkan relevansinya terhadap sembilan kelompok kebutuhan informasi *chain of custody.*
3. Salah satu bentuk implementasi yang relevan diterapkan untuk mendukung dokumentasi *chain of custody* adalah menggunakan pendekatan metadata eksternal .xml. Dalam konsep tersebut, *file* metadata *chain of custody* merupakan *file* yang berbeda/terpisah dengan *file* bukti digital. Informasi yang disimpan di dalam *file chain of custody* .xml dikategorikan berdasarkan informasi metadata statik dan informasi metadata dinamik.

6.2 Saran

Sebagai pengembangan lebih lanjut berdasarkan hasil penelitian yang telah dilakukan, maka beberapa saran yang dapat penulis cantumkan diantaranya :

1. Penelitian ini hanya menggunakan lima formulir *chain of custody* untuk menghasilkan 42 *field* informasi. Setiap instansi memiliki dokumentasi informasi *chain of custody* bukti digital yang berbeda-beda. Pada penelitian selanjutnya, untuk meningkatkan kualitas dan memperkaya informasi dokumentasi akan lebih baik apabila 42 *field* informasi yang sudah ada dapat divalidasi dan dicocokkan dengan lebih banyak formulir *chain of custody* lainnya.

2. Penelitian ini telah menguji hasil 42 *field* informasi untuk *chain of custody* bukti digital dengan memetakan informasi menggunakan dokumen SNI ISO/IEC 27037. Pada penelitian selanjutnya, agar hasil uji lebih tepat dan akurat maka akan lebih baik apabila terdapat metode atau cara lain yang dapat digunakan untuk mengukur kualitas *field* informasi yang dihasilkan agar dapat memenuhi kebutuhan *chain of custody* bukti digital.
3. Kebutuhan *Chain Of Custody* terutama untuk bukti digital akan terus meningkat. Selain itu persepsi individu tentang bagaimana penanganan *Chain Of Custody* juga akan terus berkembang. Pada penelitian selanjutnya salah satu pendekatan yang dapat digunakan dalam domain *chain of custody* adalah pendekatan berbasiskan pengetahuan (*knowledge base*).

DAFTAR PUSTAKA

Ashcroft, J., Daniels, D. J., & Hart, S. V. (2004). *Forensic Examination of Digital Evidence : A Guide for Law Enforcement*. United State *of* America. Retrieved from http://www.ojp.usdoj.gov/nij

Baca, M. (2008). *Introduction to Metadata: Second Edition* (Second). Getty Publications. Retrieved from http://www.getty.edu/publications/intrometadata/setting-the-stage/

Carrier, B. (2005). *FileSystem Forensic Analysis*. Adisson Wesley Professional.

Coons, P. (2015). How to Document Your Chain of Custody and Why It's Important. Retrieved August 28, 2015, from http://d4discovery.com

Cosic, J. (2017). Formal Acceptability of Digital Evidence. *Springer International Publishing*. http://doi.org/10.1007/978-3-319-44270-9

Cosic, J., & Baca, M. (2010a). A Framework to (Im) Prove „ Chain of Custody " in Digital Investigation Process. *Proceedings of the 21st Central European Conference on Information and Intelligent Systems.*, 435–438. http://doi.org/10.13140/RG.2.14813.9282

Cosic, J., & Baca, M. (2010b). Do We Have Full Control Over Integrity in Digital Evidence Life Cycle ?, 429–434.

Cosic, J., & Cosic, Z. (2012). Chain of custody and life cycle *of* digital evidence. *Computer Technology and Application 3*, (January 2012), 126–129.

Cosic, J., Cosic, Z., & Baca, M. (2011). An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence. *JIOS Journal of Information and Organization Science*, *35*(1), 1–13.

Dahiya, Y., & Sangwan, M. S. (2014). Developing and Enhancing the Security of Digital Evidence Bag. *International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)*, *1*(2), 14–25. Retrieved from www.arcjournal.org

Dunlap, R., Mark, L., & Rugaber, S. (2008). Earth system curator : metadata infrastructure for climate modeling, 131–149. http://doi.org/10.1007/s12145-008-0016-1

ENISA, & Andreson, P. (2014). Electronic evidence - a basic guide for First Responders (Good practice material for CERT first responders). http://doi.org/10.2824/068545

Gartner, R. (2016). *Metadata*. Switzerland: Springer. http://doi.org/10.1007/978-3-319-40893-4

Gayed, T. F., Lounis, H., & Bari, M. (2012). Cyber Forensics : Representing and (Im) Proving the Chain of Custody Using the Semantic web. In *The Fourth International Conference on Advanced Cognitive Technologies and Applications* (pp. 19–23).

Ge, H., & Rao, R. N. (2015). A business metadata modeling approach for data integration based on SDMX. *Network Security and Communication Engineering: Proceedings of the 2014 International Conference on Network Security and Communication*

Engineering (NSCE 2014), 403. http://doi.org/10.1201/b18660-90

Giova, G. (2011). Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems, *11*(1).

Graves, M. W. (2013). The Anatomy of a Digital Investigation. Retrieved August 28, 2017, from www.informit.com

Grube, P. P., Boehringer, D., Richter, T., Spiecker, C., Natho, N., Maier, C., & Zutin, D. (2011). A Metadata Model for Online Laboratories. *Ieee*, 618–622.

Kemp, S. (2017). We are social: Digital in 2017 Global Overview. Retrieved July 15, 2017, from https://es.slideshare.net/wearesocialsg/digital-in-2017-global-overview

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. *NIST Special Publication*.

Kuntze, N., Rudolph, C., Richter, J., Kuntze, N., & Rudolph, C. (2017). Securing Digital Evidence . Securing Digital Evidence, (July). http://doi.org/10.1109/SADFE.2010.31

Leintz, R. (n.d.). What is the Chain of Custody - Definition, Procedures & Importance. Retrieved July 12, 2017, from http://study.com/academy/lesson/what-is-the-*chain-of-custody*-definition-procedures-importance.html

Liu, X., & Qin, J. (2014). An Interactive Metadata Model for Structural , Descriptive ,. *Journal of the Association For Information Science and Technology*, *65*(5), 964–983. http://doi.org/10.1002/asi

Luthfi, A., & Prayudi, Y. (2015). Model Bisnis Digital Forensics Untuk Mendukung Penanganan Bukti Digital dan Investigasi Cybercrime. *Konferensi Nasional Informatika (KNIF) STIE ITB at Bandung*.

NISO. (2004). *Understanding Metadata*. United State of America: NISO Press. Retrieved from www.niso.org

Prayudi, Y. (2014). Problema Dan Solusi Digital Chain Of Custody Dalam Proses Investigasi Cybercrime. *Senasti*, (ISSN : 235-536X).

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2014). Digital Evidence Cabinets : A Proposed Framework for Handling Digital Chain of Custody. *International Journal of Computer Applications*, *107*(9), 30–36.

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2015). A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia. *I. J. Computer Network and Information Security*, (October), 1–8. http://doi.org/10.5815/ijcnis.2015.11.01

Prayudi, Y., Luthfi, A., Munasir, A., Pratama, R., & Kunci, K. (2014). Pendekatan Model Ontologi Untuk Merepresentasikan Body of Knowledge Digital Chain of Custody. *Cybermatika*, *2*, 36–43.

Prayudi, Y., & SN, A. (2015). Digital Chain of Custody : State of the Art. *International Journal of Computer Applications*, *114*(5), 8887.

Qin, Jin, Dobreski, B., & Brown, D. A. (2016). Metadata and Reproducibility : A Case Study of Gravitational Wave Research Data. *International Journal of Digital Curation*, *11*, 218–231. http://doi.org/10.2218/ijdc.v11i1.399

Raghavan, S. (2014). A Framework for Identifying Associations in Digital Evidence Using Metadata Keywords, (May), 1–238. Retrieved from http://eprints.qut.edu.au/72659/1/Sriram_Raghavan_Thesis.pdf

Riley, J. (2017). *U Nderstanding M Etadata What Is Metadata ,And What Is It For?* 3600 Clipper Mill Road: National Information Standards Organization (NISO). Retrieved from www.niso.org

Ryder, K. (2002). Computer Forensics - We've had an incident, who do we get to investigate? *SANS Institute InfoSec Reading Room*.

Shah, Z. I., & Ibrahim, R. (2014). The Design of Android Metadata based on Reverse Engineering using UML, 579–586. http://doi.org/10.1007/978-981-4585-18-7

S*oft*ware, G. (2013). *EnCase Forensic Imager Version 7.06*. Guidance Software Inc. Retrieved from http://*download*.guidances*oft*ware.com/

Tanner, A. L., Shook, Hardy, & Bacon. (2011). METADATA : WHY THE FUSS ? A White Paper on Metadata. *Bloomberg Law Reports - Technology Law*, *2*(15), 1–9.

Thomson, L. L. (2011). *Admissibility Of Electronic Documentation As Evidence In U. S. Court*. United State *of* America.

Vandoven, Sa. (2014). Forensic Images : For Your Viewing Pleasure. *SANS Institute InfoSec Reading Room*.

Woods, K., Chassan*off*, A., & Lee, C. A. (2013). Managing and Transforming Digital Forensics Metadata for Digital Collections. *10th International Conference on Preservation of Digital Objects*, (p. 203).

