

DAFTAR ISI

HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN.....	iii
HALAMAN PERSEMBAHAN	iv
HALAMAN MOTO	v
KATA PENGANTAR	vi
INTISARI	ix
ABSTRACTION	xi
DAFTAR ISTILAH.....	xiii
DAFTAR ISI	xv
DAFTAR TABEL	xx
DAFTAR GAMBAR.....	xxii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Permasalahan.....	7
1.3 Rumusan Masalah	11
1.4 Tujuan dan Manfaat	12
1.5 Batasan Masalah.....	13
1.6 Kontribusi dan Novelty Penelitian	15
1.7 Struktur Disertasi.....	16
BAB II TINJAUAN PUSTAKA	18
2.1 Permasalahan Umum Chain of Custody	18
2.2 Penelitian Sejenis	22
2.3 Paten Seputar Chain of Custody.....	25
2.4 Lingkup Penelitian	26
2.4.1 Penanganan Awal Bukti Digital.....	27
2.4.2 Workflow Process Chain of Custody	28
2.4.3 Metadata Chain of Custody.....	34

2.4.4	Sentralisasi Penyimpanan Bukti Digital.....	40
2.4.5	<i>Access Control</i> Terhadap Bukti Digital	44
2.5	State of The Art	46
BAB III LANDASAN TEORI		54
3.1	Pengantar	54
3.2	Penanganan Awal Bukti Digital.....	55
3.2.1	Bukti Digital	55
3.2.2	Akuisisi Bukti Elektronik.....	62
3.3	Workflow Process Chain of Custody	64
3.4	Standar Informasi Chain of Custody	68
3.4.1	Makna Chain of Custody.....	68
3.4.2	Metadata File.....	72
3.5	Sentralisasi Penyimpanan Bukti Digital.....	78
3.5.1	Manajemen Storage.....	78
3.5.2	Penyimpanan Imaginer.....	80
3.5.3	Enkripsi dan Dekripsi Text	82
3.6	Trusted Computing.....	85
3.7	Keamanan Komputer.....	86
3.8	Access Control Policy	88
3.9	Evaluasi	99
3.9.1	Model Validasi Forensika Digital	99
3.9.2	Metrik Pengukuran Keamanan Sistim.....	101
3.9.3	Daubert Criteria Scoring	103
BAB IV RANCANGAN PENELITIAN		105
4.1	Terminologi dan Asumsi Dasar yang Digunakan	105
4.1.1	Framework	105
4.1.2	Bukti Digital	106
4.1.3	Chain of Custody.....	107
4.1.4	Pihak yang terlibat.....	108
4.2	General dan Conceptual Model.....	109

4.3	Kebutuhan Framework	112
4.4	Desain Penelitian	113
4.4.1	Perancangan Workflow Process Chain of Custody	114
4.4.2	Perancangan Standar Metadata Chain of Custody	115
4.4.3	Perancangan Konsep Sentralisasi Penyimpanan	117
4.4.4	Perancangan Konsep Access Control Policy	118
4.4.5	Perancangan Integrasi, Simulasi dan Validasi	119
4.5	Alat dan Tempat Penelitian	120
4.6	Data dan Model Evaluasi	120
BAB V KOMPONEN KONSEPTUAL		125
5.1	Regular dan Pos Acquisition Handling	125
5.1.1	Regular Handling	125
5.1.2	Post Acquisition Handling	127
5.1.3	Analisa Post Acquisition Handling	128
5.2	<i>Workflow Process</i> Untuk Chain of Custody Bukti Digital	130
5.2.1	WPCoC-3IR	130
5.2.2	Multiview Workflow Process	133
5.2.3	Simulasi dan Validasi Workflow Process	136
5.2.4	Analisa Regulasi Untuk WPCoC-3IR	137
5.2.5	Penerapan WPCoC-3IR Pada Laboratorium Forensik	139
5.3	Standar Informasi Chain of Custody	142
5.3.1	Proses Mendapatkan Acuan Informasi	143
5.3.2	Informasi Chain of Custody Bukti Digital	144
5.3.3	Pseudo Metadata	150
5.3.4	Korelasi Pseudo Metadata Dengan ISO 27037:2014	151
5.3.5	Evaluasi Pseudo-Metadata	153
5.4	Rangkuman Komponen Konseptual	157
BAB VI KOMPONEN TEKNIS		160
6.1	Lemari Imajiner Penyimpanan Bukti Digital	160
6.1.1	Sentralisasi Penyimpanan	160

