KPK
Komisi Pemberantasan Korupsi

Pusat Edukasi Antikorupsi
Cipta • Karya • Berdaya

kemitraan
partnership

AFDI
ASOSIASI FORENSIK DIGITAL INDONESIA

Manajemen Pengelolaan Bukti Elektronik

Kamis 3 Desember 2020

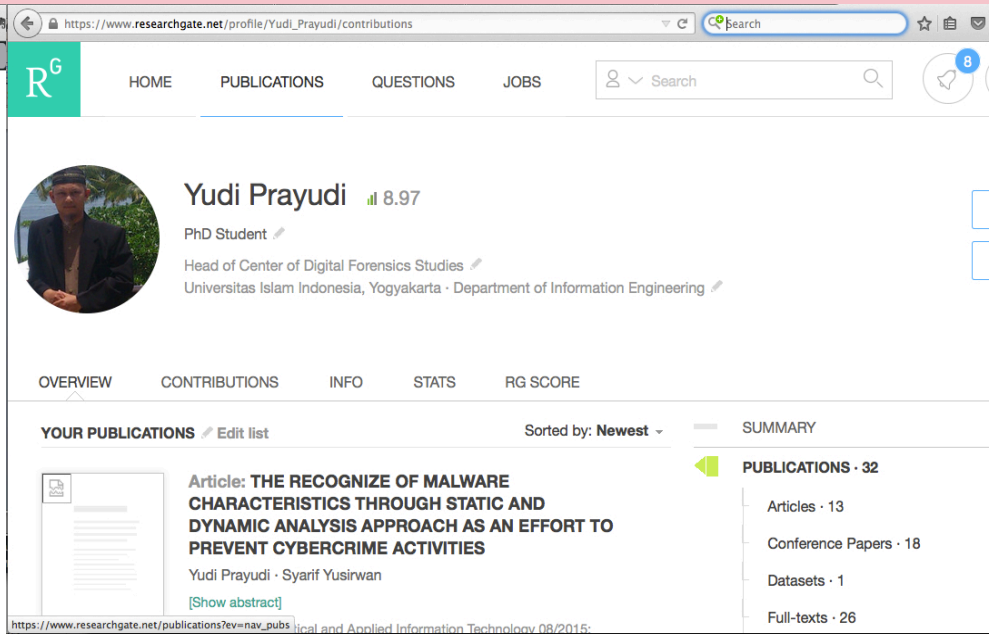
Yudi Prayudi
Pusat Studi Forensika Digital - PUSFID
Universitas Islam Indonesia Yogyakarta

Profile

Yudi Prayudi

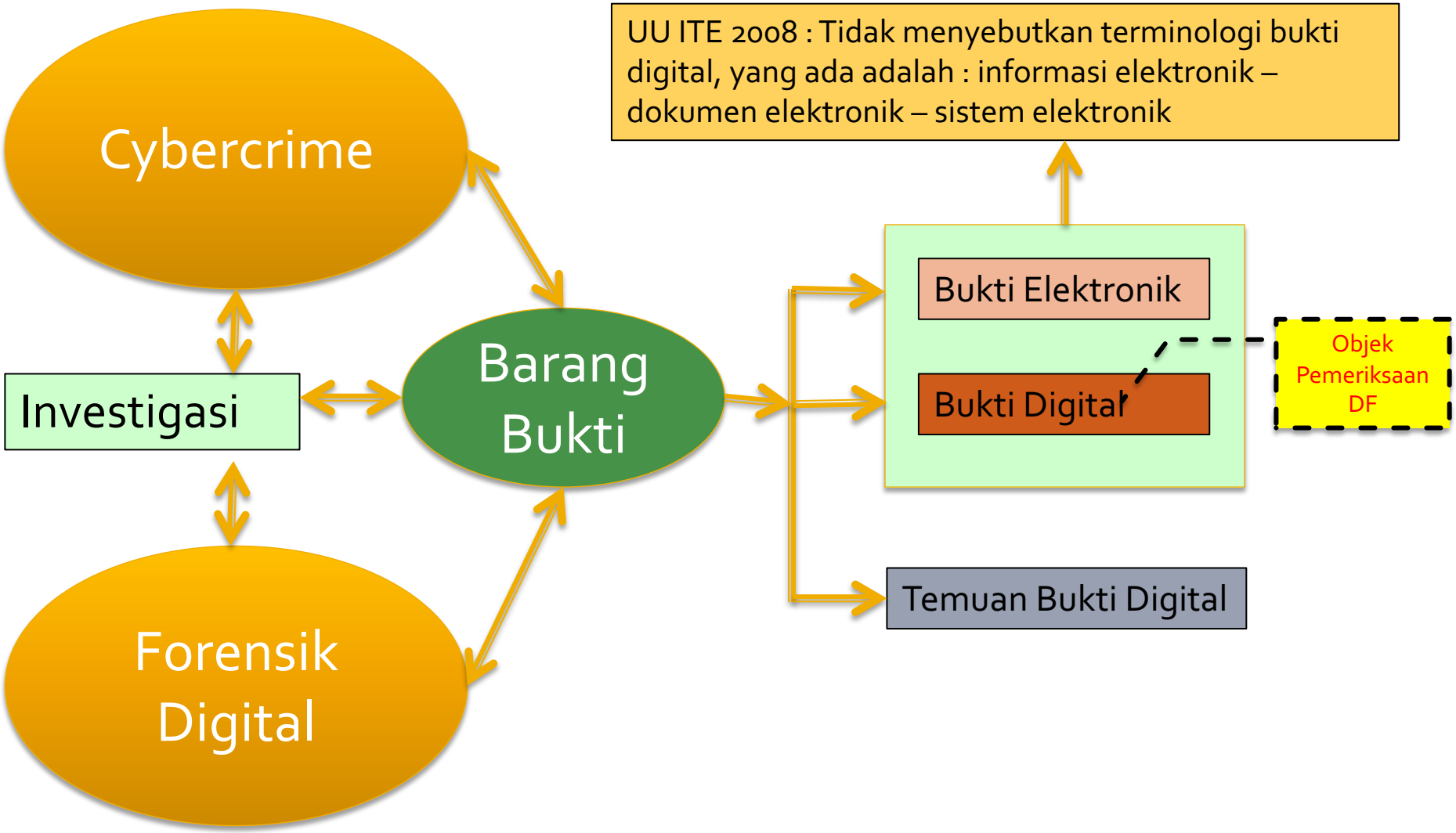
S1 UGM : Computer Graphics
S2 ITS : Image Watermarking and Steganography
S3 UGM: : Digital Evidence Cabinets

- Koordinator Konsentrasi Forensika Digital, Magister Informatika FTI UII Yogyakarta
- Asesor KAN 17025 untuk Lab Digital Forensik
- Kepala Pusat Studi Forensika Digital (PUSFID) UII Yogyakarta
- Editor jurnal Internasional forensic : IJDCF, IJESDF, IJISP



Latar Belakang

Terminologi



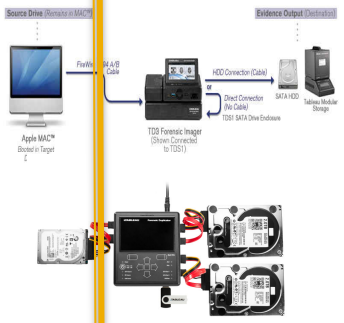
Latar Belakang

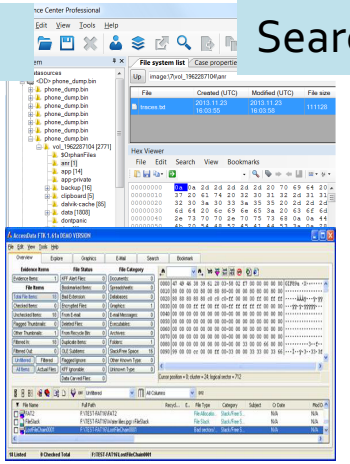
Bukti Elektronik – Bukti Digital

Bukti Elektronik	Bukti Digital	Temuan Bukti Digital
Multimedia File	Audio, Image, Video,	Analisa Orisinalitas, Fakta

