PENGEMBANGAN FRAMEWORK PELAPORAN CYBER CRIME

DARYONO
13917211

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Magister Teknik Informatika

Program PascasarjanaFakultas Teknologi Industri

Universitas Islam Indonesia

2017

Lembar Pengesahan Pembimbing

PENGEMBANGAN FRAMEWORK PELAPORAN CYBER CRIME

Nama : DARYONO
NIM : 13917211

Yogyakarta, 26 Maret 2017

Pembimbing I,

Dr. Bambang Sugiantoro, M.T

Lembar Pengesahan Penguji

PENGEMBANGAN FRAMEWORK PELAPORAN CYBER CRIME

Nama :DARYONO

NIM :13917211

Yogyakarta, 26 Maret 2017

Tim Penguji,

Dr. Bambang Sugiantoro, M.T
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, S.T.,M. Sc

Kata Pengantar

Assalamualaikum Wr. Wb.

Alhamdulillah hirobbi 'alamin penulis ucapkan kepada ALLAH SWT yang selalu memberikan kesehatan dan keselamatan pada diri penulis untukmenyelesaikan tesis ini dengan judul **" PENGEMBANGAN FRAMEWORK PELAPORAN CYBERCRIME "** sebagai persyaratan untuk mencapai gelar Magister Komputer pada program Pasca Sarjana Universitas Islam Indonesia.

Pada kesempatan ini dengan penuh kerendahan hati penulis haturkan ucapan terima kasih yang tak terhingga dan penghargaan yang setinggi-tingginya kepada kedua orang tua saya serta Istri dan Kedua anak saya beserta kedua mertua saya yang selalu memotivasi tiada henti memberi doa dan kasih sayangnya kepada penulis.

Di samping itu, secara khusus penulis haturkan terima kasih kepada:

1. Rektor UII Yogyakarta, Bapak Dr. Ir. Harsoyo, M.Sc dan para Pembantu Rektor.
2. Bapak Dekan Fakultas Teknologi Industri, Dr.R. Teduh Dirgahayu,ST.,M.Sc dan Ibu Wakil Dekan Dr. Sri Kusumadewi, S.Si., MT, atas motivasi, koreksi dan kemudahan pelayanan selama studi.
3. Bapak Dr. R. Teduh Dirgahayu, ST., M.Sc. sebagai Ketua Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia.
4. Dosen pembimbing Bapak Dr. Bambang Sugiantoro, M.T. Selaku dosen pembimbing, Terima kasih atas segala bantuan dukungan, semangat dan pengetahuannya serta kemudahan yang diberikan.
5. Dosen penguji , Bapak Ahmad Lutfi, S.Kom.,M. Kom.,Bapak YudiPrayudi,S.Si,M.Kom.dan Bapak Dr.Imam Riadi yang telah memberikan motivasi dan semangat serta bimbingan yang sangat berarti bagi penulis dalam menyelesaikan tesis ini.
6. Bapak AKBP Bakti Andriono, M.Kom., yang telah memberikan tempat untuk penelitian Di Polda Yogyakarta.
7. Seluruh Dosen dan civitas Magister Teknik Informatika, baik secara langsung maupun tidak langsung telah membantu penulis selama masamasa studi penulis.
8. Staf Administrasi dan tata usaha Magister Teknik Informatika,Universitas Islam Indonesia, yang telah membantu dalam segala urusan administrasi di kampus.

9. Rekan-rekan mahasiswa MTI angkatan 09 yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lain.
10. Semua pihak yang telah membantu penulis selama penyusunan skripsi ini yang tidak dapat penulis sebutkan satu persatu.

Semoga Allah SWT senantiasa memberikan berkat dan anugrah-Nya berlimpah bagi beliau-beliau yang tersebut di atas. Sangat disadari dalam tesis ini terdapat banyak kekurangan oleh karena itu semua saran dan kritik penulis terima dengan lapang dada demi kesempurnaan penulisan tesis ini. Akhirnya harapan penulis semoga tesis ini bermanfaat bagi kita semua.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, Maret 2017

Daryono

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. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, Maret 2017

