Daftar Isi

Abstrak iv

Abstract v

Pernyataan keaslian tulisan vi

Publikasi selama masa studi vii

Kontribusi yang diberikan oleh pihak lain dalam tesis ini viii

Halaman Persembahan ix

Kata Pengantar x

Daftar Isi ii

Daftar Tabel v

Daftar Gambar iii

Bab I Pendahuluan xx

1.1 Latar Belakang 1

1.2 Rumusan Masalah 4

1.3 Batasan Masalah 4

1.4 Tujuan Penelitian 4

1.5 Manfaat Penelitian 4

1.6 Review Penelitian 4

1.7 Metodologi Penelitian 9

1.8 Sistematika Penulisan 9

Bab II Landasan Teori 11

2.1 *Framework* 11

2.2 Email 11

2.2.1 Struktur Email 11

2.2.2 Bentuk Komunikasi Email 13

2.2.3 Analisis Email 14

2.3 Investigasi Email *Forensics* 15

2.3.1 Investigasi Forensik 15

2.3.2 Email *Forensics* 16

2.3.3 Teknik Investigasi Email *Forensics* 16

2.4 Barang Bukti 17
2.5 *Systems Development Life Cycle* (SDLC) 18
Bab III Metodologi Penelitian 20
3.1 *Identifying Research Problem* 21
3.2 Studi Literatur 21
3.3 SDLC untuk *Framework* 22
3.3.1 *Planning* 23
3.3.2 *Analysis* 24
3.3.3 *Design* 26
3.3.4 *Implementation* 28
3.3.5 *Maintenance* 28
3.4 *Testing Framework* 29
3.4.1 Evaluasi *Framework* 29
3.4.2 Ujicoba *Framework* 30
3.4.3 Analisis *Framework* 31
3.4.4 Laporan 31
Bab IV Hasil dan Pembahasan 32
4.1 SDLC untuk Pengembangan *Framework* 32
4.1.1 *Planning* 32
4.1.2 *Analysis* 34
4.1.3 *Design* 37
4.1.4 *Implementation* 47
4.1.5 *Maintenance* 54
4.2 *Testing Framework* 54
4.2.1 Evaluasi *Framework* 54
4.2.2 Ujicoba *Framework* 56
4.2.3 Analisis *Framework* 111
Bab V Penutup 117
5.1 Kesimpulan 117
5.2 Saran 117
Daftar Pustaka 118

Daftar Tabel

Tabel 1. 1 Jumlah pengguna dan akun email tahun 2015 serta perkiraan sampai dengan tahun 2019 1
Tabel 1. 2 Rangkuman Literatur Review 7
Tabel 3. 1 Tahapan SDLC pada proses pengembangan *framework* 22
Tabel 3. 2 Ekstrasi tahapan *framework* dan tahap investigasi email *forensics* 24
Tabel 3. 3 Input output pada proses *planning* 24
Tabel 3. 4 Identifikasi tahapan *framework* dan teknik investigasi email *forensics* 25
Tabel 3. 5 Input output pada proses *analysis* 26
Tabel 3. 6 Eliminasi tahapan *framework* dan teknik investigasi email *forensics* 27
Tabel 3. 7 Perbandingan *framework* dan teknik sebelumnya dengan *framework yang* telah dikembangkan terkait investigasi email *forensics* 27
Tabel 3. 8 Input output pada proses *design* 28
Tabel 3. 9 Input output pada proses *implementation* 28
Tabel 3. 10 Input output pada proses *maintenance* 29
Tabel 3. 11 Perbandingan *framework* yang telah dikembangkan dengan *framework* dan teknik investigasi email *forensics* sebelumnya. 31
Tabel 3. 12 Kelebihan dan kekurangan *framework* 31
Tabel 4. 1 Ekstraksi tahapan *framework* dan teknik investigasi email *forensics* 34
Tabel 4. 2 Input-output pada proses *planning* 34
Tabel 4. 3 Identifikasi *framework* dan tahapan investigasi email *forensics* 36
Tabel 4. 4 Input output pada proses *analysis* 37
Tabel 4. 5 Pendefinisian tahapan *framework* dan tahapan analisis email 38
Tabel 4. 6 Identifikasi urutan tertinggi dengan terminologi yang sama 39
Tabel 4. 7 Pemberian tahapan baru 40
Tabel 4. 8 Urutan tahapan yang memiliki tahapan baru 41
Tabel 4. 9 Urutan tahapan yang memiliki tahapan baru 43
Tabel 4. 10 Perbandingan *framework* dan tahapan investigasi sebelumnya dengan *framework yang* telah dikembangkan 45
Tabel 4. 11 Input output pada proses *design* 46
Tabel 4. 12 Detail *framework* yang telah dikembangkan 51
Tabel 4. 13 Input output pada proses *Implementation* 53
Tabel 4. 14 Input output pada proses *Maintenance* 54