Xiankun, Z., Lei, D., & Shan, G. (2010). The Knowledge Description of Emergency Information Semantic Metadata Model and Its Application, 2–5. http://doi.org/10.1109/ISME.2010.152

Yang, B., Qiao, L., Cai, N., Zhu, Z., & Wulan, M. (2017). Manufacturing process information modeling using a metamodeling approach. *The International Journal of Advanced Manufacturing Technology*. http://doi.org/10.1007/s00170-016-9979-0

Zaino, J. (2016). 2017 Trends in Data Strategy. Retrieved July 1, 2017, from http://www.dataversity.net/2017-trends-data-strategy/

Zheng, J. (2015). Research and Application of Data Modeling and Integration Based on Metadata, 525–528. http://doi.org/10.1109/ITME.2015.160

Republik Indonesia. 2010. Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 Tahun 2010 Tentang Tata Cara Pengelolaan Barang Bukti di Lingkungan Kepolisian Negara Republik Indonesia

Republik Indonesia. 2009. Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 Tahun 2009 Tentang Tata Cara Dan Persyaratan Permintaan Pemeriksaan Teknis Kriminalistik Tempat Kejadian Perkara Dan Laboratoris Kriminalistik Barang Bukti Ke Pada Laboratorium Forensik Kepolisian Negara Republik Indonesia.

Standar Nasional Indonesia ISO/IEC. (2014). *Teknologi Informasi – Teknik Keamanan – Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital* No. 27037).

LAMPIRAN

LAMPIRAN 1. Pengujian Model Informasi Metadata Secara Fungsional

Tabel 1 Hasil Pengujian Fungsional Model Informasi Metadata

No	Skenario Pengujian	Test Case	Hasil Yang Diharapkan	Hasil Pengujian
1	Masuk ke aplikasi Digital *Chain of custody*	*User* belum melakukan Login	Aplikasi menampilkan halaman awal digital *chain of custody* dan hanya terdapat satu menu aktif yaitu menu login	Sesuai harapan
2	Login menggunakan akun *user* yang belum terdaftar baik sebagai *first responder* ataupun *officer*	*User*name : taka Password : morita	Aplikasi akan menampilkan peringatan bahwa *user*name tidak terdaftar dan meminta *user* untuk memasukkan *user*name dan password yang benar	Sesuai harapan
3	Login sebagai *first responder*	*User*name : helvi Paswword : 123	Login berhasil dan aplikasi akan menampilkan halaman awal dimana akan terdapat menu yang dapat digunakan diantaranya logout, open *file*, manage *file*, view xml dan view metadata	Sesuai harapan
4	Memuat *file* bukti digital ke dalam aplikasi DCOC	Login sebagai : *first responder* Memilih menu open dan memuat sebuah *file* bukti digital (DN_TOSHIBA _FDD.E01) yang disimpan di dalam direktori *cabinet* Bagian informasi dokumentasi yang dapat diakses oleh *first responder* terbatas pada	Aplikasi akan menampilkan halaman formulir untuk menginputkan informasi manajemen *chain of custody* Aplikasi menampilkan Tab Olah Tkp, bukti elektronik, bukti digital, *download* dan *report* Aplikasi akan mengekstrak informasi atribut *file* digital diantaranya *file*name, size, date created, time created, md5 hash, sha1 dan sha256 ke dalam *field* informasi yang terdapat pada “Tab Bukti Digital” serta *user*	Sesuai harapan

No	Skenario Pengujian	Test Case	Hasil Yang Diharapkan	Hasil Pengujian
		informasi olah TKP, bukti elektronik dan bukti digital	tidak dapat memodifikasi informasi tersebut	
5	Create *file* metadata *chain of custody* baru dengan nama *file chain of custody* menggunakan nama *file* bukti digital	*File* bukti digital yang digunakan : bird.avi *File* temporary metadata *chain of custody* yang dihasilkan : bird.xml Memasukkan informasi Olah TKP dan menekan tombol save	Aplikasi menyimpan informasi Olah TKP ke dalam *file* temporary metadata *chain of custody* dengan nama bird.xml di dalam forlder temporary	Sesuai harapan
6	Menambahkan informasi pada Tab Bukti Elektronik ke dalam *file* metadata *chain of custody*	Memasukkan informasi pada *field* yang terdapat pada Tab Bukti elektronik dan menekan tombol SAVE	Aplikasi menambahkan informasi pada Tab Bukti Elektronik ke dalam *file* temporary metadata bird.xml	Sesuai harapan
7	Menambahkan informasi pada Tab Bukti Digital ke dalam *file* metadata *chain of custody*	Memasukkan informasi pada *field* yang terdapat pada Tab Bukti Digital dan menekan tombol SAVE	Aplikasi menambahkan informasi pada Tab Bukti Digital ke dalam *file* metadata bird.xml	Sesuai harapan
8	*First Responder* mengajukan request untuk dapat men*download file* bukti digital	Login sebagai : *first responder* *First Responder* mengajukan permintaan *download* terhadap *file* bukti digital bird.xml untuk	Aplikasi menyimpan permintaan *download file* bukti digital yang dilakukan oleh *first responder*. Aplikasi hanya akan mendokumentasikan *entry chain of custody* dan	Sesuai harapan

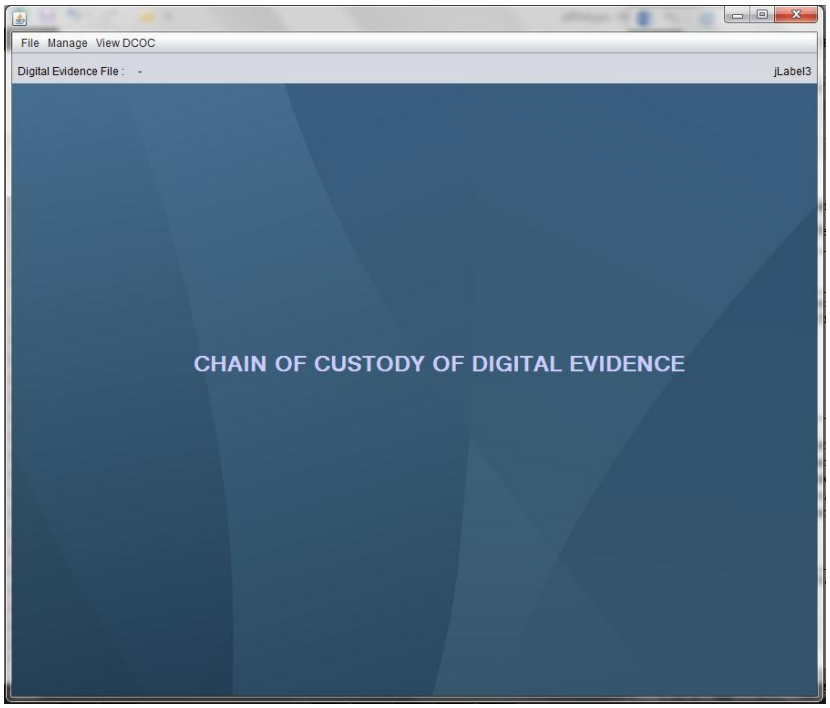
No	Skenario Pengujian	Test Case	Hasil Yang Diharapkan	Hasil Pengujian
		dapat di setujui oleh *officer*	*download request* tersebut sebagai interaksi terhadap bukti digital (*chain of custody*) setelah *officer* melakukan *approve* terhadap *request* tersebut	
9	Mencetak laporan (formulir) *chain of custody*	Menekan tombol "generate *report*" yang terdapat "Tab *Report*"	Aplikasi menampilkan prtingatan bahwa *file* metadata *chain of custody* yang dimaksud tidak ditemukan. Hal ini karena *entry* ersebut belum di *approve* oleh *officer*	Sesuai harapan
10	Login sebagai *Officer*	*User*name : erwin Paswword : 456	Login berhasil dan aplikasi akan menampilkan halaman awal dimana akan terdapat menu yang dapat digunakan diantaranya logout, open *file*, manage *file* dan view xml	Sesuai harapan
11	Melakukan manajemen *file chain of custody* dengan memuat *file* metadata *chain of custody* bukti digital ke dalam aplikasi DCOC	Login sebagai : *Officer* Memilih menu *manage* → *Open file* dan memuat *file* temporary metadata bukti digital (bird.xml) yang disimpan di dalam folder temporary untuk di approve dan disimpan sebagai metadata *chain of custody file* digital ke dalam folder metadata. Aplikasi akan menampilkan halaman formulir	Aplikasi menampilkan halaman formulir manajemen DCOC dan memuat informasi metadata bird.xml ke dalam *field* informasi yang sesuai Aplikasi menampilkan Tab Olah Tkp, bukti elektronik, bukti digital, *chain of custody*, *download* dan *report*	Sesuai harapan

No	Skenario Pengujian	Test Case	Hasil Yang Diharapkan	Hasil Pengujian
		manajemen DCOC dan memuat informasi metadata ke dalam *field* informasi yang sesuai Bagian informasi dokumentasi yang dapat diakses oleh *officer* adalah informasi olah TKP, bukti elektronik, bukti digital dan *chain of custody* (interaksi)		
12	Melakukan UPDATE informasi metadata *chain of custody*	*File* metadata *chain of custody* : bird.xml Mengubah satu atau beberapa informasi dari *field* informasi dan menekan tombol UPDATE	Aplikasi menyimpan perubahan informasi sesuai dengan informasi baru yang dimasukkan pada *field* informasi ke dalam *file* metadata *chain of custody* bird.xml	Sesuai harapan
13	Melakukan approve atau menyetujui request *download* yang diminta oleh *first responder*	Login sebagai : *Officer* *Officer* menekan tombol approve pada Tab *chain of custody*	Aplikasi akan menyimpan informasi sebagai intereksi terhadap bukti digital (dalam kasus ini adalah "*download*") Nilai *field* informasi approved time dan received time akan secara otomatis berubah menyesuaikan dengan waktu sistem dan akan disimpan ke dalam informasi *chain of custody*	Sesuai harapan