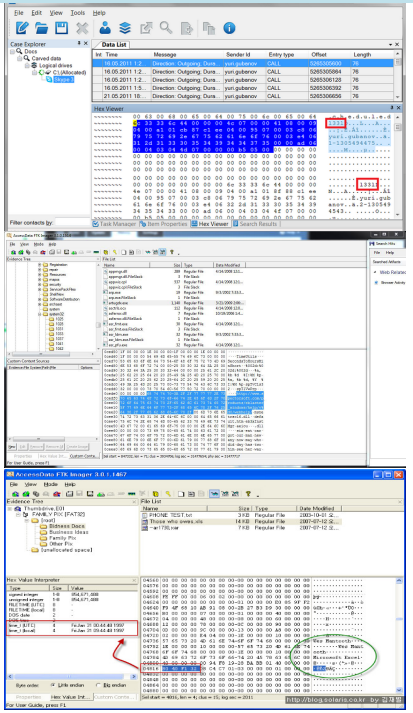
Offline

Akuisisi dan Imaging



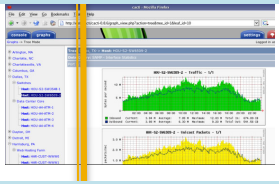


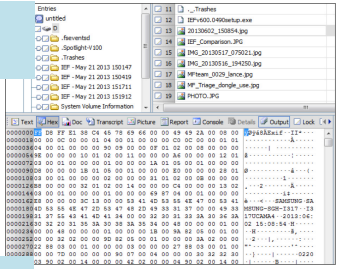
Searching - Eksplorasi dan Analisa



Online

Capture, record, log

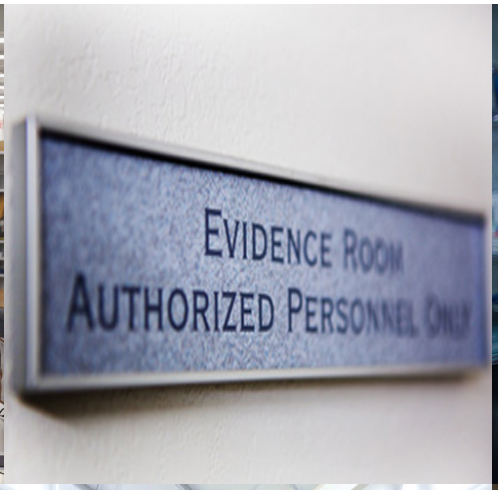


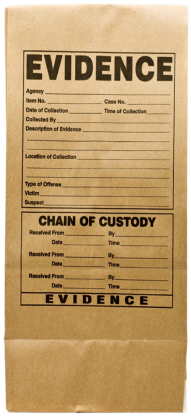


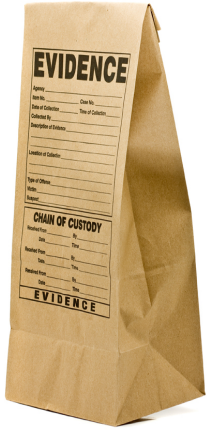
Akuisisi dan Imaging

Latar Belakang

Penanganan Barang Bukti Fisik







Latar Belakang

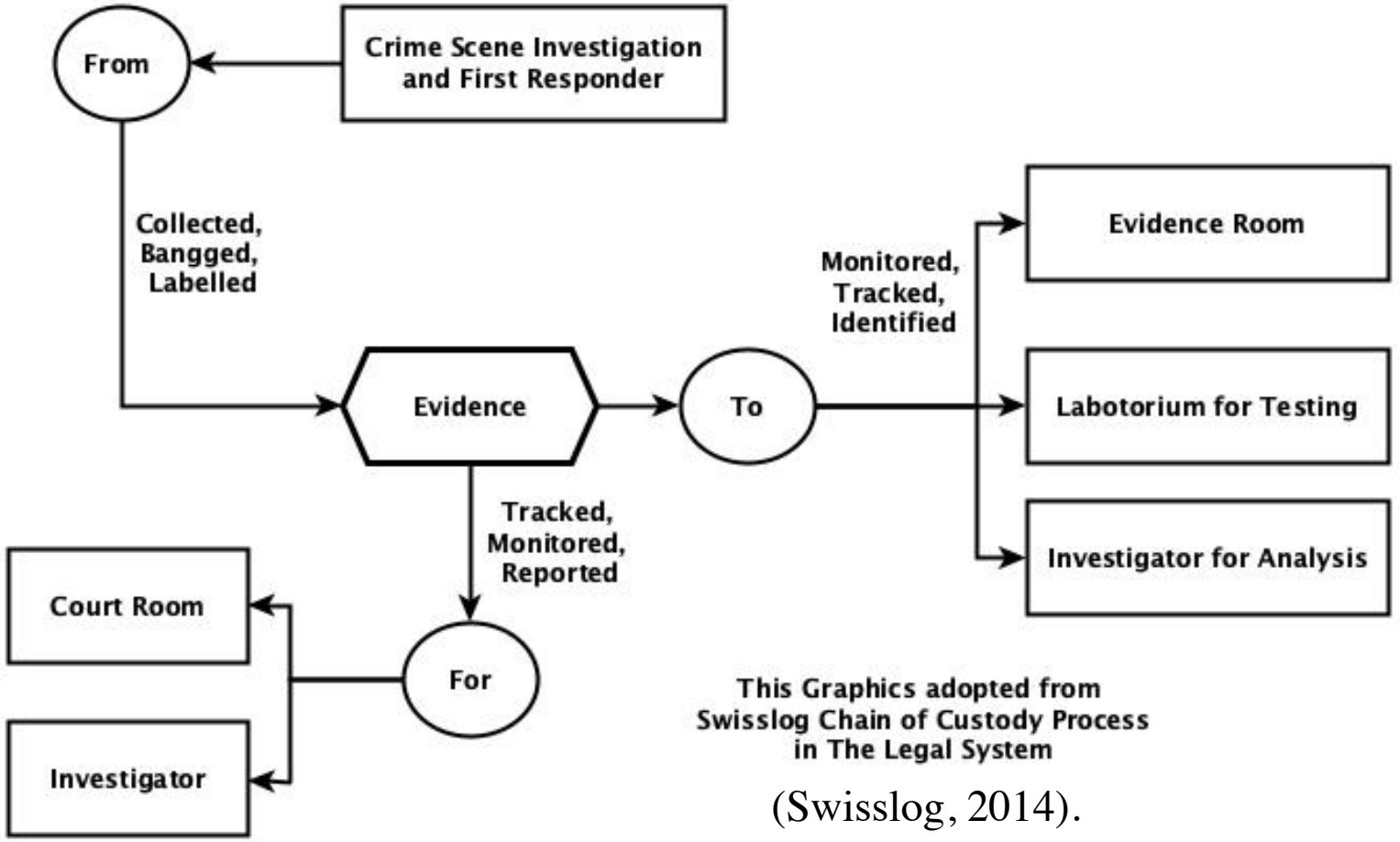
Chain of Custody

Chain of custody adalah sebuah prosedur untuk secara kronologis melakukan pendokumentasian terhadap barang bukti serta pencatatan interaksi terhadapnya Giova (2011).

Chain Of Custody adalah: " *A Road Map That Shows how evidence was collected, analyzed and preserved in order to presented as evidence in court*" Vacca (2005).

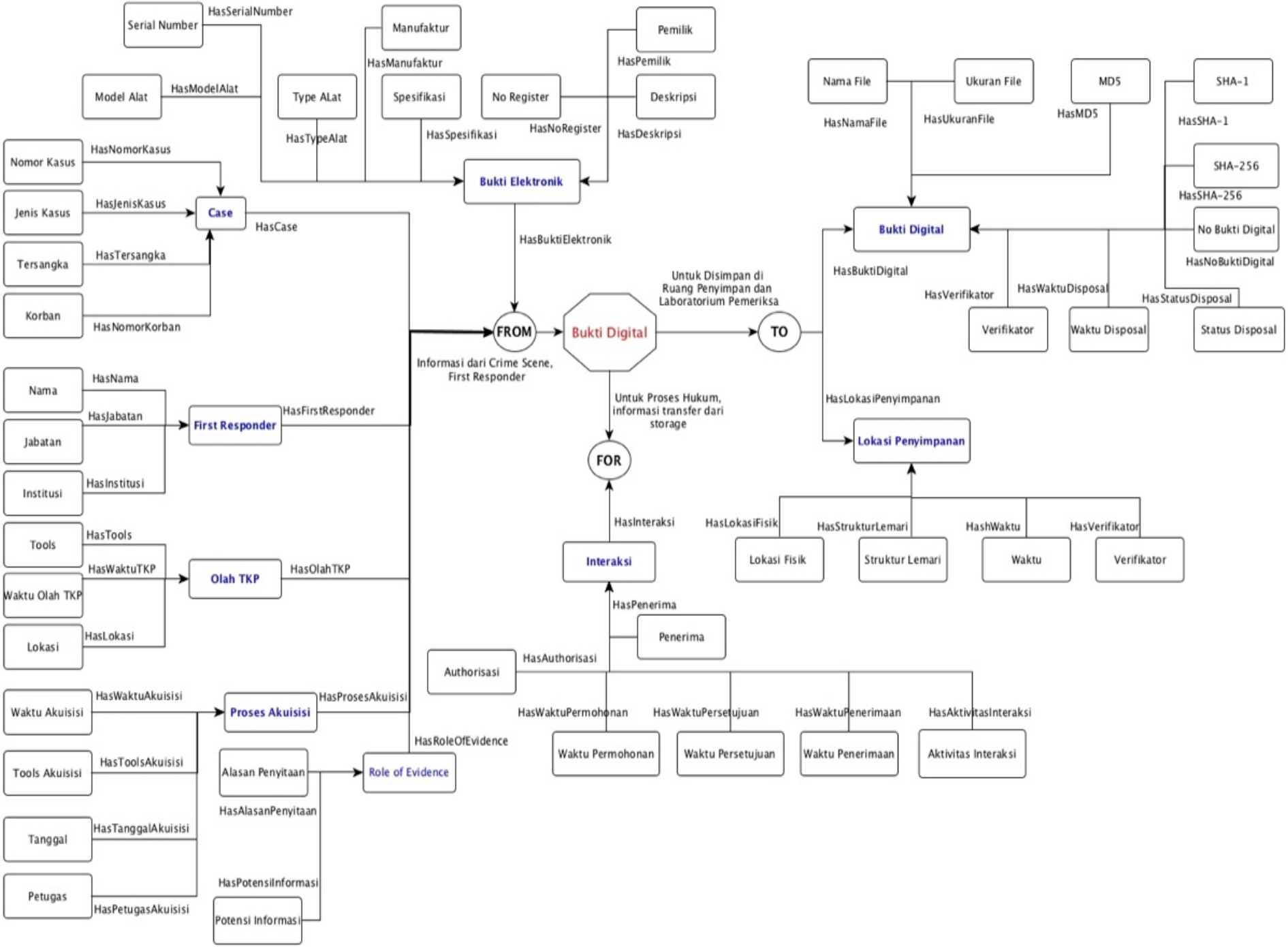
Latar Belakang

Fungsi Chain of Custody



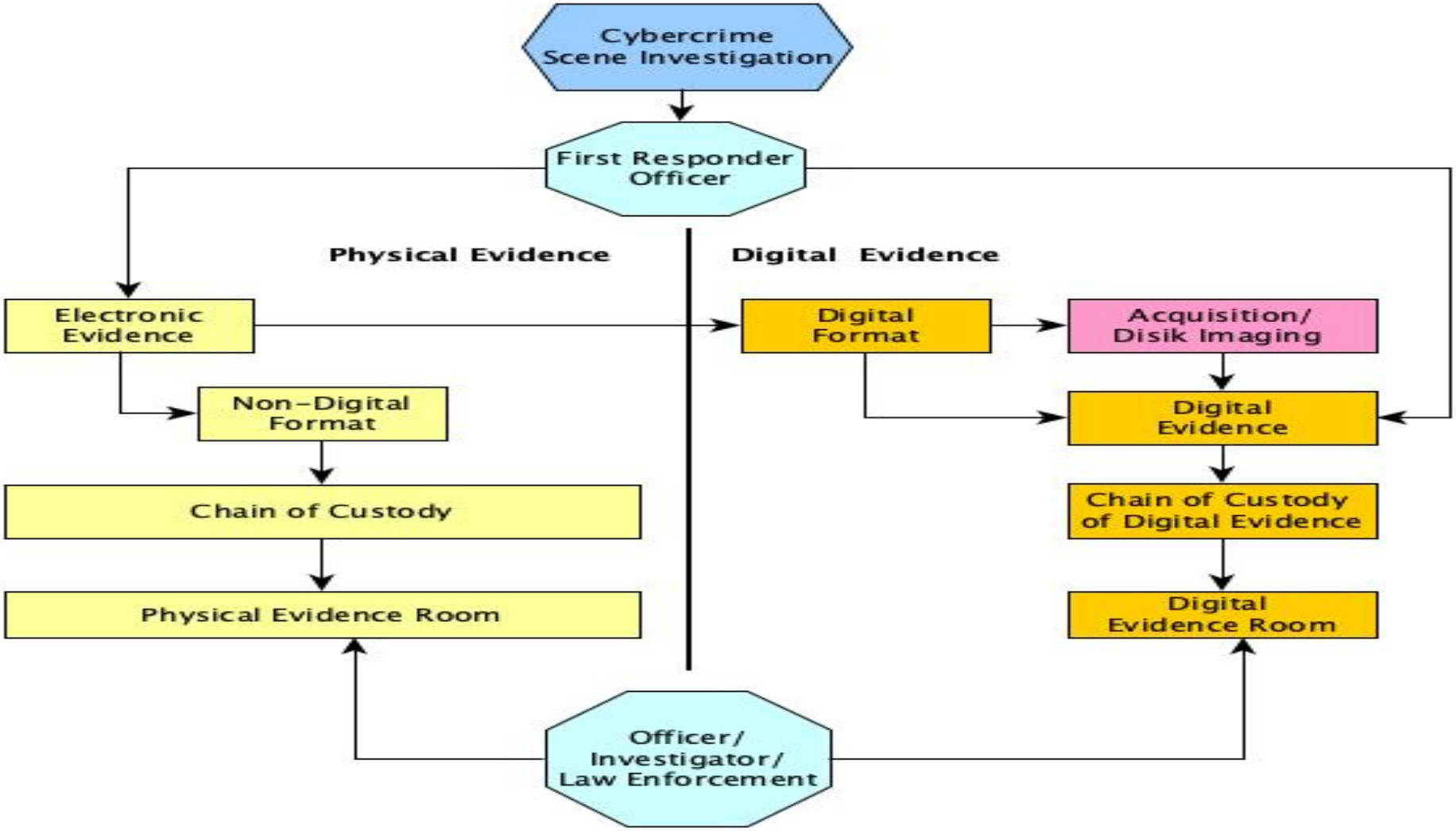
This Graphics adopted from Swisslog Chain of Custody Process in The Legal System