6.1.2	Komponen Pendukung	161
6.1.3	Konsep Lemari Imaginer Penyimpanan Bukti Digital	162
6.1.4	Struktur XML Lemari Imaginer Penyimpanan Bukti Digital	166
6.1.5	Use Case Diagram	168
6.1.6	Issue Timeline Pada Lemari Imaginer Penyimpanan.....	170
6.1.7	Issue Keamanan Dokumen Plaintext XML.....	172
6.1.8	Implementasi Lemari Imaginer Penyimpanan Bukti Digital	173
6.1.9	Evaluasi Lemari Imaginer Penyimpanan Bukti Digital	175
6.2	Access Control Policy	176
6.2.1	Proses Pengembangan Access Control Policy	177
6.2.2	Policy Statement.....	177
6.2.3	Attribute Based Access Control (ABAC)	179
6.2.4	Policy Implementation	182
6.2.5	Policy Validation.....	185
6.2.6	Komparasi dengan Literatur.....	188
6.3	Rangkuman Komponen Teknis	189
BAB VII EVALUASI DIGITAL EVIDENCE CABINET		192
7.1	Rangkuman Framework	192
7.2	Implementasi Digital Evidence Cabinet.....	194
7.2.1	Jenis Bukti Digital	194
7.2.2	Prototype Digital Evidence Cabinet.....	194
7.2.3	Skenario Studi Kasus	196
	Output Digital Evidence Cabinet	198
7.2.4	Chain of Custody Pada Digital Evidence Cabinet	200
7.2.5	Issue Keamanan Digital Evidence Cabinet	204
7.3	Keterbatasan Implementasi Digital Evidence Cabinet.....	210
7.3.1	Ukuran File Bukti Digital.....	211
7.3.2	Infrastruktur Client Server dan Storage	211
7.3.3	Time Stamp Authority.....	212
7.4	Evaluasi Framework Digital Evidence Cabinet	214

7.4.1	Kebutuhan Dasar Framework.....	214
7.4.2	Evaluasi Penerapan Framework	217
7.4.3	Secure and Trusted Environment	220
7.4.4	Daubert Criteria Scoring Sebagai Feedback	224
7.5	Evaluasi Regulasi Digital Evidence Cabinet.....	227
7.5.1	Konsistensi Penerapan Regulasi.....	228
7.5.2	Kendala Regulasi Penerapan Digital Evidence Cabinet	231
BAB VIII KESIMPULAN DAN SARAN		234
8.1	Kesimpulan.....	234
8.2	Saran.....	235
DAFTAR PUSTAKA		236
LAMPIRAN		253
Lampiran 1: Tempat Observasi Awal Penelitian.....		254
Lampiran 2: Artefak Publikasi Hasil Penelitian		255
Lampiran 3: Concept Mapping Penelitian Disertasi.....		256
Lampiran 4: WPCoC-3IR		257
Lampiran 5: Validasi 3IR Multiview Business Model		258
Lampiran 6: Tabel Output Pengujian Access Control		262
Lampiran 7: Data Simulasi Sistem DEC		270
Lampiran 8: Contoh Implementasi Struktur XML LIPBID		271
Lampiran 9: Acuan Skoring DREAD.....		273
Lampiran 10: Data Subject Matter Expert.....		276
Lampiran 11: Contoh Isian Daubert Criteria		278