No	Skenario Pengujian	Test Case	Hasil Yang Diharapkan	Hasil Pengujian
			file DN_TOSHIBA_FDD.xml Pada aplikasi ini diasumsikan bahwa pada saat *officer* menekan tombol approve maka *first responder* juga telah menerima *file* bukti digital tersebut	
14	Melakukan VIEW struktur metadata *file* bird.xml	Login sebagai : *Officer* *Officer* memilih menu manage → view xml *file* → memeilih *file* bird.xml	Aplikasi memparser dan menampilkan isi *file* bird.xml ke dalam text area	Sesuai harapan
15	Melakukan *Download report*/formulir *chain of custody* metadata *file* bird.xml	*Officer* memilih Tab *Report* → pilih *Download report*	Aplikasi akan mencetak formulir dalam format .pdf	Sesuai harapan

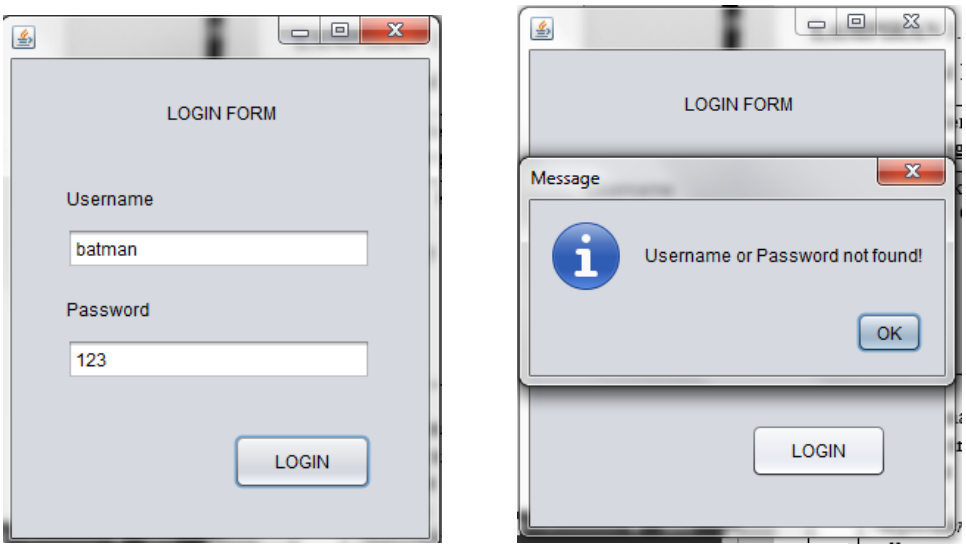
LAMPIRAN 2 Gambar Pengujian Fungsional Menggunakan Aplikasi

4. Pengujian Tabel 1 No 1



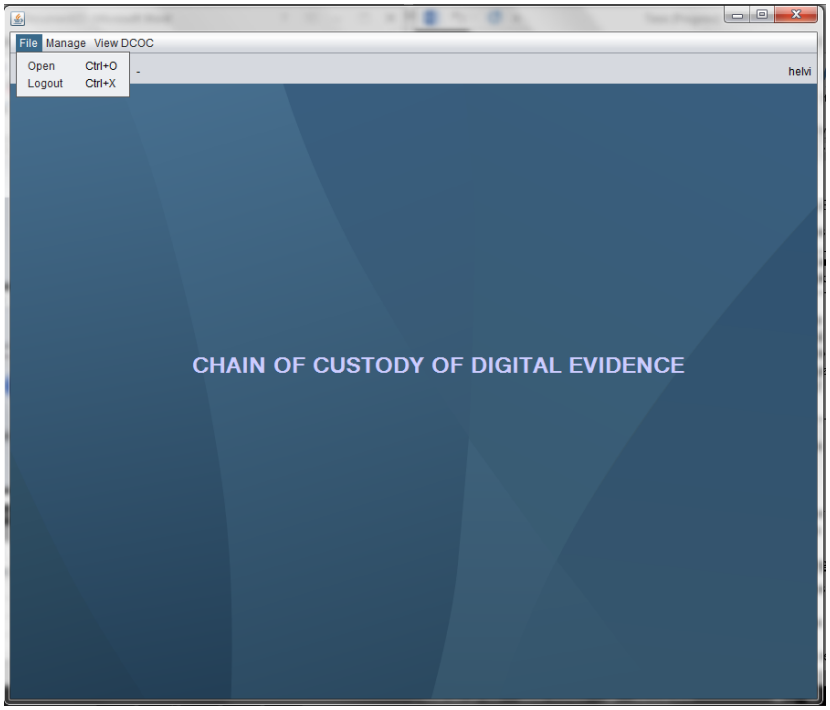
Gambar 1 Halaman Awal Aplikasi DCOC

5. Pengujian Tabel 1 No 2



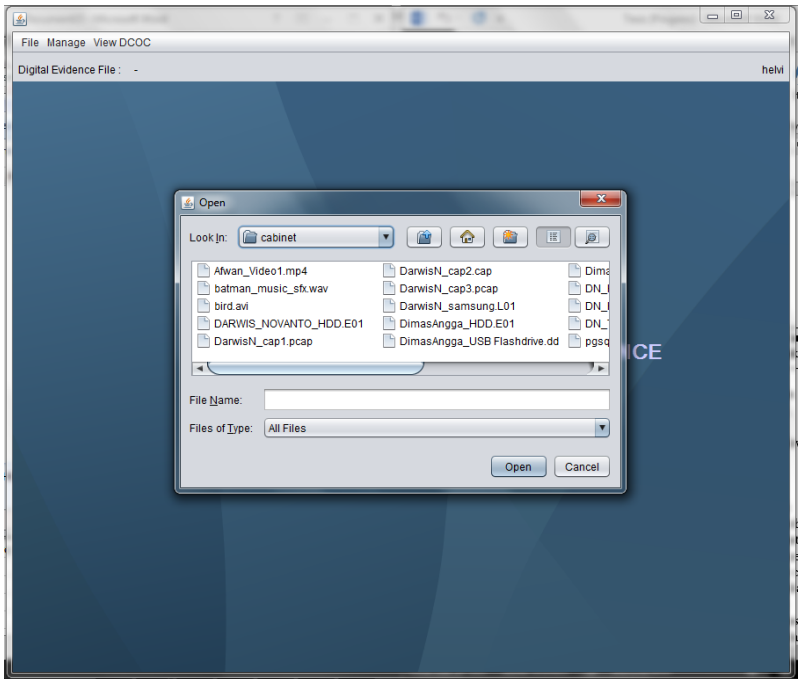
Gambar 2 Halaman *Log in* (**User*name & *Password* belum terdaftar)