(Swisslog, 2014).


Serial Number
HasSerialNumber
Manufaktur
HasManufaktur
Pemilik
HasPemilik
Model Alat
HasModelAlat
Type ALat
HasTypeAlat
Spesifikasi
HasSpesifikasi
No Register
HasNoRegister
Deskripsi
HasDeskripsi
Bukti Elektronik
Nama File
HasNamaFile
Ukuran File
HasUkuranFile
MD5
HasMD5
SHA-1
HasSHA-1
SHA-256
HasSHA-256
Nomor Kasus
HasNomorKasus
Jenis Kasus
HasJenisKasus
Case
HasCase
Tersangka
HasTersangka
Korban
HasNomorKorban
HasBuktiElektronik
Bukti Digital
HasBuktiDigital
No Bukti Digital
HasNoBuktiDigital
HasVerifikator
HasWaktuDisposal
HasStatusDisposal
Verifikator
Waktu Disposal
Status Disposal
Untuk Disimpan di Ruang Penyimpan dan Laboratorium Pemeriksa
FROM
Bukti Digital
TO
Informasi dari Crime Scene, First Responder
Untuk Proses Hukum, informasi transfer dari storage
FOR
HasLokasiPenyimpanan
Lokasi Penyimpanan
Nama
HasNama
Jabatan
HasJabatan
Institusi
HasInstitusi
First Responder
HasFirstResponder
HasInteraksi
HasLokasiFisik
HasStrukturLemari
HashWaktu
HasVerifikator
Interaksi
Lokasi Fisik
Struktur Lemari
Waktu
Verifikator
Tools
HasTools
Waktu Olah TKP
HasWaktuTKP
Lokasi
HasLokasi
Olah TKP
HasOlahTKP
HasPenerima
Penerima
Authorisasi
HasAuthorisasi
HasWaktuPermohonan
HasWaktuPersetujuan
HasWaktuPenerimaan
HasAktivitasInteraksi
Waktu Permohonan
Waktu Persetujuan
Waktu Penerimaan
Aktivitas Interaksi
Waktu Akuisisi
HasWaktuAkuisisi
Proses Akuisisi
HasProsesAkuisisi
HasRoleOfEvidence
Tools Akuisisi
HasToolsAkuisisi
Alasan Penyitaan
Role of Evidence
HasAlasanPenyitaan
Tanggal
HasTanggalAkuisisi
Petugas
HasPetugasAkuisisi
HasPotensiInformasi
Potensi Informasi

Permasalahan

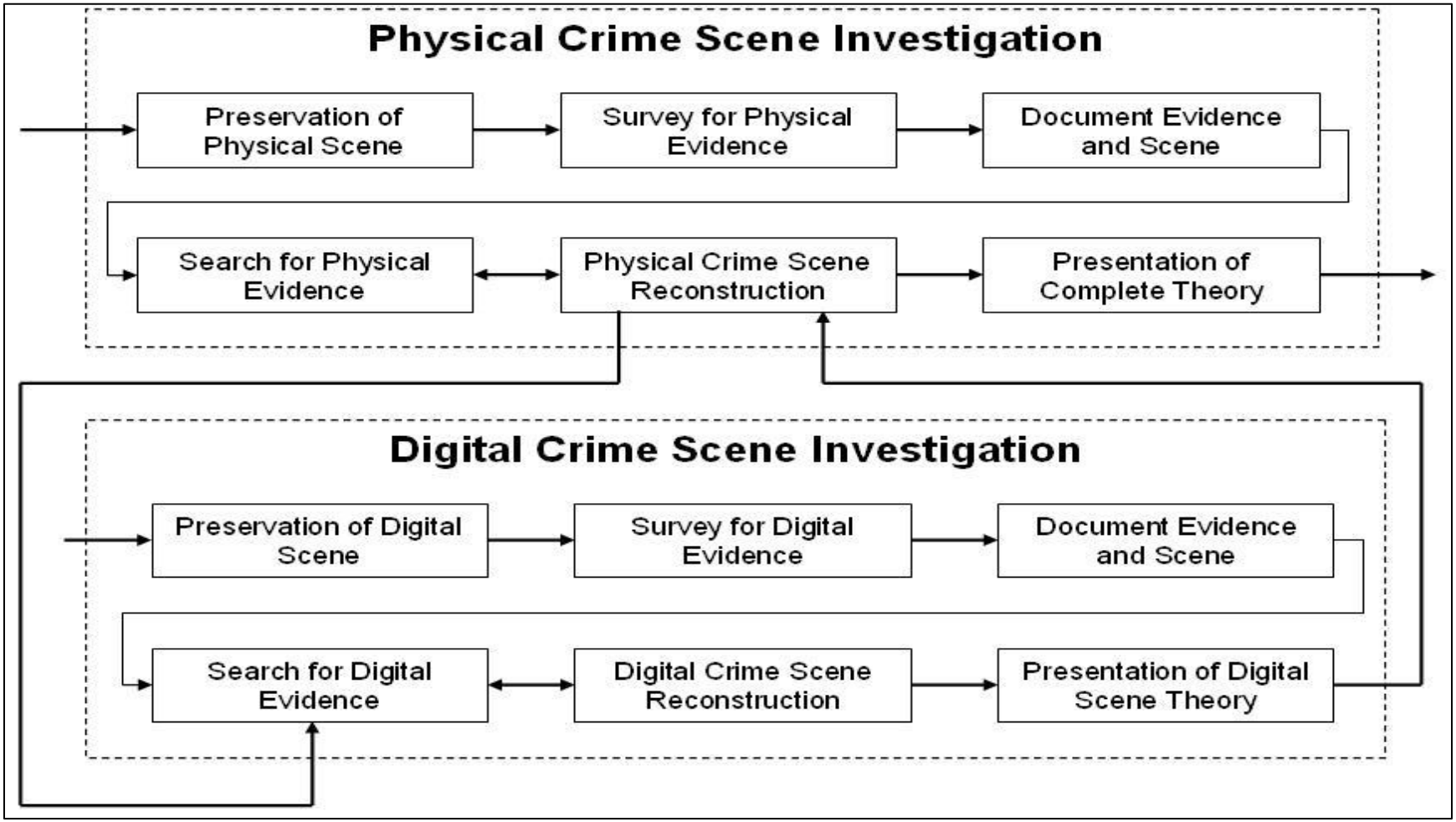
Bukti Elektronik (Fisik) dan Bukti Digital



Masalah

- Sejumlah regulasi standar dalam hal penanganan bukti digital, seperti ACPO, NIJ atau ISO 27037, tidak menjelaskan dengan detail tentang mekanisme penyimpanan bukti digital (ACPO, 2012; Ashcroft dkk., 2004; BSN, 2014).
- Bahkan terminologi yang masih digunakan adalah definisi bukti digital dalam konteks perangkat elektronik (fisik).
- Perlu kajian dikalangan penegak hukum tentang mekanisme untuk penanganan bukti digital agar bisa sejalan dengan penanganan barang bukti fisik.

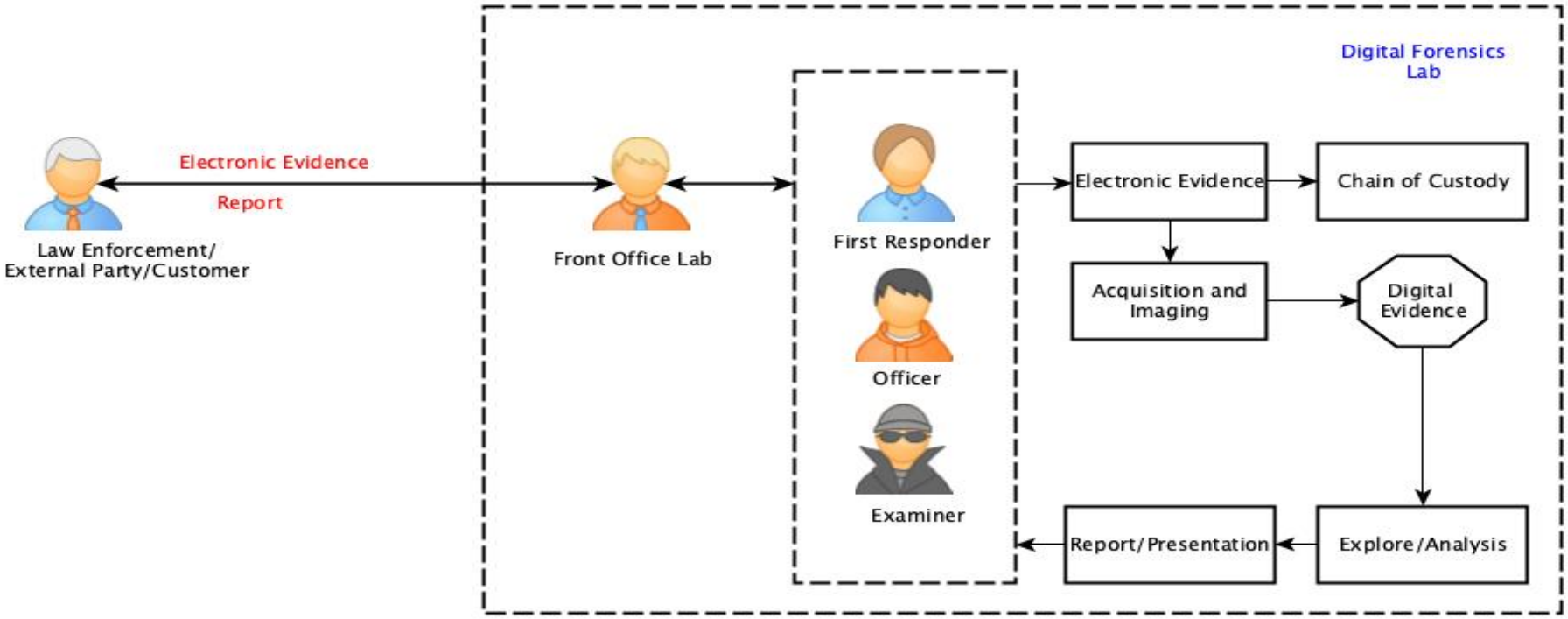
Kesatuan Penanganan BB



(Carrier dan Spafford, 2003)

Permasalahan

Temuan Lapangan



Aktivitas yang mendukung pencatatan informasi bukti digital dan kontrol aksesibilitas masih belum menjadi perhatian para pemeriksa atau praktisi forensik digital. Aspek penyimpanan, pencatatan informasi dan kontrol aksesibilitas terhadap bukti digital umumnya hanya diterapkan untuk kepentingan dokumentasi barang bukti fisik semata, namun tidak pada bukti digital.