Daryono,S.Pd,S.Kom

Abstrak

Pada era globalisasi seperti sekarang ini. perkembangan teknologi sangatlah pesat, Teknologi Informasi dan Komunikasi (TIK) telah menjadi bagian hidup manusia yang tidak dapat dipisahkan. Keberadaan TIK juga bisa digunakan membuat kita menjadi lebih mudah dan menyenangkan. Akan tetapi TIK juga bisa digunakan untuk tindak kejahatan, Kejahatan dalam TIK atau Cybercrime adalah suatu tindak criminal yang dilakukan dengan menggunakan Teknologi Komputer sebagai alat kejahatan utama. Dengan banyaknya orang yang mengalami kejahatan Cyber mengalami kesulitan untuk melaporkan kepada pihak yang berwajib karena ketidaktahuan yang menangani kasus kejahatan dunia maya dan keengganan mereka untuk melaporakank karena prosedur pelaporan dikepolisian yang begitu rumit dan model pelaporan masih bersifat Konvensional.Maka disini penulis mengembangkan framework untuk pelaporan Cybercrime kepihak yang berkompeten agar masyarakat mudah dan cepat dalam melaporkan kasus cybercrime kepada pihak kepolisian dengan mudah dan cepat.penelitian ini dilakukan di Mapolda Kota Yogyakarta, metode ini mengacu pada penelitian sebelumnya yang dilakukan oleh Yong-dal shin yaitu New model for cybercrime investigation procedur dan untuk metode yang digunakan dalam penelitian ini adalah Metode Zahman Framework yaitu merupakan metode EAP yang banyak digunakan dengan langkah-langkah yang sistemis, mudah dipahami dan dapat dijadikan control.hasil pengembangan yang dibuat oleh penulis yaitu mengembangkan SOP pelaporan di kepolisian mapolda Yogyakarta menjadi pengembangan framework pelaporan cybercrime berbasis web.

Kata kunci :

framework, cybercrime, html

Abstract

In this globalization era. very rapid technological development, Information and Communication Technology (ICT) has become part of human life that can not be separated. The existence of ICTs can also be used to make us easier and more enjoyable. However ICT can also be used for crime, crime in the ICT or the Cybercrime is a criminal acts committed using computer technology as a major crime. With so many people experiencing Cyber crimes have difficulties to report to the authorities because of ignorance that handles cases of cyber crimes and their reluctance to melaporakank because dikepolisian reporting procedures are so complicated and reporting model still Konvensional.Maka here the authors develop a framework for reporting cybercrime kepihak competent so that people easily and quickly in cybercrime cases reported to the police easily and cepat.penelitian was conducted in Yogyakarta City police Headquarters, this method refers to an earlier study conducted by Shin Yong-dal: New models for cybercrime investigation procedure of and for the method used in this research is the method Zahman Framework is an EAP method that is widely used by systemic steps, easy to understand and can be used as control.hasil development created by the author is developing a reporting SOP in Yogyakarta police Headquarters into the development of cybercrime reporting framework Web-based.

Keywords :

framework, cybercrime, html

Publikasi selama masa studi

Tidak ada publikasi yang menjadi bagian dari tesis

Kontribusi yang diberikan oleh pihak lain dalam tesis ini

Tidak ada kontribusi dari pihak lain

Halaman Persembahan

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Karya ini saya persembahkan kepada :

Kedua orang tua saya yang senantiasa menjadi orang tua terhebat dan tak pernah mengeluh dalam bekerja demi membiayai pendidikan anaknya.
Kedua mertua saya yang telah memberikan doa dan semangat kepada saya sehingga sampai pendidikan Pascasarjana saya selesai.
Istri dan Kedua anaknya saya yang tercinta yang juga memberikan doa dan memotivasi kepada saya dalam menempuh pendidikan pascasarjana saya selesai.

Pada akhirnya saya persembahkan karya saya ini kepada semua pembaca, untuk ditelusuri dan menjadi inspirasi yang akhirnya bisa ditarik hikmahnya.

Daftar Isi

Takarir dan Singkatan

SPK : Sentra Pelayanan Kepolisian.

Cybercrime : Kejahatan dengan menggunakan perangkat Teknologi Informasi dan Komunikasi.

Framework : Kerangka kerja adalah sebuah software untuk memudahkan para programmer membuat aplikasi atau web yang isinya adalah berbagai fungsi, plugin, dan konsep sehingga membentuk suatu sistem tertentu.