6. Pengujian Tabel 1 No 3

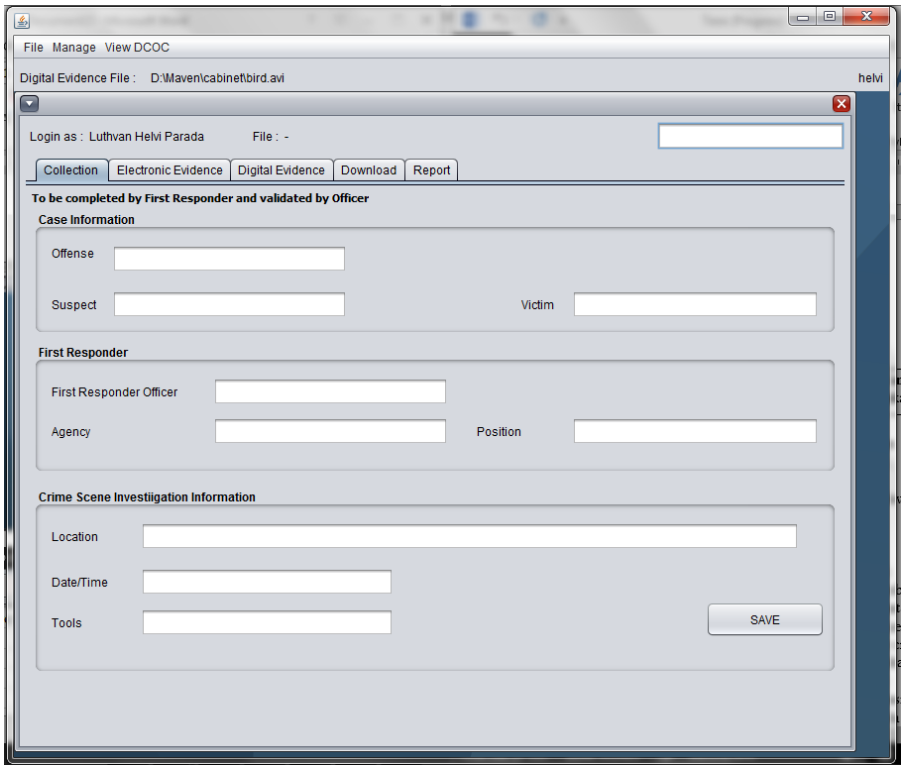


Gambar 3 Halaman Menu *First Responder*

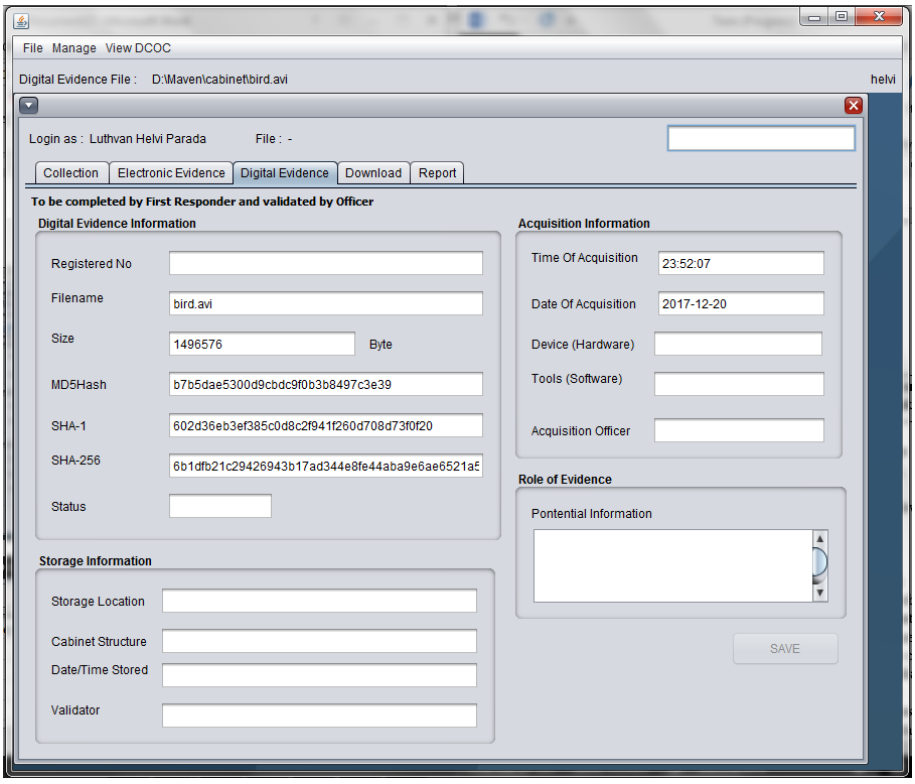
7. Pengujian Tabel 1 No 4



Gambar 4 Halaman *Open File* Digital

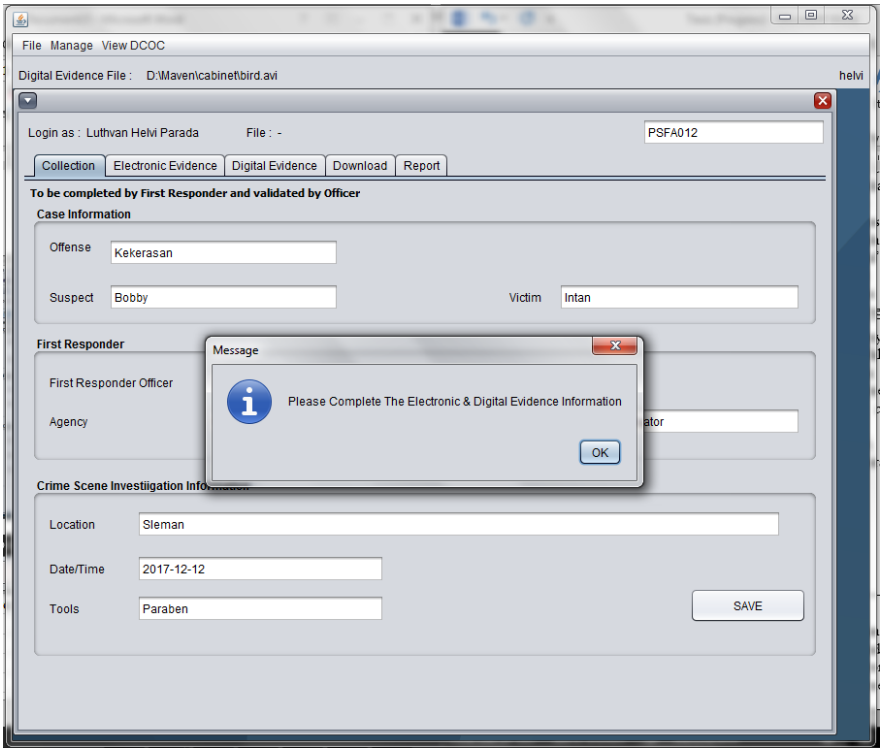


Gambar 5 Halaman Formulir *Entry Chain Of Custody* Baru



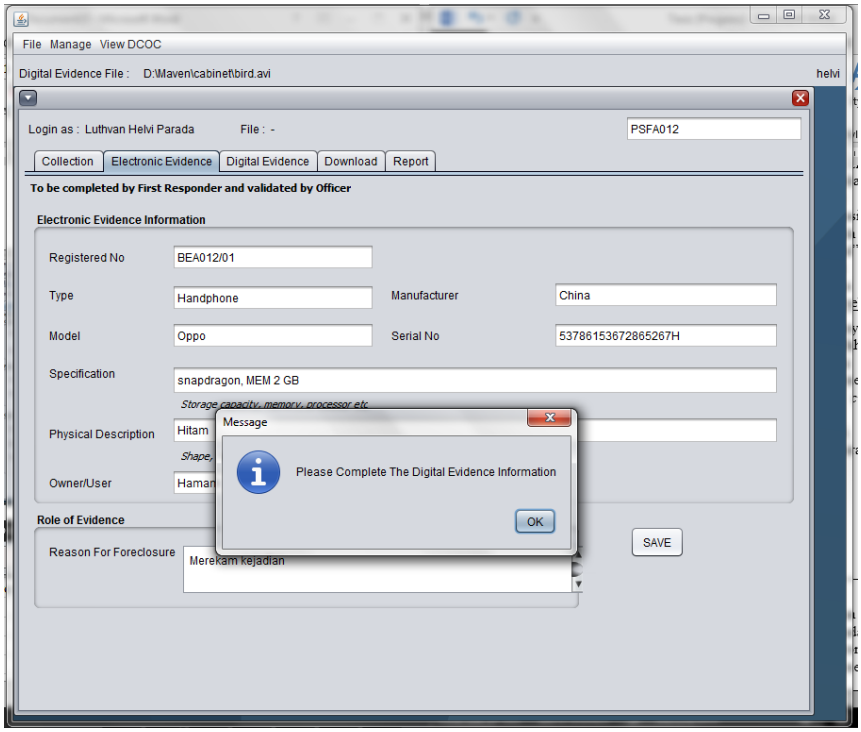
Gambar 6 Informasi Yang Diekstrak Langsung Dari *File* Digital

8. Pengujian Tabel 1 No 5



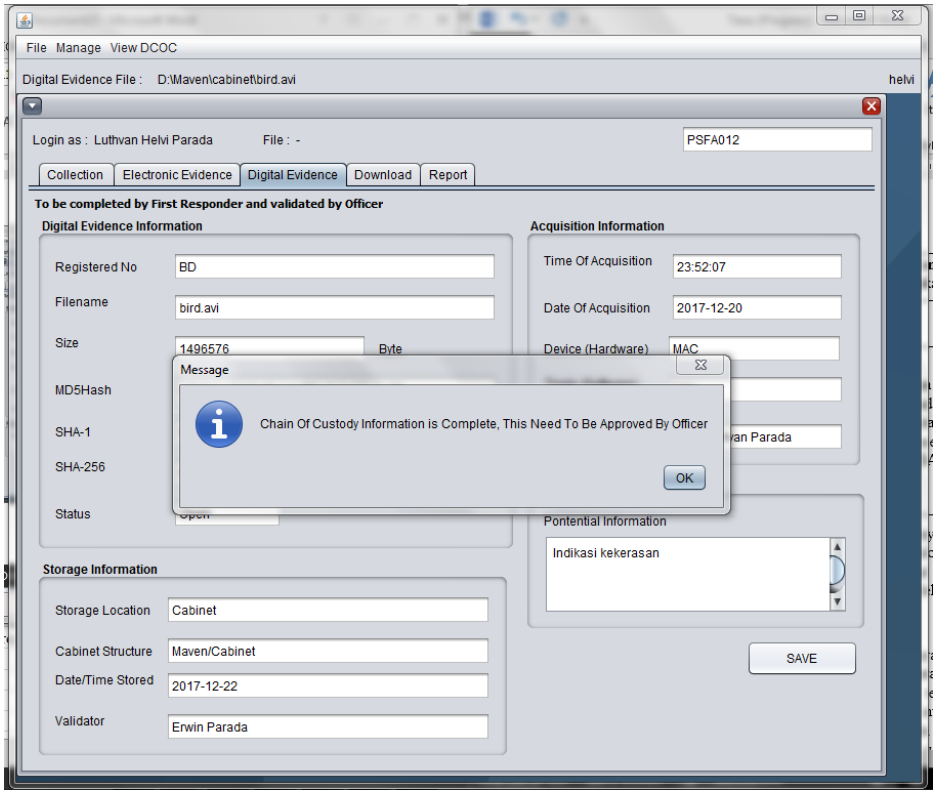
Gambar 7 Konfirmasi Simpan Informasi *Collection*