Permasalahan

CHAIN OF CUSTODY

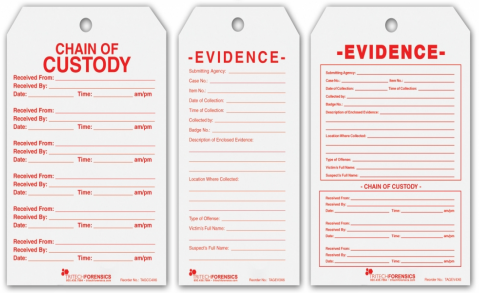
Regulasi:
pada Perkap 10/2010 dan Perkap 8/2014 serta ISO 27037.

Bukti Elektronik / Fisik

Bukti Digital

Kantong Barang Bukti

?



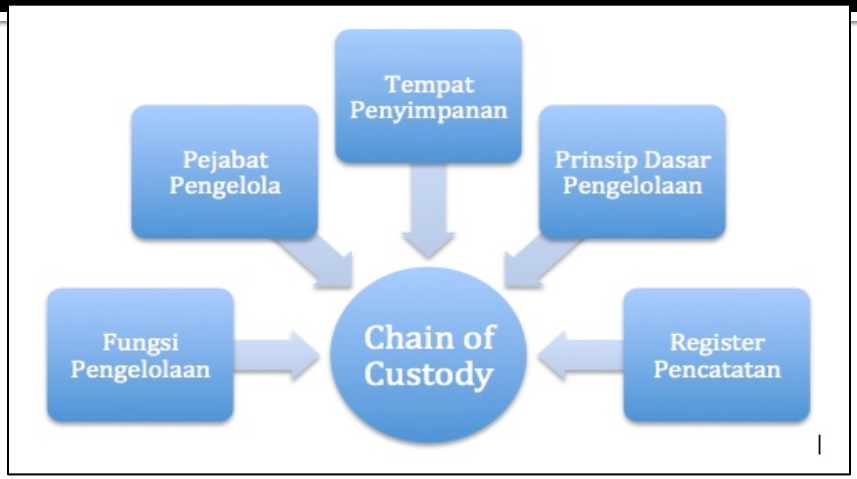
Chain of Custody

?

Solusi

Aturan Penanganan Barang bukti Fisik

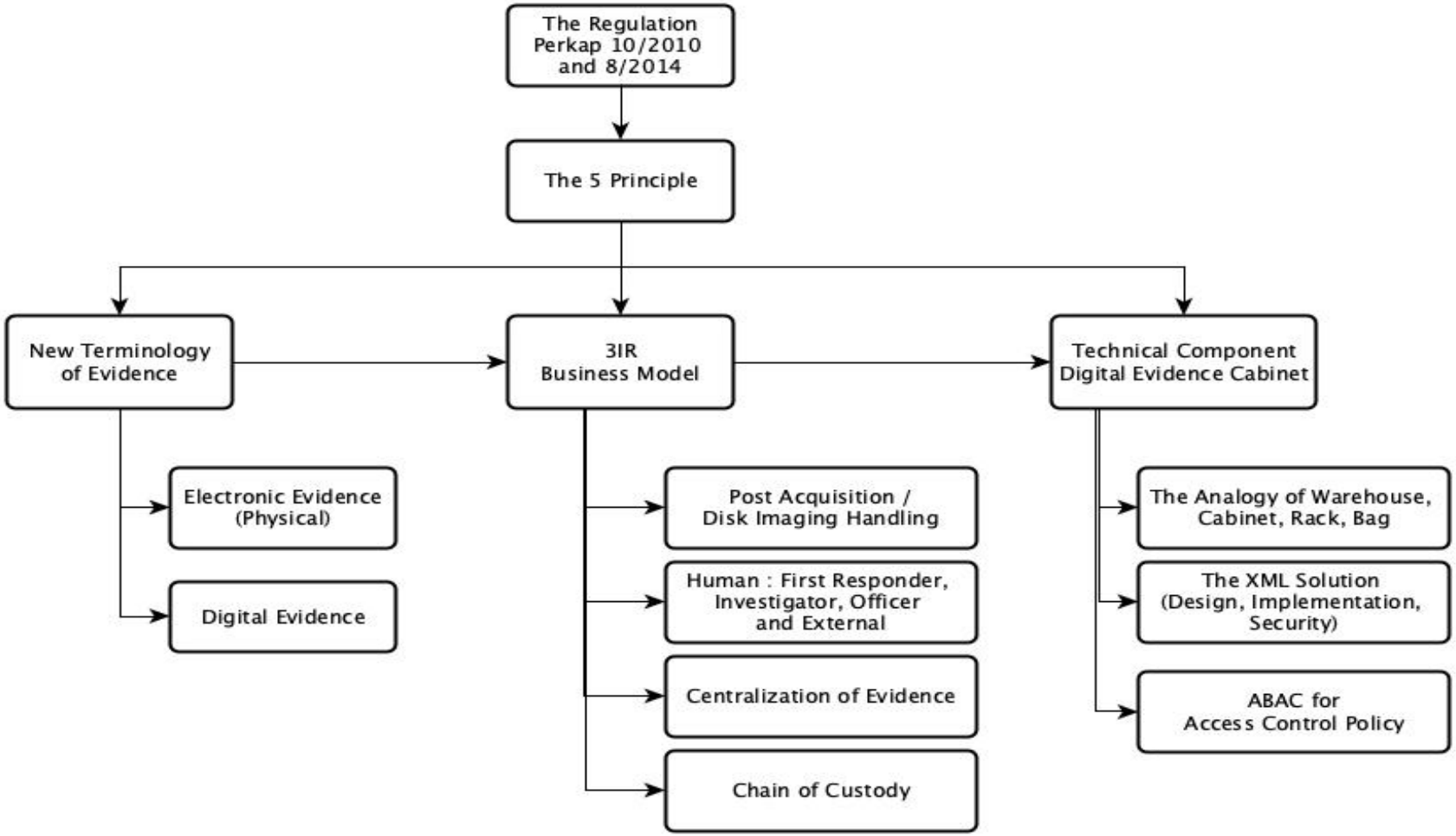
Perkap 10/2010 tentang Tata Cara Pengelolaan Barang Bukti



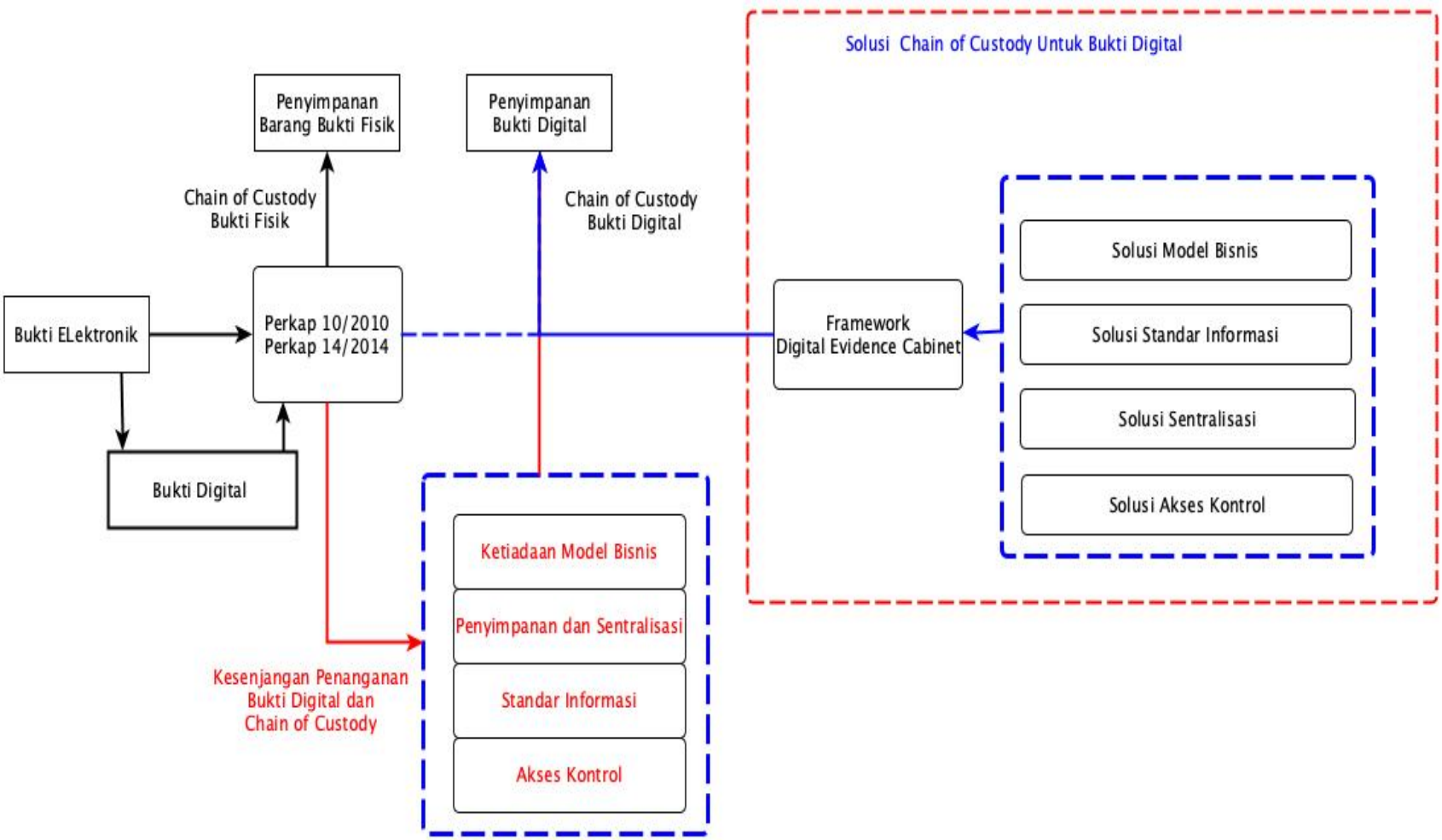
1. Memenuhi fungsi pengelolaan, yaitu: meliputi tata cara atau proses penerimaan, penyimpanan, pengamanan, perawatan, pengeluaran dan pemusnahan benda sitaan dari ruang atau tempat khusus penyimpanan barang bukti.
2. Adanya pejabat yang memiliki kewenangan untuk menerima, menyimpan, mengamankan, merawat, mengeluarkan dan memusnahkan benda sitaan dari ruang atau tempat khusus penyimpanan barang bukti.
3. Adanya tempat khusus untuk penyimpanan barang bukti berdasarkan sifat dan jenisnya.
4. Adanya prinsip-prinsip pengelolaan barang bukti: legalitas, transparan, akuntabel dan efektif.
5. Adanya kewajiban untuk melakukan pencatatan ke dalam buku register dan disimpan pada tempat penyimpanan barang bukti