Tabel 4. 15 Perbandingan *framework* dan tahapan forensik email 54
Tabel 4. 16 Data konten dari masing – masing email 78
Tabel 4. 17 Identitas masing – masing email 78
Tabel 4. 18 Informasi alamat email pengirim 80
Tabel 4. 19 Pemeriksaan alamat email 83
Tabel 4. 20 ringkasan informasi waktu dari pesan email 88
Tabel 4. 21 ID pesan pada masing – masing pesan email 90
Tabel 4. 22 alamat *client IP email* pengirim 97
Tabel 4. 23 protokol yang digunakan pengirim 100
Tabel 4. 24 keterangan file signature 102
Tabel 4. 25 Hasil *trace email* dari masing – masing *header* 107
Tabel 4. 26 *Examination* penelitian studi kasus 110
Tabel 4. 27 Perbedaan *framework* sebelumnya dengan yang dikembangkan 113
Tabel 4. 28 Kelebihan dan kekurangan *framework* 115

Daftar Gambar

Gambar 1. 1 Metode Penelitian 9
Gambar 2. 1 Contoh *header* 12
Gambar 2. 2 Contoh *body* dan *formatting options* pada pesan email 13
Gambar 2. 3 *Framework* investigasi email *forensics* 17
Gambar 2. 4 Tahapan SDLC 18
Gambar 3. 1 Metode Penelitian 20
Gambar 3. 2 Proses ekstraksi tahapan investigasi 24
Gambar 3. 3 Proses identifikasi tahapan investigasi 25
Gambar 3. 4 Proses eliminasi tahapan investigasi 26
Gambar 3. 5 Tahapan *testing* penelitian 29
Gambar 3. 6 Ilustrasi investigasi email *forensics* 30
Gambar 4. 1 *Framework* investigasi email *forensics* 33
Gambar 4. 2 Tahapan utama *framework* yang dikembangkan 48
Gambar 4. 3 Detail *framework* yang telah dikembangkan 49
Gambar 4. 4 Tahapan baru Framework yang dikembangkan 50
Gambar 4. 5 Ilustrasi pemeliharaan *framework* 54
Gambar 4. 6 Ilustrasi simulasi kasus 56
Gambar 4. 7 ilustrasi pengiriman pesan menggunakan gmail 57
Gambar 4. 8 Ilustrasi pengiriman pesan menggunakan Ymail 57
Gambar 4. 9 Ilustrasi kasus 1 pengiriman pesan email spoofing 58
Gambar 4. 10 Ilustrasi kasus 2 pengiriman pesan email spoofing 59
Gambar 4. 11 Ilustrasi kasus 3 pengiriman kasus email spoofing 60
Gambar 4. 12 *Framework* sebelumnya 61
Gambar 4. 13 *Framework* yang telah dikembangkan 62
Gambar 4. 14 Ilustrasi *notification* 63
Gambar 4. 15 Contoh barang bukti 64
Gambar 4. 16 Persiapan instalasi *Mozilla Thunderbird* 64
Gambar 4. 17 Proses pengaturan akun email pada Mozilla Thunderbird 65
Gambar 4. 18 Folder Mozilla Thunderbird 66
Gambar 4. 19 Persiapan awal instalasi AD FTK Imager v 3.2.0.0 66
Gambar 4. 20 Ilustrasi *Imaging* 67
Gambar 4. 21 proses seleksi sumber bukti 68