9. Pengujian Tabel 1 No 6



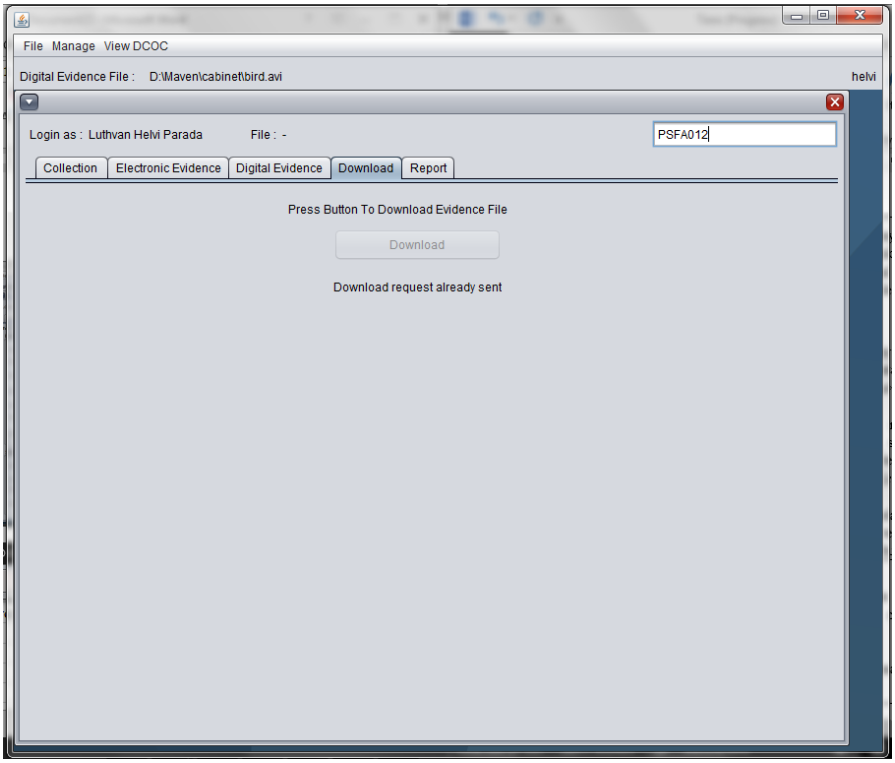
Gambar 8 Konfirmasi Simpan Informasi *Electronic Evidence*

10. Pengujian Tabel 1 No 7



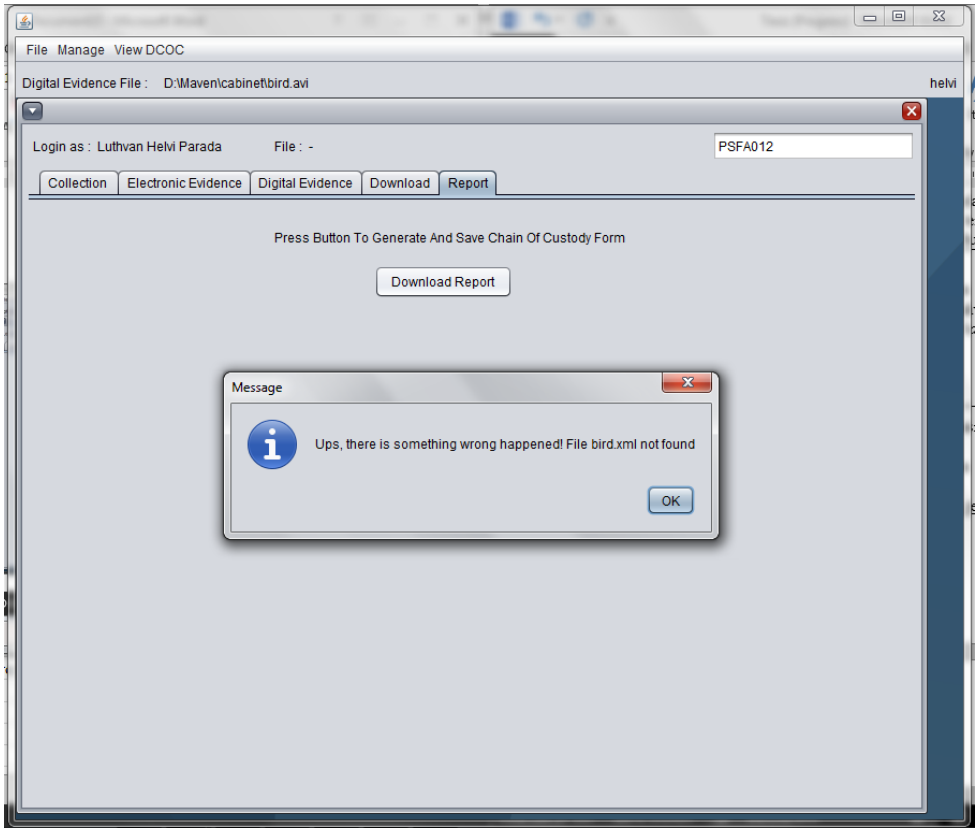
Gambar 9 Konfirmasi Simpan Informasi *Digital Evidence*

11. Pengujian Tabel 1 No 8



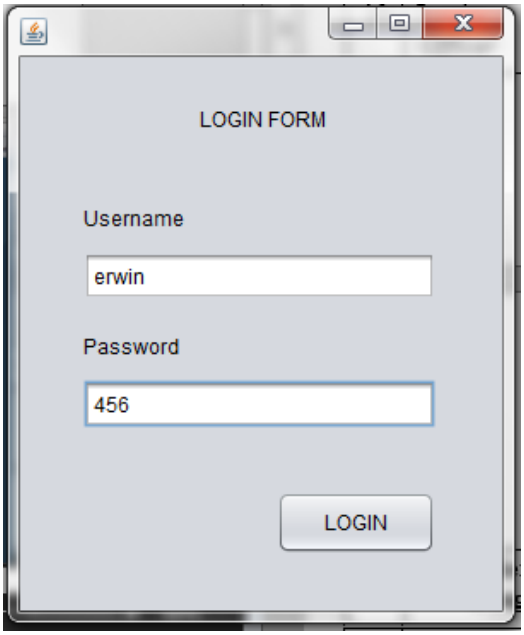
Gambar 10 Halaman *Request Download* Bukti Digital