Solusi

Pendekatan Berbasis Regulasi



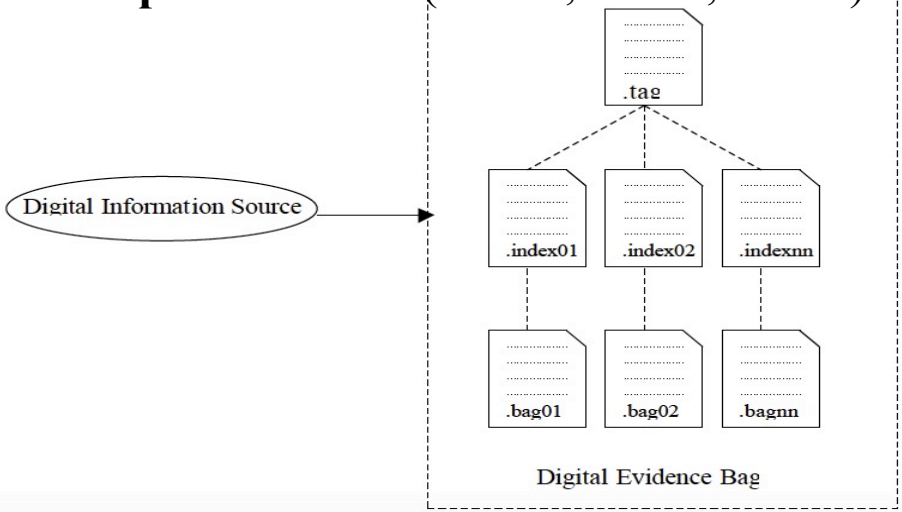
Ide Solusi

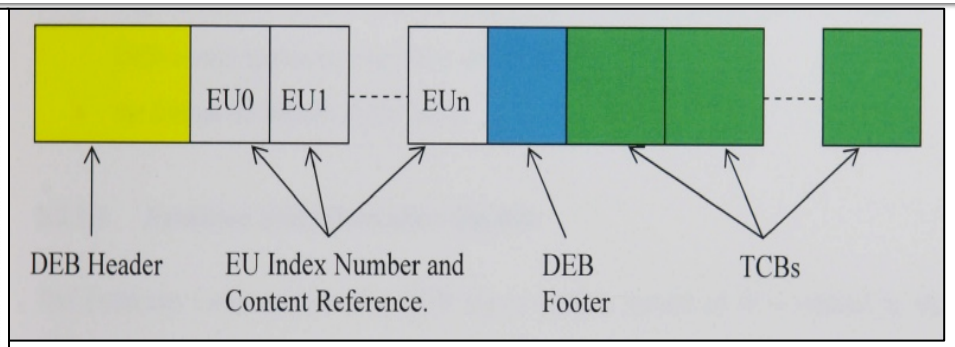

Solusi Chain of Custody Untuk Bukti Digital
Penyimpanan Barang Bukti Fisik
Penyimpanan Bukti Digital
Chain of Custody Bukti Fisik
Chain of Custody Bukti Digital
Bukti ELektronik
Perkap 10/2010 Perkap 14/2014
Framework Digital Evidence Cabinet
Solusi Model Bisnis
Solusi Standar Informasi
Solusi Sentralisasi
Solusi Akses Kontrol
Bukti Digital
Ketiadaan Model Bisnis
Penyimpanan dan Sentralisasi
Standar Informasi
Akses Kontrol
Kesenjangan Penanganan Bukti Digital dan Chain of Custody

Pustaka

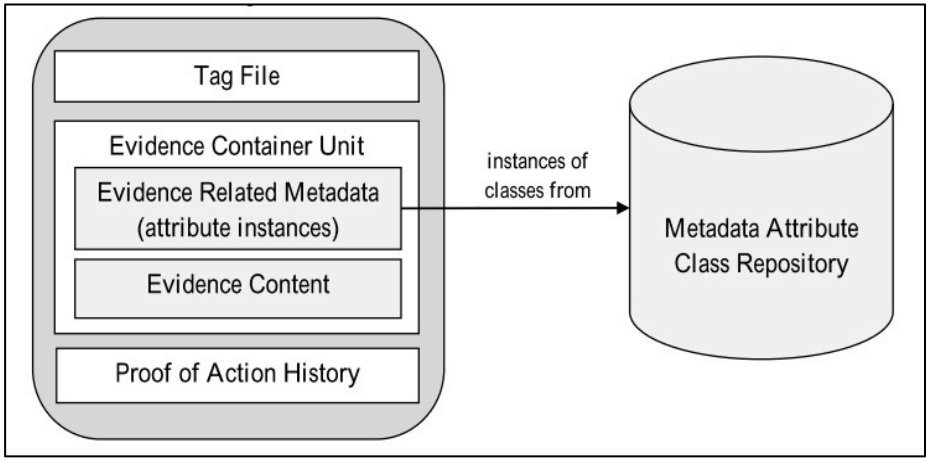
Digital Evidence Bag

Konsep Dasar DEB (Turner, 2008a, 2005b)





Digital Evidence Container Souza (2013)



Solusi penyimpanan bukti digital secara imaginer melalui analogi kantong dan label pencatatan oleh Turner (2008a, 2005b).Pendekatan DEB mengarah pada solusi struktur file yang dihasilkan dari proses *imaging*. Komponen utama DEB berupa Tag, Index dan Bag diimplementasikan lewat 4 bagian format file berupa : *DEB Header, Evidence Unit, DEB Footer* dan *Tag Continuity Block* (TCB).

Modeling DF

DF = {I_{PS}, D_{OS}, C_{OS}, **(E, A, R)**$_{WC}$}, dimana:

I: Identifikasi bukti elektronik/ digital (*Identification*) terhadap *Primary Source* (PS)

D: Sentralisasi penyimpanan bukti digital melalui *Digital Evidence Cabinet* (DEC) untuk objek *Original Source* (OS)

C: Chain of Custody Bukti Digital (*Chain of Custody*) untuk objek *Original Source* (OS)

E: Eksplorasi Bukti Digital (*Exploration*) untuk objek *Working Copy* (WC)

A: Analisa bukti digital (*Analyze*) untuk objek *Working Copy* (WC)

R: Presentasi/ Laporan bukti digital (*Report*) untuk objek *Working Copy* (WC)

DF = **{Pi [DE** $_{WC}$**, Tj, Lk] , Ci[DE**$_{OS}$**]i}**, dimana :

Pi: Proses pemeriksaan bukti digital

DE_{WC}: Working Copy dari Bukti Digital

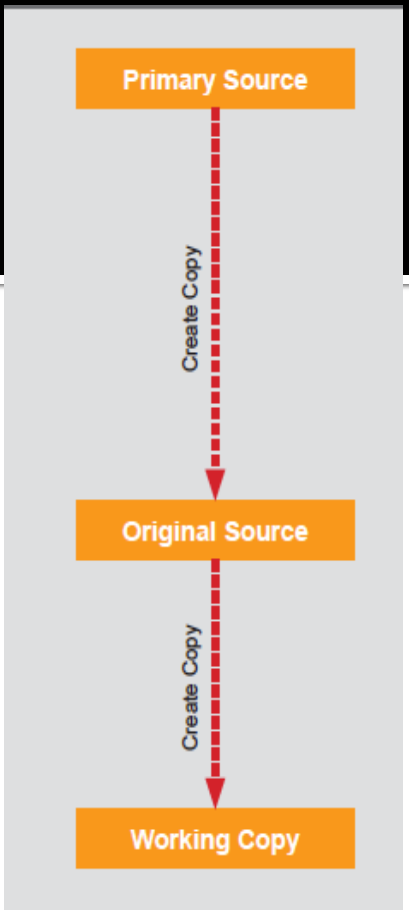
Tj: Teknik, Metode, Pendekatan, Sistim, Tools yang digunakan