BANUM : Admin Bagian Umum

KASUBDIT : Admin Kepala Sub Direktorat

DFD : Data flow diagram

ERD : Entitas Rlationship Diagram

Bab I Pendahuluan

1.1. Latar Belakang

Pada era globalisasi seperti sekarang ini, perkembangan teknologi sangatlah pesat, Teknologi Informasi dan komunikasi (TIK) telah menjadi bagian hidup manusia yang tidak dapat dipisahkan. keberadaan TIK membuat hidup kita menjadi lebih mudah dan menyenangkan. Tetapi TIK juga bisa digunakan untuk tindak kejahatan. *cybercrime* adalah suatu tindak criminal yang dilakukan dengan menggunakan Teknologi komputer sebagai alat kejahatan utama. Cybercrime didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan teknologi internet. (Mustari, 2015).

Sejalan dengan perkembangan teknologi gadget sekarang ini, kejahatan dalam dunia TIK juga sejalan berkembang sangat cepat. berdasarkan laporan state of the internet 2013 dalam berita surat kabar online yang berjudul *Indonesia berada di urutan kedua dalam daftar lima besar negara asal serangan kejahatan siber atau cybercrime.* wakil direktur tindak pidana ekonomi khusus bareskrim polri kombespol Agung setya mengatakan, dalam kurun waktu tiga tahun terakhir, tercatat 36,6 juta serangan cybercrime terjadi di Indonesia. hal ini sesuai dengan data security threat 2013 yang menyebutkan Indonesia adalah negara paling berisiko mengalami serangan cybercrime. sejak 2012 sampai dengan april 2015, subdit IT atau cybercrime telah menangkap 497 orang tersangka kasus kejahatan di dunia maya. dari jumlah tersebut, sebanyak 389 orang di antaranya merupakan warga negara asing, dan 108 orang merupakan warga negara Indonesia total kerugian *cybercrime* di Indonesia mencapai Rp 33,29 miliar. angka ini jauh lebih besar dibandingkan perampokan nasabah bank secara konvensional, sementara itu, sepanjang 2012 sampai dengan 2014, terdapat 101 permintaan penyelidikan terhadap kasus *fraud* atau penipuan dari seluruh dunia. ini artinya, setiap 10 hari terdapat satu kejadian selama tiga tahun terakhir. (Kompas.com, 12 Mei 2015).

Dari informasi diatas masih banyak Masyarakat yang menggunakan perangkat gadget Mulai dari Handphone, Smartphone, Tablet, Laptop dan PC yang sudah terkoneksi dengan jaringan internet, masih banyak orang yang mengalami kejahatan Cybercrime karena ketidak tahuan pengetahuan masyarakat Indonesia sendiri untuk melaporkan kepihak yang bertanggung jawab yang menangani kasus kejahatan dunia maya dan keengganan mereka untuk melaporkan karena prosedur dikepolisian yang begitu rumit dan untuk model pelaporan yang masih konvensional. Sesuai dengan Pasal 1 angka 24 dan 25 UU No. 8 Tahun 1981 prosedur pelaporan atau Pengaduan Masyarakat kepada Polri Sbb:

1. Masyarakat/ Pelapor dapat datang ke Kantor Polisi terdekat berdasarkan tempat kejadian perkara yang akan dilaporkan.
2. Masyarakat/ Pelapor akan diterima oleh Petugas SPK.
3. Oleh Petugas SPK masyarakat/ pelapor akan diambil keterangannya untuk dituangkan dalam format berdasarkan apa yang dilaporkan.
4. Setelah diterima laporannya masyarakat akan diberikan Surat Tanda Penerimaan Laporan.
5. Masyarakat tidak dipungut biaya apapun.

Atau juga bisa melaporkan tindak kejahatan cybercrime dengan via telephon dan via email cybercrime@polri.go.id.serta terkendala faktor SDM dikepolisian yang menanggani kasus kejahatan cybercrime masih minim sekali karena disetiap Polda sampai Polsek baru sebagian kecil yang menangani kasus cybercrime karena terkendala faktor SDM yang belum siap.

Sistem informasi pelaporan yang ada dikepolisian sekarang ini adalah sistem pelayanan pengaduan lewat via telephon dan via email serta kasus yang dilaporkan tentang kejahatan cybercrime masih dicampur dengan tindak kriminal secara umum dan penanganannya lama direspon oleh pihak kepolisian dikarenakan harus memilah mana laporan kriminal umum dan kejahatan cybercrime, maka disini penulis mempunyai ide membuat Framework pelaporan melalui sistem informasi berbasis web agar pelaporan yang khusus dengan kejahatan cybercrime bisa berdiri sendiri tidak bercampur dengan tindak kriminal

dengan cepat secara umum agar pelaporan dari masyarakat yang mengalamn mudahi tindak kejahatan cybercrime mudah direspon oleh pihak yang berkompeten.