12. Pengujian Tabel 1 No 9



Gambar 11 Konfirmasi Gagal *Download* Formulir

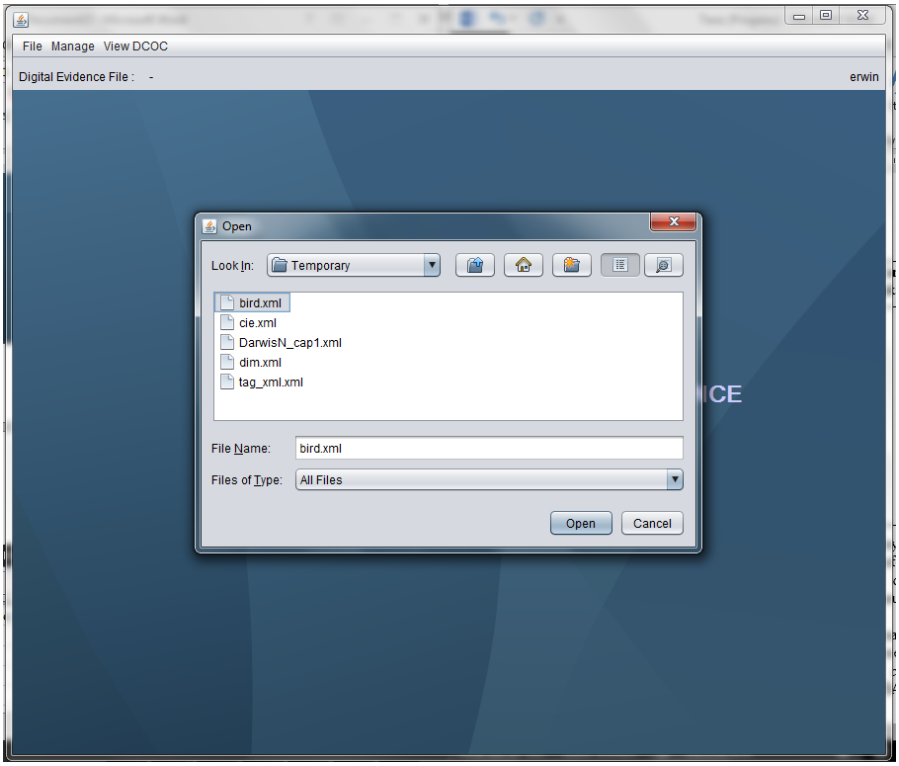
13. Pengujian Tabel 1 No 10



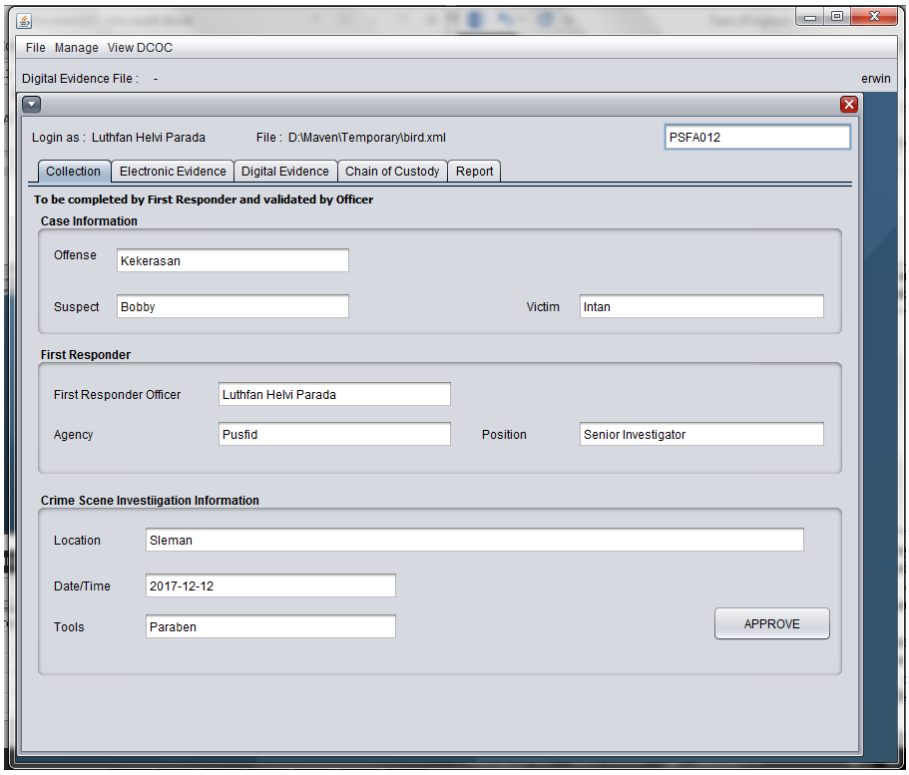
Gambar 12 Halaman *Log in Officer*

Gambar 13 Halaman Menu *Officer*

14. Pengujian Tabel 1 No 11

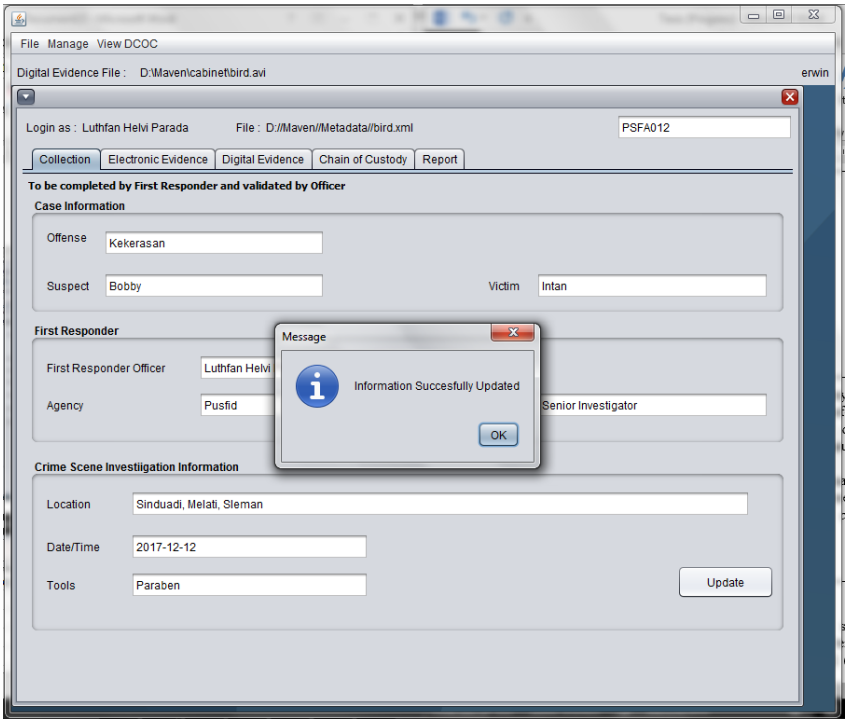


Gambar 14 Halaman Open *File* Temporary Metadata



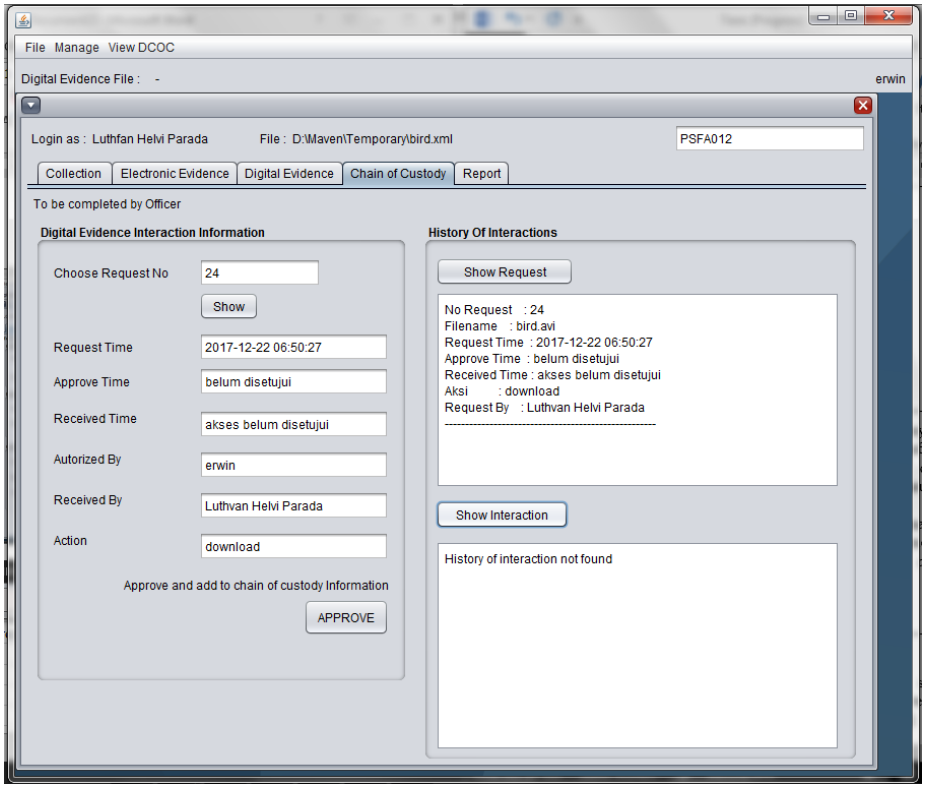
Gambar 15 Formulir Menampilkan Inormasi Metadata Sesuai *Field* Untuk Di *Approve*