Lk: Aspek Legal yang relevan

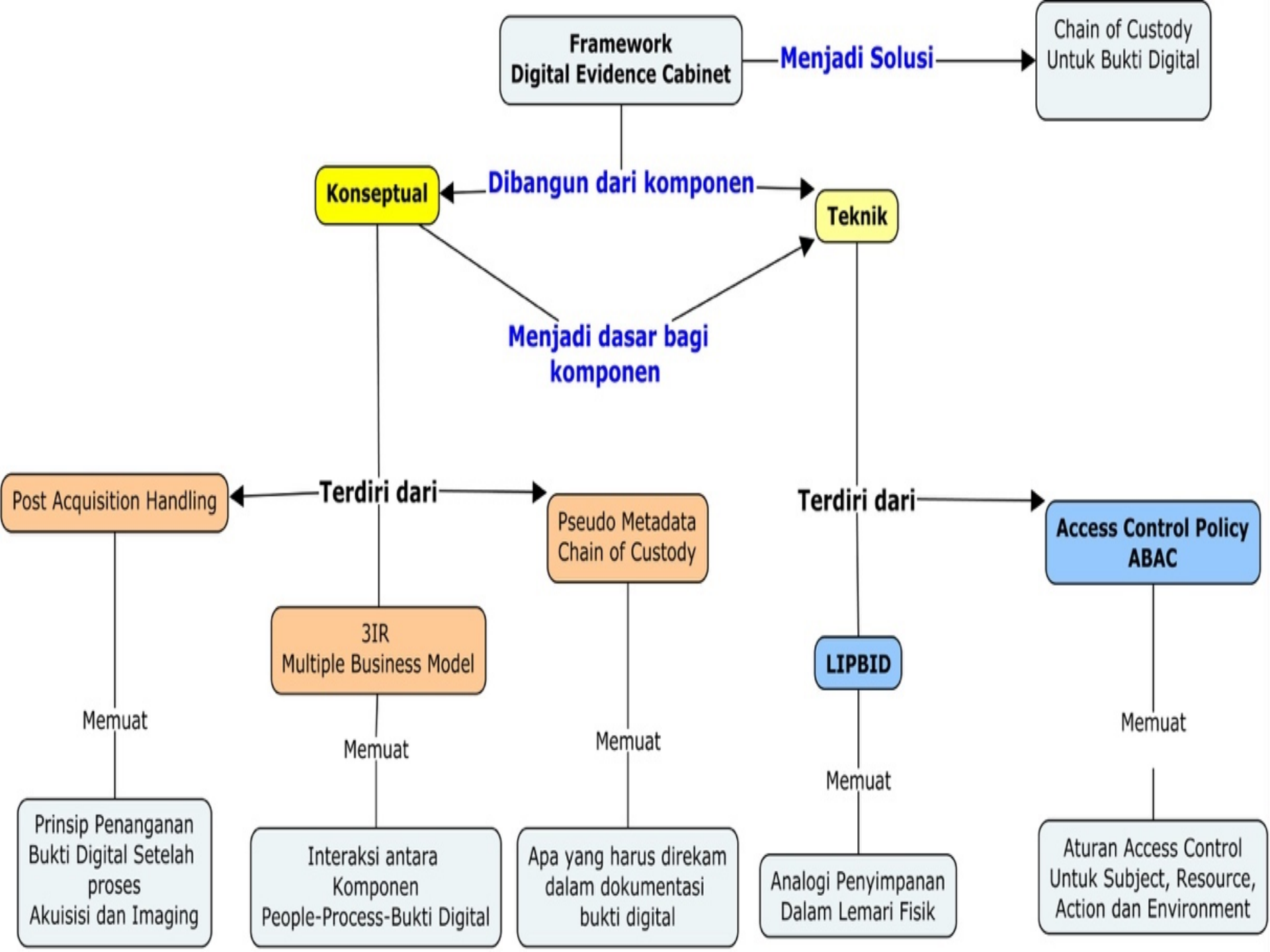
C: Chain of Custody untuk bukti digital

DE_{OS}: Original Source dari Bukti Digital

Model CoC

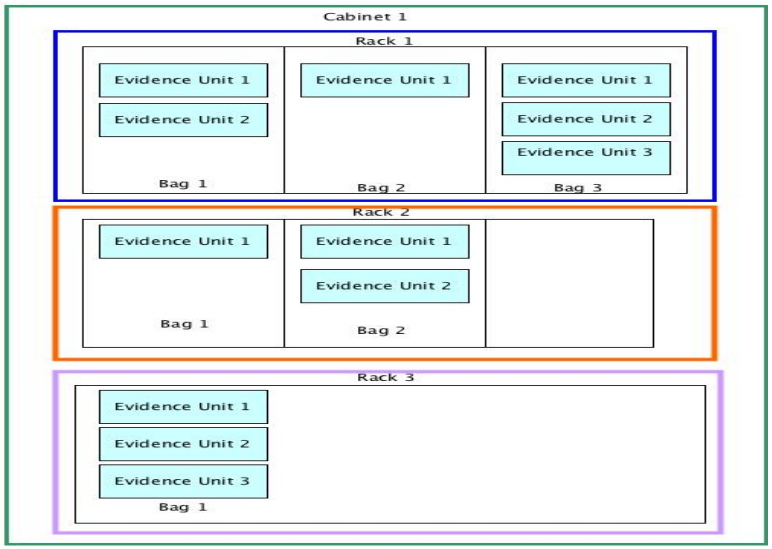


Pemeriksaan bukti digital akan melibatkan *working copy* dari bukti digital, teknik tertentu, serta aspek legal yang relevan. Pemeriksaan terhadap bukti digital didukung oleh *chain of custody* dari bukti digital pada *original source* yang tersimpan dalam *Digital Evidence Cabinet*.


Framework
Digital Evidence Cabinet
Menjadi Solusi
Chain of Custody
Untuk Bukti Digital
Konseptual
Dibangun dari komponen
Teknik
Menjadi dasar bagi
komponen
Post Acquisition Handling
Terdiri dari
Pseudo Metadata
Chain of Custody
Terdiri dari
Access Control Policy
ABAC
3IR
Multiple Business Model
LIPBID
Memuat
Memuat
Memuat
Memuat
Memuat
Prinsip Penanganan
Bukti Digital Setelah
proses
Akuisisi dan Imaging
Interaksi antara
Komponen
People-Process-Bukti Digital
Apa yang harus direkam
dalam dokumentasi
bukti digital
Analogi Penyimpanan
Dalam Lemari Fisik
Aturan Access Control
Untuk Subject, Resource,
Action dan Environment