Gambar 4. 22 informasi bukti dan menentukan folder penyimpanan akuisisi 68
Gambar 4. 23 memulai proses akusisi 69
Gambar 4. 24 proses verifikasi hasil akuisisi 70
Gambar 4. 25 Ilustrasi akusisi barang bukti 70
Gambar 4. 26 proses menambah bukti yang akan diekstrak 71
Gambar 4. 27 Proses memilih file bukti yang akan diekstrak 72
Gambar 4. 28 proses ekstrasi bukti 72
Gambar 4. 29 proses ekstraksi sedang berlangsung 72
Gambar 4. 30 ilustrasi ekstraksi bukti *imaging* 73
Gambar 4. 31 proses *recovery* data email 73
Gambar 4. 32 file direktori email dari hasil ekstraksi sebelumnya 74
Gambar 4. 33 Ilustrasi *email extraction* 74
Gambar 4. 34 Ilustrasi memeriksa identitas pelaku 75
Gambar 4. 35 ilustrasi pemeriksaan *header email* 75
Gambar 4. 36 konten ke 1 email sah (*legitimate*) 75
Gambar 4. 37 konten ke 2 email sah (*legitimate*) 75
Gambar 4. 38 konten ke *1 email spoofing* 76
Gambar 4. 39 konten ke 2 *email spoofing* 76
Gambar 4. 40 konten ke 3 *email spoofing* 76
Gambar 4. 41 *Return-Path* ke 1 email sah (*legitimate*) 76
Gambar 4. 42 *Return-Path* ke 2 email sah (*legitimate*) 77
Gambar 4. 43 *Return-Path* ke 1 *email spoofing* 77
Gambar 4. 44 *Return-Path* ke 2 *email spoofing* 77
Gambar 4. 45 *Return-Path* ke 3 *email spoofing* 77
Gambar 4. 46 Ilustrasi memeriksa alamat email sah ke 1 78
Gambar 4. 47 Ilustrasi memeriksa alamat email sah ke 2 79
Gambar 4. 48 ilustrasi memeriksa alamat email *spoofing* ke 1 79
Gambar 4. 49 ilustrasi memeriksa alamat email *spoofing* ke 2 79
Gambar 4. 50 ilustrasi memeriksa alamat email *spoofing* ke 3 79
Gambar 4. 51 pengecekan validasi email sah 81
Gambar 4. 52 pengecekan validasi email *spoofing* 81
Gambar 4. 53 pengecekan validasi email *spoofing* 82
Gambar 4. 54 Pengecekan *IP address* 82
Gambar 4. 55 Pengecekan *IP address* 83
Gambar 4. 56 Ilustrasi memeriksa waktu pesan dibuat 84