15. Pengujian Tabel 1 No 12

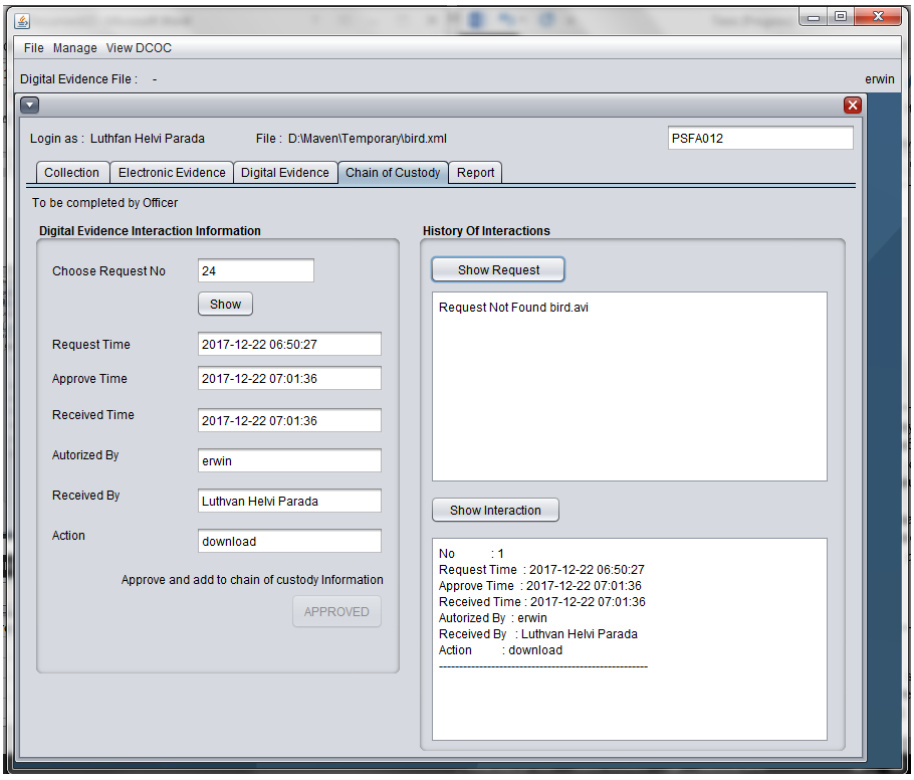


Gambar 16 Konfirmasi *Chain Of Custody* Berhasil Disimpan

16. Pengujian Tabel 1 No 13

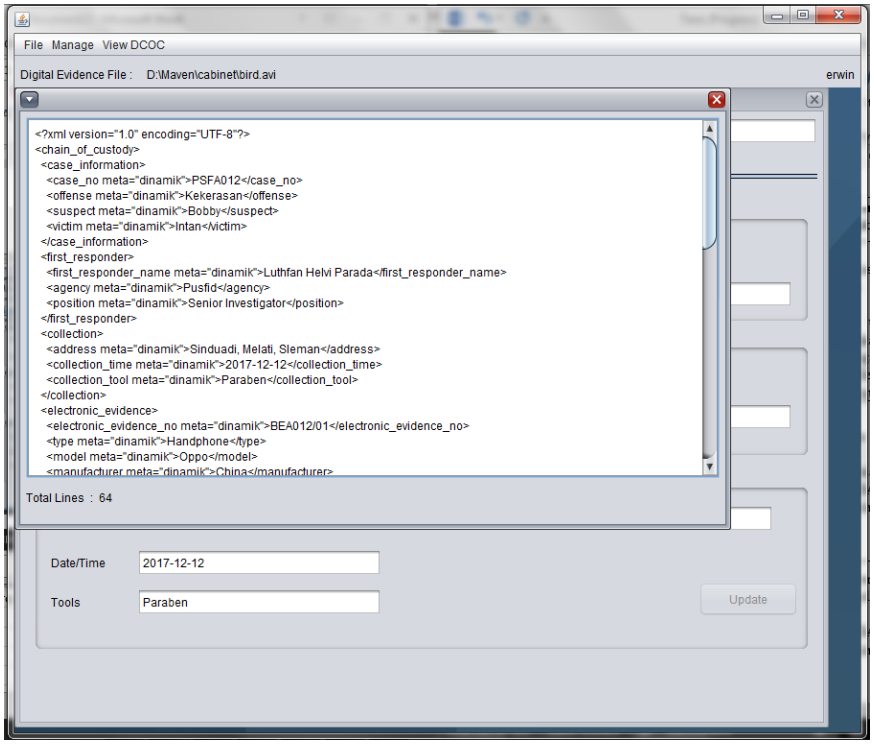


Gambar 17 Halaman *Approve Request Chain Of Custody Interactions*



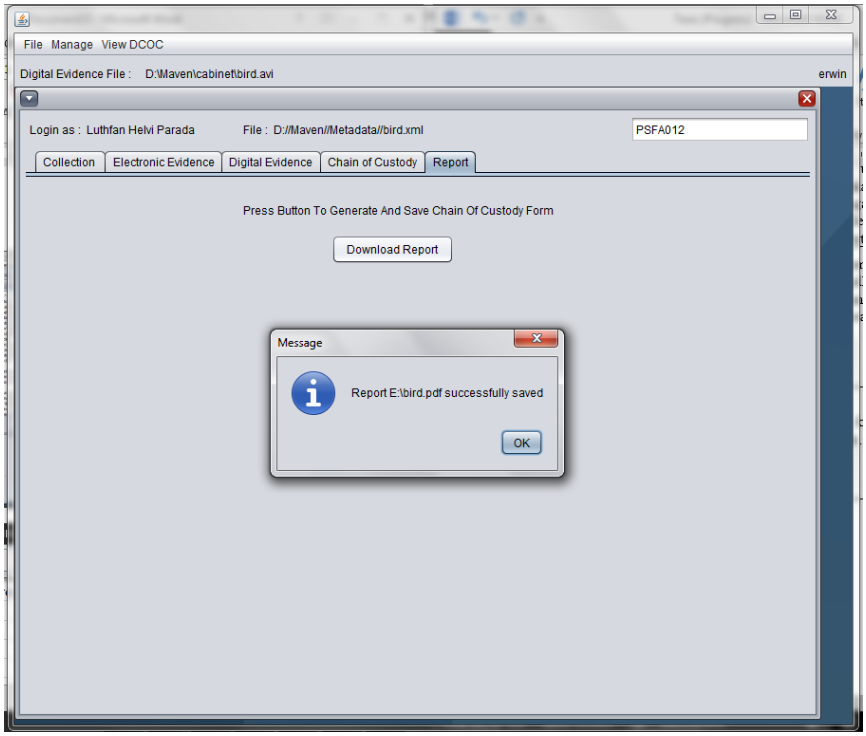
Gambar 18 Informasi Setelah *Request* Di-*Approve*

17. Pengujian Tabel 1 No 14

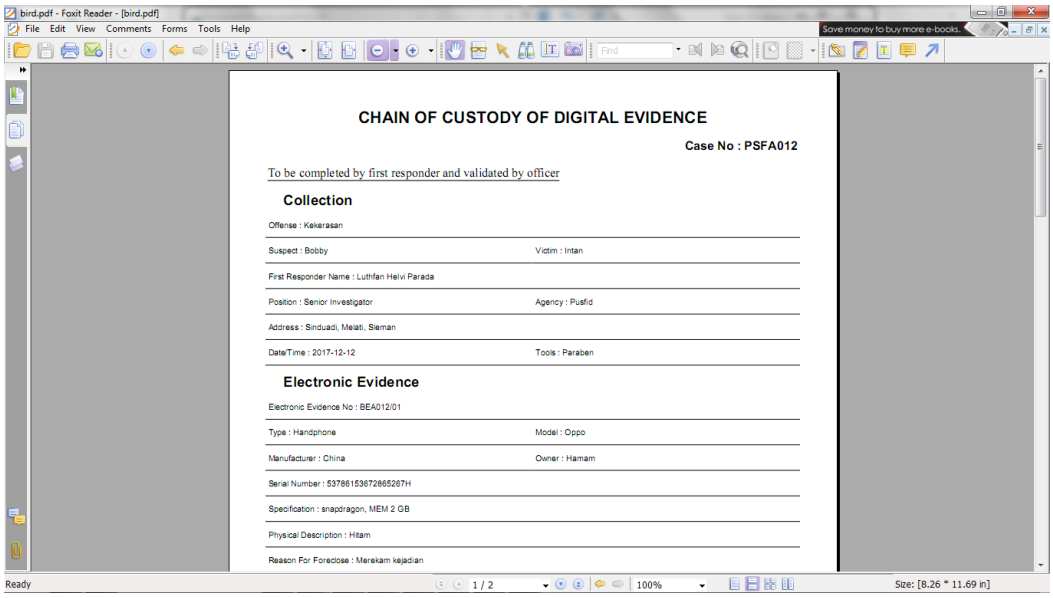


Gambar 19 Halaman View XML-Metadata

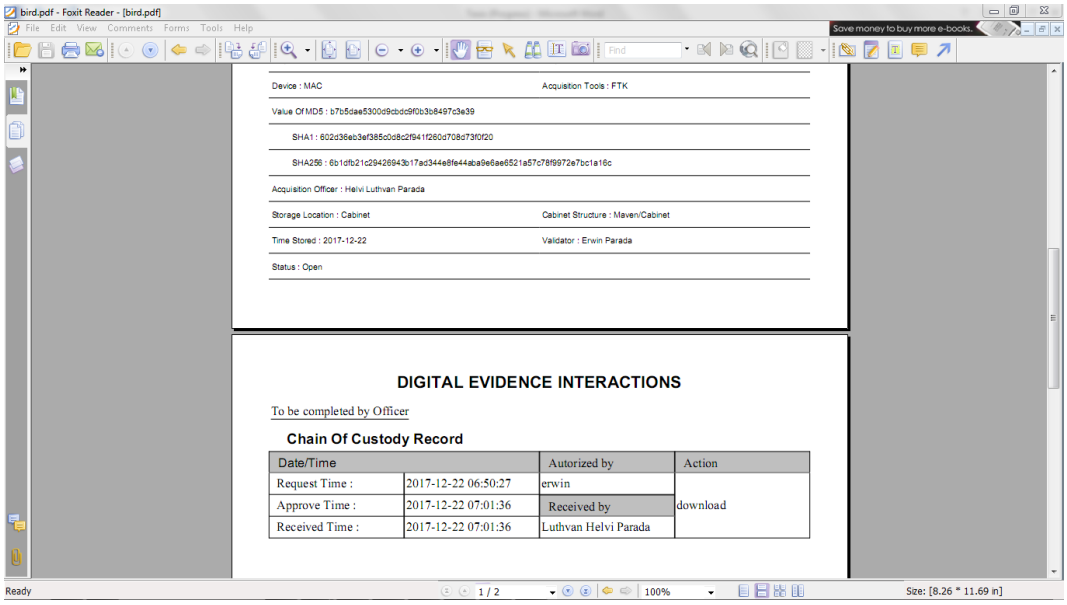
18. Pengujian Tabel 1 No 15



Gambar 20 Konfirmasi *Report*/Formulir Berhasil Disimpan



Gambar 21 Tampilan Halaman *Report* 1



Gambar 22 Tampilan Halaman *Report* 2

LAMPIRAN 3. Desain Formulir *Chain Of Custody* Bukti Digital

CHAIN OF CUSTODY OF DIGITAL EVIDENCE

Case No :_____

To be completed by First responder

Collection

Offense :

Suspect : Victim :

First Responder Name :

Position : Agency :

Address :

Date/Time : Tools :

Electronic Evidence

Electronic Evince No:

Type : Model :

Manufacturer : Owner :

Serial Number :

Spesification :

Physical Description :

Reason For Foreclose :

Digital Evidence

Digital Evidence No :

Filename : Size (Byte) :

Acquisition Time : Acquisition Date :

Device (Akuisisi) : Acquisition Tools :

Value Of MD5 :

SHA-1 :

SHA-256 :

Acquisition Officer :

Storage Location : Cabinet Structure :

Time Stored : Validator :

Potential Information :

Status :

Gambar 23 Formulir DCOC 1 (*English Ver)

DIGITAL EVIDENCE INTERACTIONS

To be completed by Officer

Chain Of Custody Record

Date / Time		Autorized by	Action
Request Time	:		
Approve Time	:	Received by	
Received Time	:		
Date / Time		Autorized by	Action
Request Time	:		
Approve Time	:	Received by	
Received Time	:		
Date / Time		Autorized by	Action
Request Time	:		
Approve Time	:	Received by	
Received Time	:		
Date / Time		Autorized by	Action
Request Time	:		
Approve Time	:	Received by	
Received Time	:		
Date / Time		Autorized by	Action
Request Time	:		
Approve Time	:	Received by	
Received Time	:		
Date / Time		Autorized by	Action
Request Time	:		
Approve Time	:	Received by	
Received Time	:		

Gambar 24 Formulir DCOC 2 (*English Ver)

CHAIN OF CUSTODY OF DIGITAL EVIDENCE

No Kasus :_____

To be completed by First responder (Diisi oleh petugas Olah TKP)

Olah Tempat Kejadian Perkara

Offense (Tipe Kasus) :

Suspect : Victim :

Nama Petugas :

Jabatan : Instansi :

Lokasi :

Waktu : Alat :

Bukti Elektronik

No Register BE:

Type : Model :

Manufaktur : Pemilik :

Serial Number :

Spesifikasi Teknis :

Deskripsi Fisik :

Alasan Penyitaan :

Bukti Digital

No Register BD :

Nama File : Ukuran (Byte) :

Waktu (Akuisisi) : Tanggal (Akuisisi) :

Device (Akuisisi) : Tools (Akuisisi) :

Nilai MD5 :

SHA-1 :

SHA-256 :

Petugas Akuisisi :

Lokasi Penyimpanan : Struktur Kabinet :

Waktu Penyimpanan : Validator :

Potensi Informasi :

Status BD :

Gambar 25 Formulir DCOC 1 (*Bahasa Ver)