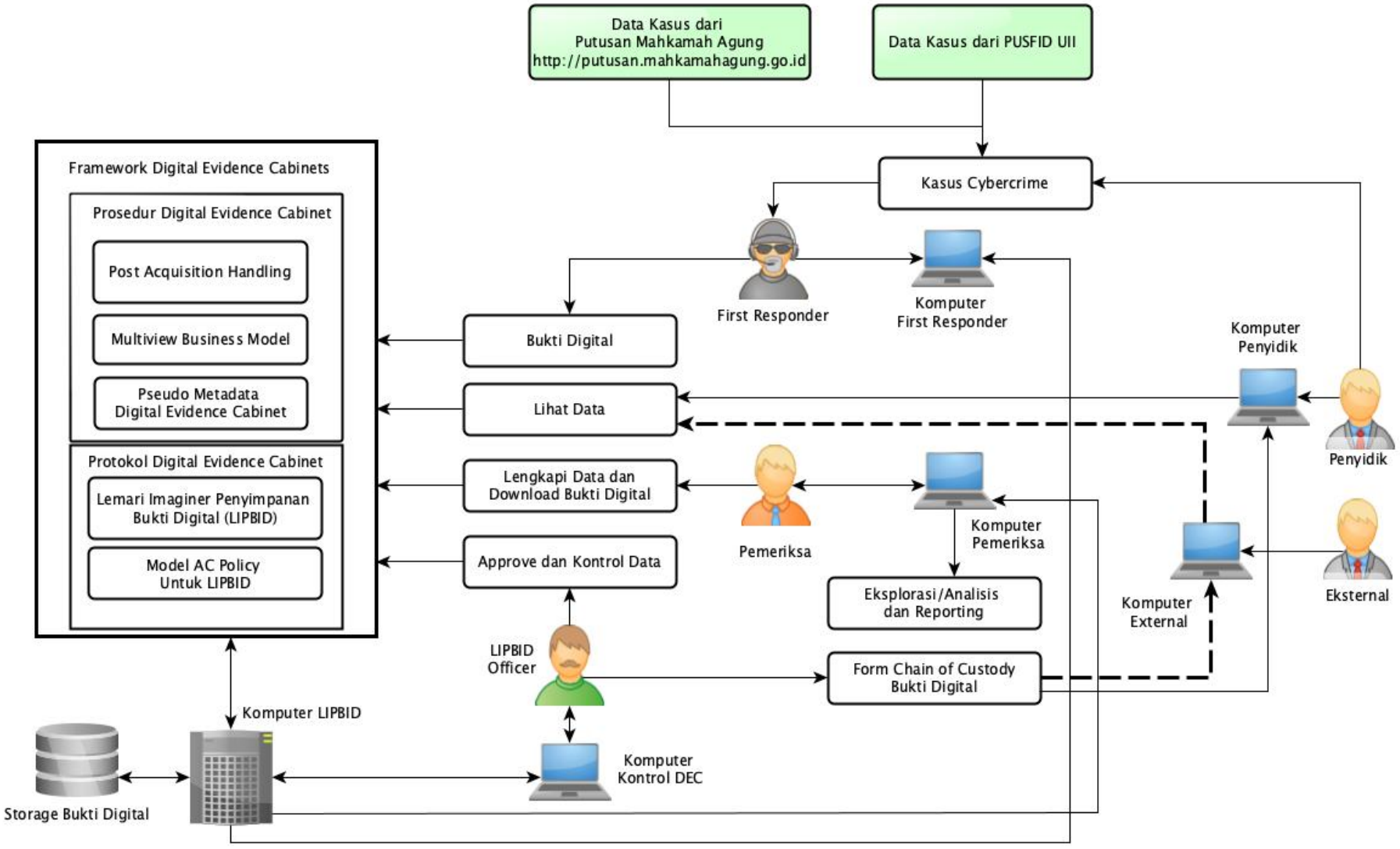
Framework

Sentralisasi
Lemari Imaginer Penyimpanan Bukti Digital

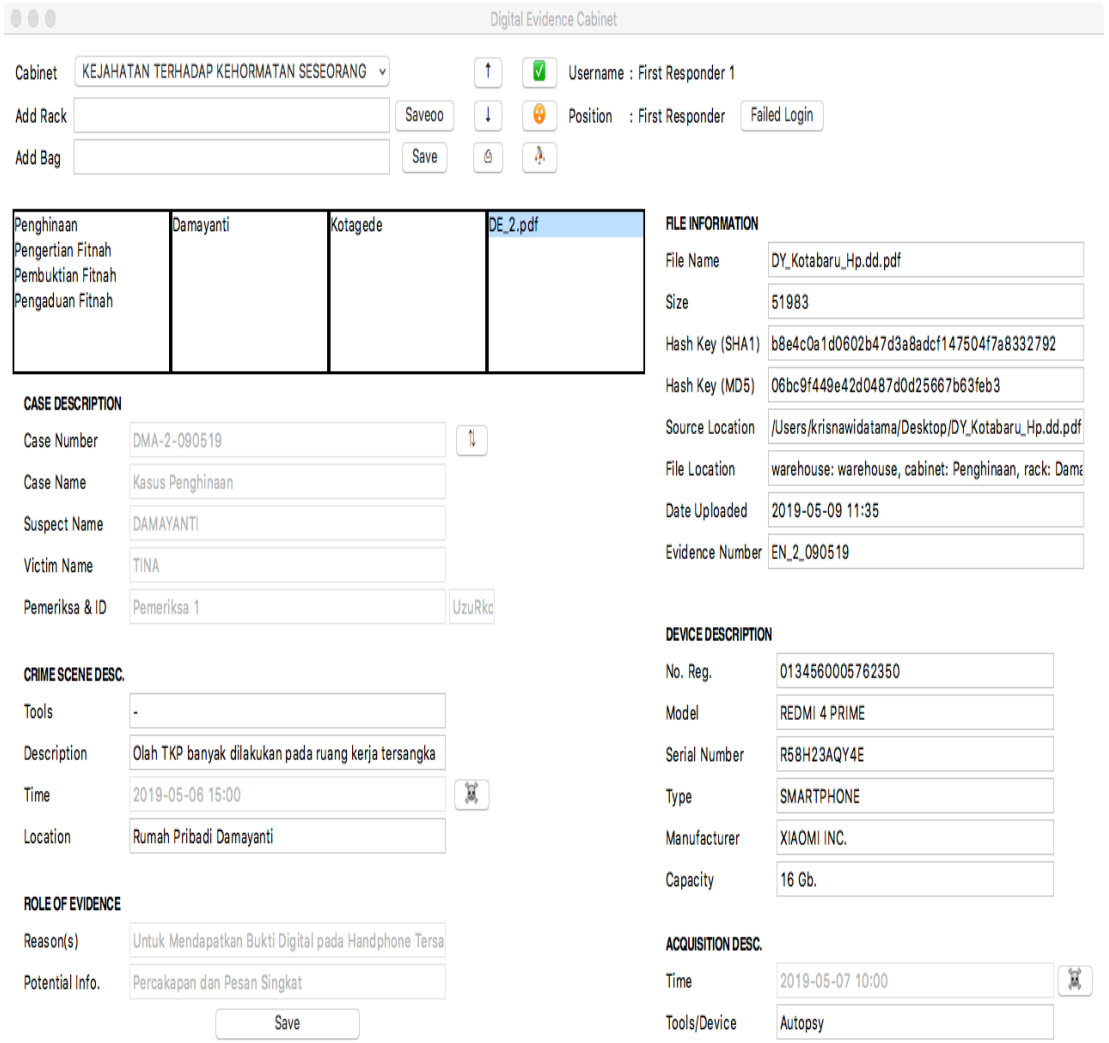


Warehouse: Laboratorium Forensika Digital FTI UII				
Lemari	**Rak**	**Kantong**	**Bukti Digital**	**Identifikasi**
Pemalsuan Surat	Damayanti	Kaliurang	1. Handphone	– Samsung Galaxy A20 – IMEI: 821209033352007
			Repository: /user/data/DEIC/case1/evidence1.dat	
			2. Dekstop	– ACER Veriton VZ4660G-D – Harddisk merk: WD Black 2TB WD2003FZEX
			Repository: user/data/DEIC/case1/evidence2.dat	

Komponen Lemari Imaginer	**Analogi Penerapannya**	**Keterangan**
Warehouse	Laboratorium Forensika Digital UII	Tempat fisik dari lokasi penyimpanan media penyimpan bukti digital
Lemari (Cabinet)	Jenis Pelanggaran/Kasus Sesuai dengan Katagori Kasus/Pelangaran	Berdasarkan KUHP, terdapat 30 Jenis Tindakan Kejahatan (Buku 2, Pasal 104 sd Pasal 485) Misalnya: Jenis Kejahatan: Pemalsuan Surat
Rak (Rack)	Nama Kasus Pada Jenis Pelanggaran yang sama	Misal: Jenis Kejahatan: Pemalsuan Surat Pada kejahatan ini terdapat kasus atasnama: Damayanti
Kantong (Bags)	Tempat TKP/Lokasi Mendapatkan barang bukti	Misal: Jenis Kejahatan: Pemalsuan Surat Pada kejahatan ini terdapat kasus atasnama: Damayanti TKP barang bukti: Kaliurang
Barang Bukti (Evidence Unit)	Jenis barang bukti pada TKP yang sama	Misal: Jenis Kejahatan: Pemalsuan Surat Pada kejahatan ini terdapat kasus atasnama: Damayanti TKP barang bukti: Kaliurang Barang bukti: Handphone dan USB
Identitas Bukti Digital (Evidence Identifier)	Identitas dari bukti elektronik yang menjadi sumber bukti digital	Misal: Jenis Kejahatan: Pemalsuan Surat Pada kejahatan ini terdapat kasus atasnama: Damayanti TKP barang bukti: Kaliurang Barang bukti: Handphone dengan informasi (jenis, spek) dan USB dengan jenis informasi (jenis, spek)
Tempat Penyimpanan (Evidence Repository)	Tempat penyimpanan dari bukti digital	–Bukti Digital Handphone hasil akuisisinya tersimpan di: lokasi folder penyimpanan tertentu. –Bukti USB hasil akuisisinya tersimpan di: lokasi folder penyimpanan tertentu


Data Kasus dari
Putusan Mahkamah Agung
http://putusan.mahkamahagung.go.id
Data Kasus dari PUSFID UII
Framework Digital Evidence Cabinets
Prosedur Digital Evidence Cabinet
Post Acquisition Handling
Multiview Business Model
Pseudo Metadata
Digital Evidence Cabinet
Protokol Digital Evidence Cabinet
Lemari Imaginer Penyimpanan
Bukti Digital (LIPBID)
Model AC Policy
Untuk LIPBID
Kasus Cybercrime
First Responder
Komputer
First Responder
Bukti Digital
Lihat Data
Lengkapi Data dan
Download Bukti Digital
Approve dan Kontrol Data
Komputer
Penyidik
Penyidik
Pemeriksa
Komputer
Pemeriksa
Eksplorasi/Analisis
dan Reporting
Komputer
External
Eksternal
LIPBID
Officer
Form Chain of Custody
Bukti Digital
Komputer LIPBID
Komputer
Kontrol DEC
Storage Bukti Digital

Prototype



CHAIN OF CUSTODY OF DIGITAL EVIDENCE

To be completed by First responder and Investigator

Crime Scene	
Case Name	Kasus Penghinaan
Suspect:	Damayanti
Victim:	Tina
Location	Rumah Tersangka
Time	2019-05-06 07:00
Tools (Live Forensics)	-
Tools Description	Ditemukan di Tas Tersangka dan Tas tersebut ada DI Rumah Pribadi Tersangka
First Responder	First Responder 1
Institution	Institusi First Responder 1

Electronic Evidence	
Register Number	0134560005762350
Type	FLASHDISK
Model	USB
Manufacture	SAMSUNG INC.
Serial Number	Z50J12AYY5A
Foreclosure Reasons	Mencari Bukti Pendukung

Digital Evidence	
Evidence Number	EN_3_090519
Case Number	DMY-3-090519
File Name	DY_Kotabaru_USB.dd.pdf
Time (Acquisition)	2019-05-06 02:05
Device (Acquisition)	EnCase
Size (Byte)	20106
Hashing (SHA1)	5bb19fe8b141ec1916aef4cca08d52bfcae18b71
Hashing (MD5)	28fe4a0280ea61cc969ee3cb23b76e4d
Source	/Users/krisnawidatama/Desktop/DY_Kotabaru_USB.dd.pdf
Cabinet Structure	warehouse: warehouse, cabinet: Penghinaan, rack: Damayanti, bag: Kotagede
Potential Information	MS. Word
Status	Active
Date (Closed)	-
Validator	Officer

Chain Of Custody Record

Date/Time		Accessed by
Accessed	2019-05-09 14:53	Officer
Action: Viewing Details		
Date/Time		**Accessed by**
Accessed	2019-05-09 14:54	First Responder 1
Action: Viewing Details		
Date/Time		**Accessed by**
Accessed	2019-05-09 14:54	First Responder 1
Action: Viewing Details		
Date/Time		**Authorized by**
Requested	2019-05-09 14:58	Officer
Approved	2019-05-09 14:58	**Submitted by**
Received	---	First Responder 1/Institusi First Responder 1
Action: Added Data		
investigator	UzuRko	
tools_cs	-	
desc_cs	Ditemukan di Tas Tersangka dan Tas tersebut ada DI Rumah Pribadi Tersangka	
time_cs	2019-05-06 07:00	
location_cs	Rumah Tersangka	
reg_number	0134560005762350	
device_model	USB	
serial_number	Z50J12AYY5A	
device_type	FLASHDISK	
manufacturer	SAMSUNG INC.	
capacity	64 Gb.	
acquisition	2019-05-06 02:05	
tools_acq	EnCase	

Solusi Penanganan BBE

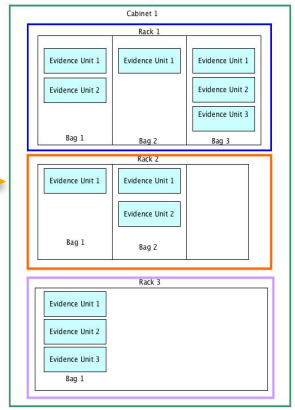
CHAIN OF CUSTODY

Regulasi:
pada Perkap 10/2010 dan Perkap 8/2014 serta ISO 27037.

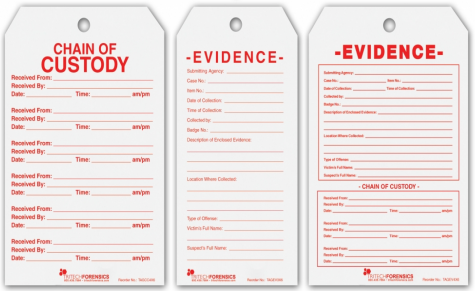
Bukti Elektronik / Fisik

Bukti Digital

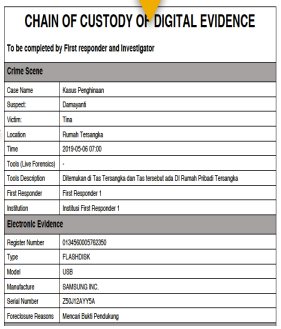
Kantong Barang Bukti



Digital Evidence Cabinet



Chain of Custody



CHAIN OF CUSTODY OF DIGITAL EVIDENCE

To be completed by First responder and Investigator

Crime Scene	
Case Name	Kasus Penghinaan
Suspect:	Damayanti
Victim:	Tina
Location	Rumah Tersangka
Time	2013-05-06 07:00
Tools (Live Forensics)	-
Tools Description	Ditemukan di Tas Tersangka dan Tas tersebut ada Di Rumah Pribadi Tersangka
First Responder	First Responder 1
Institution	Institusi First Responder 1
Electronic Evidence	
Register Number	01345600057823S0
Type	FLASHDISK
Model	USB
Manufacture	SAMSUNG INC.
Serial Number	Z5GJ12AYY5A
Foreclosure Reasons	Mencari Bukti Pendukung

Komponen Solusi

- Post Acquisition → Adanya pola fikir baru dalam hal penanganan awal bukti digital dengan fokus pada objek hasil akuisisi/disk imagining/file biner.
- Model Bisnis → Ada peran yang jelas dari 4 katagori pihak yang berinteraksi dengan bukti digital.
- Pseudo Metadata → Adanya rujukan informasi untuk kepentingan *chain of custody* bukti digital dalam bentuk elemen dan schema metadata statis dan dinamis.