Gambar 4. 57 kota di dunia dengan *time zone -0800* 85
Gambar 4. 58 kota di dunia dengan *time zone +0700* 85
Gambar 4. 59 ilustrasi memeriksa waktu pesan 85
Gambar 4. 60 ilustrasi time menggunakan UTC +0000 86
Gambar 4. 61 ilustrasi memeriksa waktu pesan 86
Gambar 4. 62 ibu kota negara dengan koordinat +0300 86
Gambar 4. 63 ilustrasi memeriksa waktu pesan 87
Gambar 4. 64 ibu kota negara dengan koordinat +0100 87
Gambar 4. 65 Ilustrasi memeriksa wakti pesan 87
Gambar 4. 66 Ilustrasi pengecekan wilayah dengan time zone +0300 88
Gambar 4. 67 Ilustrasi memeriksa ID pesan 89
Gambar 4. 68 ilustrasi pemeriksaan ID pesan 89
Gambar 4. 69 ilustrasi pemeriksaan ID pesan 89
Gambar 4. 70 ilustrasi pemeriksaan ID pesan 90
Gambar 4. 71 ilustrasi pemeriksaan ID pesan 90
Gambar 4. 72 Ilustrasi memeriksa alamat IP pengirim 91
Gambar 4. 73 pemeriksaan *IP client* 92
Gambar 4. 74 pemeriksaan *IP client* pada Studi Kasus 2 92
Gambar 4. 75 pemeriksaan keaslian *IP client* 93
Gambar 4. 76 pemeriksaan *IP client* 93
Gambar 4. 77 pemeriksaan keaslian *IP client* 93
Gambar 4. 78 memeriksa *RIPE database* 94
Gambar 4. 79 memeriksa *client IP* 94
Gambar 4. 80 Pemeriksaan informasi *IP client* 95
Gambar 4. 81 memeriksa *RIPE database* 95
Gambar 4. 82 memeriksa *IP client* 96
Gambar 4. 83 memeriksa keaslian *client IP* 96
Gambar 4. 84 memeriksa *RIPE database* 97
Gambar 4. 85 Ilustrasi memeriksa protokol yang digunakan 98
Gambar 4. 86 ilustrasi memeriksa protokol yang digunakan 98
Gambar 4 87 ilustrasi memeriksa protokol yang digunakan 99
Gambar 4. 88 ilustrasi memeriksa protokol yang digunakan 99
Gambar 4. 89 Ilustrasi memeriksa protokol yang digunakan 99
Gambar 4. 90 Ilustrasi memeriksa informasi kontak lain dari email pelaku 101
Gambar 4. 91 Ilustrasi *file signature* pada pesan email masuk 101

Gambar 4. 92 pengaturan *file signature* 102
Gambar 4. 93 memulai kasus baru 103
Gambar 4. 94 memilih tipe/jenis *client email* 103
Gambar 4. 95 *tracer email* sah dari studi kasus 1 104
Gambar 4. 96 *tracer email* sah studi kasus 2 104
Gambar 4. 97 *tracer email spoofing* studi kasus 1 105
Gambar 4. 98 *trace email spoofing* studi kasus 2 105
Gambar 4. 99 *tracer email spoofing* studi kasus 3 106
Gambar 4. 100 Ilustrasi *Trace email original* 108
Gambar 4. 101 Ilustrasi *report & visualisation* 111
Gambar 4. 102 Perbedaan *framework* 112

Takarir dan Singkatan

SDLC	:	*Systems Development Life Cycle*
Email	:	*Electronic Mail*
dkk	:	dan kawan–kawan
IEFAF	:	*Integrated E-Mail Forensic Analysis Framework*
URL	:	*Uniform Resource Locator*
IDFIF	:	*Integrated Digital Forensics Investigation Framework*
IIF	:	*Investigasi and Intelijen Framework*
HTTP	:	*Hypertext Transfer Protocol*
POP3	:	*Post Office Protocol versi 3*
IMAP	:	*Internet Message Access Protocol*
SMTP	:	*Simple Mail Transport Protocol*
Cc	:	*Carbon copy*
Bcc	:	*Blind carbon copy*
IP	:	*Internet Protocol*
Gmail	:	*Google Mail*
Ymail	:	*Yahoo Mail*
SSL	:	*Secure Socket Layer*
AD FTK	:	*Access Data Forensic ToolKit*
MD5	:	*Message Digest algortihm 5*
SHA1	:	*Secure Hash Algorithm 1*
IPV4	:	*Internet Protocol version 4*
IPV6	:	*Internet Protocol version 6*
RIPE	:	*Réseaux IP Européens*
TLS	:	*Transport Layer Security*
ISP	:	*Internet Service Provider*