DIGITAL EVIDENCE INTERACTIONS

Formulir Usulan

To be completed by Officer (Diisi Oleh Petugas Pengelola Barang Bukti)

Chain Of Custody Record

Tanggal / Waktu		Autorized by :	Aksi :
Request Time	:		
Approve Time	:	Received by :	
Received Time	:		
Tanggal / Waktu :		Autorized by :	Aksi :
Request Time	:		
Approve Time	:	Received by :	
Received Time	:		
Tanggal / Waktu		Autorized by :	Aksi :
Request Time	:		
Approve Time	:	Received by :	
Received Time	:		
Tanggal / Waktu :		Autorized by :	Aksi :
Request Time	:		
Approve Time	:	Received by :	
Received Time	:		
Tanggal / Waktu		Autorized by :	Aksi :
Request Time	:		
Approve Time	:	Received by :	
Received Time	:		
Tanggal / Waktu :		Autorized by :	Aksi :
Request Time	:		
Approve Time	:	Received by :	
Received Time	:		

Gambar 26 Formulir DCOC 2 (*Bahasa Ver)

LAMPIRAN 4 *File* Metadata Hasil Entry *Chain Of Custody*

Tabel 1 *File* Metadata Hasil Entry COC

```
1.  <?xml version="1.0" encoding="UTF-8"?>
2.  <chain_of_custody>
3.  <case_information>
4.  <case_no meta="dinamik">PSFA012</case_no>
5.  <offense meta="dinamik">Kekerasan</offense>
6.  <suspect meta="dinamik">Bobby</suspect>
7.  <victim meta="dinamik">Intan</victim>
8.  </case_information>
9.  <first_responder>
10. <first_responder_name meta="dinamik">Luthfan Helvi Parada</first_responder_name>
11. <agency meta="dinamik">Pusfid</agency>
12. <position meta="dinamik">Senior Investigator</position>
13. </first_responder>
14. <collection>
15. <address meta="dinamik">Sinduadi, Melati, Sleman</address>
16. <collection_time meta="dinamik">2017-12-12</collection_time>
17. <collection_tool meta="dinamik">Paraben</collection_tool>
18. </collection>
19. <electronic_evidence>
20. <electronic_evidence_no meta="dinamik">BEA012/01</electronic_evidence_no>
21. <type meta="dinamik">Handphone</type>
22. <model meta="dinamik">Oppo</model>
23. <manufacturer meta="dinamik">China</manufacturer>
24. <serial_no meta="dinamik">53786153672865267H</serial_no>
25. <spesification meta="dinamik">snapdragon, MEM 2 GB</spesification>
26. <physical_description meta="dinamik">Hitam</physical_description>
27. <owner meta="dinamik">Hamam</owner>
28. </electronic_evidence>
29. <role_of_evidence>
30. <reason_for_foreclose meta="dinamik">Merekam kejadian</reason_for_foreclose>
31. <potential_information meta="dinamik">Indikasi kekerasan</potential_information>
32. </role_of_evidence>
33. <digital_evidence>
34. <digital_evidence_no meta="dinamik">BD</digital_evidence_no>
35. <filename meta="statik">bird.avi</filename>
36. <size meta="statik">1496576</size>
37. <md5 meta="statik">b7b5dae5300d9cbdc9f0b3b8497c3e39</md5>
38. <sha1 meta="statik">602d36eb3ef385c0d8c2f941f260d708d73f0f20</sha1>
39. <sha256
    meta="statik">6b1dfb21c29426943b17ad344e8fe44aba9e6ae6521a57c78f9972e7bc1a16c<
    /sha256>
40. <status meta="dinamik">Open</status>
41. </digital_evidence>
42. <acquisition>
43. <acquisition_time meta="statik">23:52:07</acquisition_time>
44. <acquisition_date meta="statik">2017-12-20</acquisition_date>
45. <device meta="dinamik">MAC</device>
46. <acquisition_tool meta="dinamik">FTK</acquisition_tool>
47. <acquisition_officer meta="dinamik">Helvi Luthvan Parada</acquisition_officer>
48. </acquisition>
49. <storage>
```

```
50. <storage_location meta="dinamik">Cabinet</storage_location>
51. <cabinet_structure meta="dinamik">Maven/Cabinet</cabinet_structure>
52. <time_stored meta="dinamik">2017-12-22</time_stored>
53. <validator meta="dinamik">Erwin Parada</validator>
54. </storage>
55. <chain_of_interactions>
56. <request_time meta="dinamik">2017-12-22 06:50:27</request_time>
57. <approve_time meta="dinamik">2017-12-22 07:01:36</approve_time>
58. <received_time meta="dinamik">2017-12-22 07:01:36</received_time>
59. <autorized_by meta="dinamik">erwin</autorized_by>
60. <received_by meta="dinamik">Luthvan Helvi Parada</received_by>
61. <action meta="dinamik">download</action>
62. </chain_of_interactions>
63. </chain_of_custody>
```

LAMPIRAN 5 Data Hasil Pengujian Menggunakan Angket/Kuesioner

Tabel 2 Tabel Data Hasil Angket/Kuesioner

Nama	Jabatan	Kelompok informasi yang terdapat di dalam gambar tersebut sudah cukup memenuhi "kebutuhan informasi " *chain of custody* bukti digital	Kelompok informasi yang ada pada Gambar tersebut sudah memuat elemen informasi yang sesuai	Berdasarkan Gambar, adakah elemen informasi yang tidak sesuai atau berada di luar konteks *chain of custody* bukti digital?	Pengelompokan informasi pada Gambar sudah mendeskripsikan bukti digital dengan baik dan mudah dipahami	Informasi yang ada pada formulir sudah cukup lengkap dalam mendokumentasikan tahapan *chain of custody* bukti digital	Informasi yang ada pada formulir tersebut sudah cukup baik dalam mendokumentasikan interaksi terhadap barang bukti digital	Informasi yang ada pada formulir sudah cukup lengkap dalam mendokumentasikan individu yang terlibat dengan bukti digital	Informasi yang ada pada formulir sudah cukup baik dalam mendokumentasikan nilai integritas dan keamanan bukti digital	Informasi yang ada pada formulir sudah mencakup informasi 5W+1H yaitu apa, siapa, mengapa, dimana, kapan dan bagaiamana terkait dengan barang bukti digital digital	Informasi yang dimuat di dalam formulir dapat dengan mudah dipahami	Formulir tersebut dapat diimplementasikan untuk mendokumentasikan *chain of custody* bukti digital
Pratomo Djati Nugroho	Dosen	Sangat setuju	Sangat setuju	Tidak ada	Sangat setuju	Sangat setuju	Sangat setuju	Sangat setuju	Sangat setuju	Sangat setuju	Sangat setuju	Sangat setuju
Afiyati	Dosen	Setuju	Setuju	Tidak ada	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju
M. Ibrahim Adha	Lawyer	Sangat setuju	Sangat setuju	Ada	Sangat setuju	Setuju	Setuju	Setuju	Setuju	Sangat setuju	Sangat setuju	Setuju
Hudi	Kepala Seksi	Setuju	Setuju	Tidak ada	Setuju	Setuju	Setuju	Setuju	Tidak berpendapat/Netral	Setuju	Setuju	Setuju
Mirza Rahadian	Staf bidang Digital Forensic	Setuju	Setuju	Tidak ada	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju
Yolly Rinaldi	Junior Manager IT Security	Setuju	Setuju	Tidak ada	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju

Nama	Jabatan	Kelompok informasi yang terdapat di dalam gambar tersebut sudah cukup memenuhi "kebutuhan informasi " *chain of custody* bukti digital	Kelompok informasi yang ada pada Gambar tersebut sudah memuat elemen informasi yang sesuai	Berdasarkan Gambar, adakah elemen informasi yang tidak sesuai atau berada di luar konteks *chain of custody* bukti digital?	Pengelompokan informasi pada Gambar sudah mendeskripsikan bukti digital dengan baik dan mudah dipahami	Informasi yang ada pada formulir sudah cukup lengkap dalam mendokumentasikan tahapan *chain of custody* bukti digital	Informasi yang ada pada formulir tersebut sudah cukup baik dalam mendokumentasikan interaksi terhadap barang bukti digital	Informasi yang ada pada formulir sudah cukup lengkap dalam mendokumentasikan individu yang terlibat dengan bukti digital	Informasi yang ada pada formulir sudah cukup baik dalam mendokumentasikan nilai integritas dan keamanan bukti digital	Informasi yang ada pada formulir sudah mencakup informasi 5W+1H yaitu apa, siapa, mengapa, dimana, kapan dan bagaiamana terkait dengan barang bukti digital digital	Informasi yang dimuat di dalam formulir dapat dengan mudah dipahami	Formulir tersebut dapat diimplementasikan untuk mendokumentasikan *chain of custody* bukti digital
Mukhlis Prasetyo Aji	Dosen	Setuju	Setuju	Tidak ada	Setuju	Tidak berpendapat/Netral	Tidak berpendapat/Netral	Tidak berpendapat/Netral	Tidak berpendapat/Netral	Setuju	Tidak berpendapat/Netral	Setuju
Ardiansyah	Pelaksana	Setuju	Setuju	Tidak ada	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju	Setuju
TRI WIDODO	DOSEN	Tidak berpendapat/Netral	Setuju	Tidak ada	Setuju	Setuju	Sangat setuju	Setuju	Sangat setuju	Sangat setuju	Sangat setuju	Setuju
Andritona Munaf	Consultant	Setuju	Tidak berpendapat/Netral	Ada	Setuju	Setuju	Setuju	Tidak berpendapat/Netral	Tidak berpendapat/Netral	Setuju	Tidak berpendapat/Netral	Setuju