Berdasarkan uraian latar belakang diatas, bahwa masyarakat perlu difasilitasi sebuah sistem informasi pelaporan tindak kejatahatan tentang cybercrime yang mudah diakses dimana saja dan kapan saja. serta kalau ada bentuk kerjasama dengan pihak yang berkompeten untuk menanggani kasus cybercrime dapat diintegrasikan dengan sistem informasi yang ada dipihak kepolisian.

1.2. Identifikasi Masalah

Berdasarkan latar belakang tersebut dapat dirumuskan bahwa permasalahan yang ada antara lain:

> Di kepolisian untuk pelaporan Cyber crime khususnya di Polda Yogyakarta masih menggunakan cara yang Konvensioanal,bagaimana merancang sebuah Framework yang dapat digunakan untuk pelayanan pelaporan masyarakat dalam kasus kejahatan cybercrime secara mudah dan cepat.

1.3. Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah pada penelitian ini adalah :

a. Bagaimana membuat framework pelaporan cybercrime?
b. Bagaimana menyajikan sebuah sistem yang memberikan informasi secara cepat dan akurat kepada masyarakat yang mengalami kasus kejahatan cybercrime?

1.4. Batasan Masalah

Untuk lebih fokus dan terarahnya penelitian maka peneliti memberikan batasan sebagai berikut :

Membahas pada Framework pelaporan dari masyarakat umum di Indonesia yang mengalami tentang cyber crime kepada pihak kepolisian khususnya di Polda Yogyakarta.

1.5. Tujuan Penelitian

Tujuan yang ingin dicapai dan diharapkan dalam penelitian ini adalah menghasilkan :

Perancangan sebuah Framework sebagai salah satu sarana untuk memberikan layanan penerimaan pelaporan cybercrime pada kepolisian.

1.6. Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah:

a. Membantu pihak kepolisian khususnya yang menangani kejahatan yang berhubungan dengan cybercrime untuk memberikan Informasi data tentang kejahatan cybercrime khususnya di indonesia.

b. Mempermudah masyarakat Indonesia untuk menyampaikan pelaporan tentang kejahatan cybercrime yang cepat melalui Sistem Informasi kepada pihak kepolisian.

1.7. Review Literatur

Untuk menunjang keterkaitan dan keterbaruan ilmu pengetahuan, berikut akan dijelaskan beberapa pendapat dari penelitian sebelumnya yang dianggap mendukung penelitian ini:

New model for cyber crime investigation Procedur,yaitu framework tahapan melakukan penanganan kasus cyber crime(Yong-dal Shin, 2011) :

1. Tahap persiapan
2. Tahap konsultasi orang yang menangani kejahatan
3. Tahap klasifikasi kejahatan cyber dan keputusan investigasi yang diprioritaskan
4. Penanganan investigasi barang bukti kejahatan cyber(melindungi korban dengan police line,mengumpulkan alat bukti cybercrime,dokumentasi berupa foto dan video,mengumpulkan alat bukti dan analisis,mendapatkan media penyimpanan dan jaringan)
5. Analisis Profile (Penyelidikan tersangka,Dalam melakukan investigasi reka ulang (untuk perlindungan dengan police line,Seting koleksi peralatan bukti kejahatan cyber,Foto pengumpulan barang bukti dan analisis, Memperoleh bukti dari media simpan, Mendapatkan barang bukti dari jaringan, Memperoleh bukti berupa printer)
6. Memanggil tersangka
7. Rekontruksi kejahatan cyber yang logis

Digital Forensic model di malaysia investigation proces Setiap kali melakukan penyelidikan komputer untuk potensi pelanggaran pidana hukum proses hukum hanya akan tergantung pada cyber law setempat . Secara umum semua kasus hanya akan mengikuti tiga langkah berikut: Pengaduan(Pelaporan), Investigasi dan Penuntutan (Sundresan, 2009).

Lee et al.mendiskusikan ilmiah tentang penyelidikan investigasi Cyber crime Forensic TKP tidak dengan proses invetigasi yang penuh, dengan mengidentifikasi empat langkah dalam proses (Seamus, 2004) :

1. Recognition, langkah pertama dimana barang atau pola yang terlihat menjadi potensi bukti, penyidik harus tahu baik apa yang dicari dan di mana dapat ditemukan, pengakuan mengarah ke dua sub yaitu dokumentasi dan pengumpulan serta pengamanan.
2. Identification, langkah berikutnya melibatkan klasifikasi bukti dan satu sub yaitu kegiatan, perbandingan (baik fisik, biologi, kimia dan sifat lainnya) yang dibandingkan dengan standar yang diketahui.