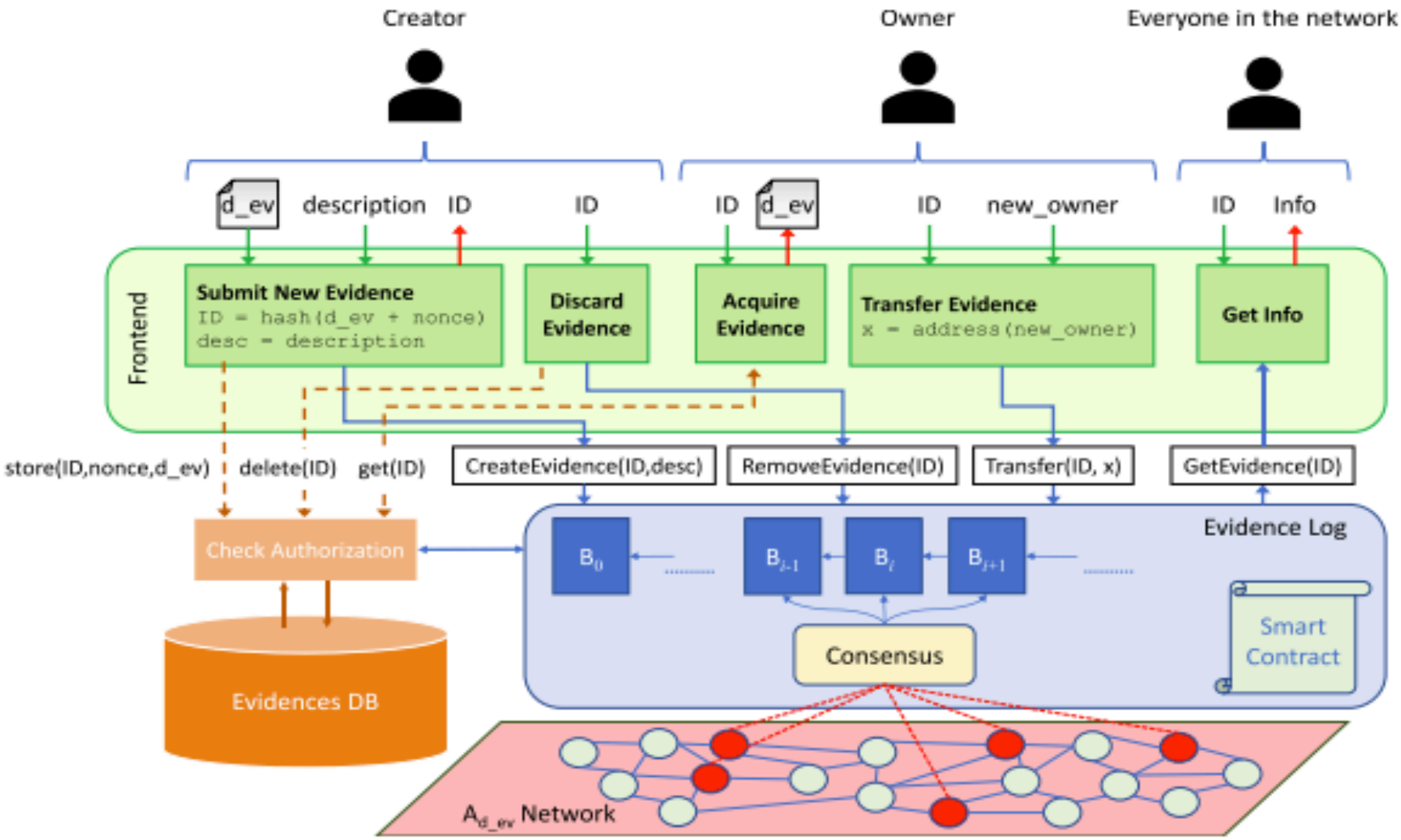
Komponen Prosedur

Komponen Teknis

- Lemari Imaginer → Adanya manajemen penyimpanan bukti digital yang lebih terstruktur melalui Cabinet, Rack, Bags dan Unit. Serta implementasinya melalui keterkaitan antara barang bukti, lokasi olah tkp, nama kasus serta jenis kejahatannya.
- Access Control → dukungan keamanan sistim penyimpanan bukti digital melalui kontrol terhadap akses pada *resource* yang dikelolanya.

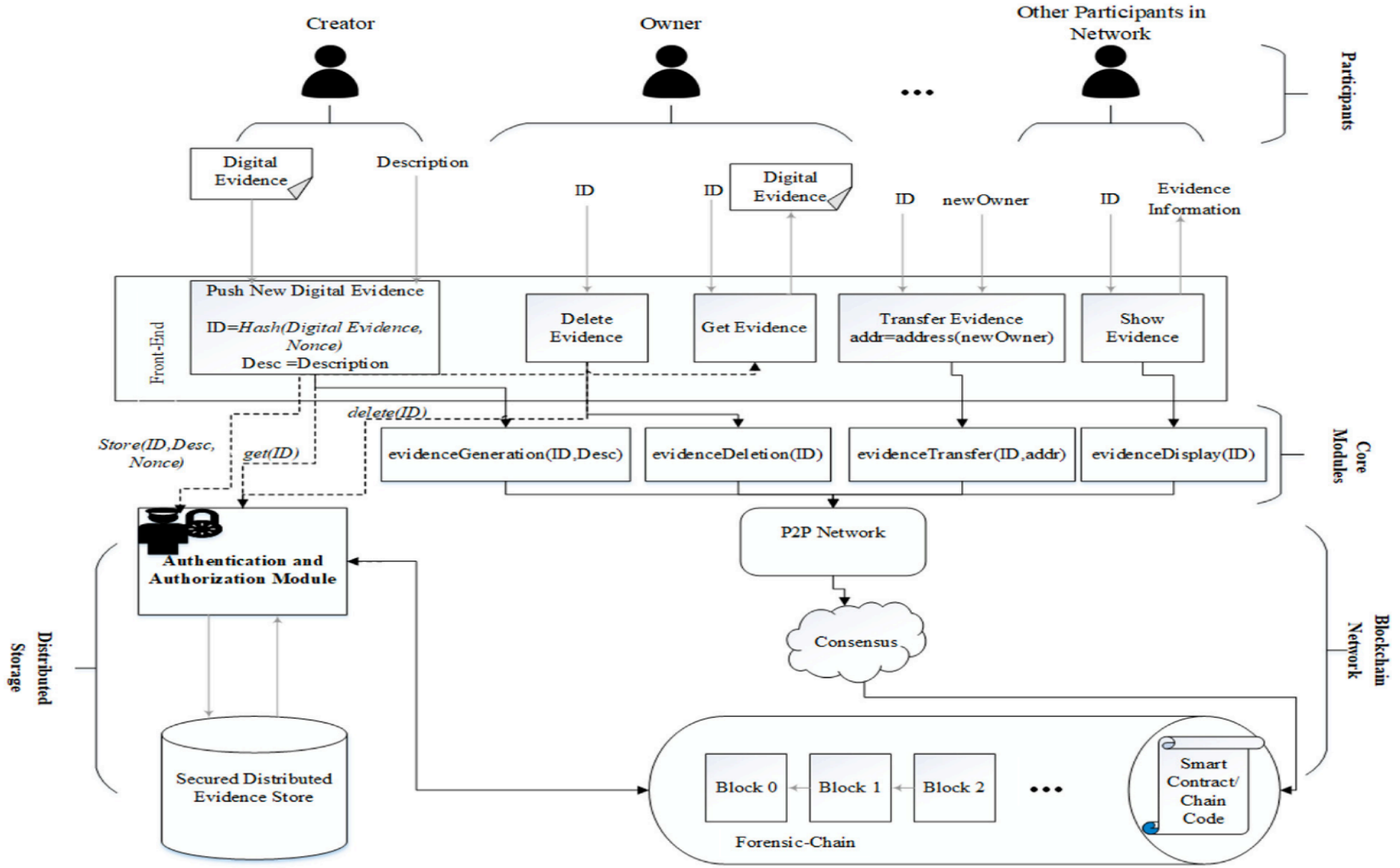
Literatur

Bonomi, S., Casini, M., Ciccotelli, C., 2018. B-CoC : A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics



Literatur

Lone, A.H., Mir, R.N., 2019. Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digit. Investig. 28, 44–55. https://doi.org/10.1016/j.diin.2019.01.002



Catatan

- UU ITE no 11/2008 dan revisinya melalui UU no 19/2016, hanya mengenal istilah sistem elektronik, informasi elektronik dan dokumen elektronik (Pasal 5). Tidak dikenal istilah bukti elektronik dan bukti digital seperti yang digunakan dalam terminologi pada paparan ini.
- Makna yang relevan dengan UU ITE tersebut adalah: bukti elektronik adalah bagian dari sistem elektronik, sementara bukti digital adalah bagian dari informasi elektronik dan dokumen elektronik. Padahal faktanya ada dua hal yang berbeda antara bukti elektronik yang sifatnya adalah fisik dengan bukti digital yang sifatnya file biner.

Catatan

- Selama ini *chain of custody* diimplementasikan pada sistem elektronik. Sehingga hampir semua implementasi dari *chain of custody* diorientasikan kepada bukti fisik.
- Dalam hal ini ada mindset dari aspek hukum yang belum sinkron dengan mindset dari aspek teknologi.
- Perlunya pemahaman yang sama dari praktisi hukum dalam mensikapi permasalahan bukti elektronik dan bukti digital dan *chain of custody*.
- Diperlukan forum terbuka untuk sharing dan komunikasi agar terdapat sinergi pemahaman antara peneliti, praktisi forensika digital dengan peneliti dan praktisi hukum.

Kesimpulan

- Perlu dukungan teknologi yang dapat diterapkan agar bukti digital dapat ditangani sebagaimana halnya barang bukti fisik.
- Namun demikian, untuk implementasi sesungguhnya perlu diikuti dengan kajian dari aspek hukum yang lebih komprehensif.
- Ahli hukum harus mulai membuka wacana untuk mempertimbangkan berbagai solusi yang ada mengenai penanganan bukti digital sehingga solusi teknologi yang ditawarkan dapat benar-benar diadopsi dalam praktik penanganan bukti digital.

Thank You

GREVZN XNFVU

http://www.decode.org/?q=GREVZN+XNFVU+

http://forensics.uii.ac.id