3. Individualization, mengacu menentukan apakah barang bukti yang ada unik sehingga dapat dikaitkan dengan individu atau peristiwa yang lain, dalam hal ini barang-barang harus dievalusi dan diinterprestasikan.
4. Reconstruction, melibatkan menyatukan output bagian dari proses, dan informasi terkait dengan yang lain dari peneliti yang telah ia peroleh, untuk memberikan rincian tentang peristiwa dan tindakan di TKP hal ini mempengaruhi dalam penulisan pelaporan dan penyampaian presentasi.

Framework Digital Investigation menurut Selamatet al, mengidentifikasi fase umum dalam model-model sebelumnya dan menghubugkan dengan peta digital investigasi forensik. framework yang dihasilkan menjadi lima tahap model yaitu Preparation (persiapan), Collection (pengumpulan atau pengamanan) relevan dengan akusisi data, mereka mencatat bahwa kajian mereka menunjukkan bahwa semua model mengandung 2, 3 dan 4 (collection and preservation,examination and analisis,presentation and reporting) hanya sedikit yang mengandung tahap 1 dan 5 yang mereka anggap penting. (Selamat,el al,2008).

Dalam penelitian tentang sistem aplikasi pencatatan tindak kejahatan pada polsek tegal selatan berbasis web, program aplikasi yang mampu mengolah data-data kepolisian yang bersangkutan dengan kasus yang terjadi dan ditangani. sistem ini juga bisa memberi informasi kepada masyarakat dan mempermudah pengguna untuk menggunakannya. Sistem informasi kejahatan berbasis web Aplikasi ini diharapkan mampu membantu kinerja kepolisian dalam menangani suatu kasus dan memberikan informasi kepada masyarakat. Penelitian ini menghasilkan program sistem aplikasi pencatatan tindak kejahatan berbasis web dan menghasilkan aplikasi untuk mengetahui Tingkat kejahatan yang terjadi di Sektor Tegal Selatan. (Siswanto, Rochim, & Somantri, 2012).

Sistem pelayanan pengaduan masyarakat pada divisi humas polri adalah sistem pelayanan pengaduan masyarakat pada divisi humas berbasis web dan permohonan informasi semua tindakan kriminalitas masyarakat melalui website divisi humas polri.adapun kinerja sistem dalam pelayanan pengaduan dan permohonan informasi yang sebelumnya sedang berjalan di divisi humas polri masih belum optimal karena pengolahannya masih dilakukan secara manual. oleh

karena itu pelayanan di divisi humas polri menjadi kurang efektif dan efisien, karena media pelayanan data memperlambat jalannya penyampaian respon terhadap pengaduan atau permohonan informasi yang disampaikan oleh masyarakat. dengan adanya sistem pelayanan pengaduan masyarakat berbasis web ini mempermudah masyarakat untuk menyampaikan pengaduan dan permohonan informasi, serta mempercepat pihak divisi humas polri untuk merespon setiap pengaduan dan permohonan informasi tersebut. dalam merancangan sistem pelayanan pengaduan masyarakat berbasis web ini dimodelkan dengan UML (Unified Modeling Languange) meliputi use case diagram, acitivity diagram dan class diagram.(Masya et al, 2012).

Pengaduan masyarakat adalah salah satu upaya untuk membuat masyarakat berperan serta menegakkan hukum dengan memberikan informasi kepada aparat penegak hukum guna menindaklanjuti pengaduan atas pelanggaran yang telah dilaporkan. Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK)sebagai lembaga inteligen di bidang keuangan dirasa perlu membangun Sebuah aplikasi untuk masyarakat baik umum maupun dilingkungan PPATK sendiri agar tidak hanya pelanggaran di luar saja yang dapat teratasi tetapi juga pelanggaran yang terjadi dilingkup. adanya aplikasi berbasis web ini dapat mempermudah masyarakat untuk melakukan pelaporan atas pelanggaran yang dicurigai atau sudah pasti terjadi terutama dilingkungan internal PPATK tanpa harus khawatir indentitasnya diketahui oleh orang lain.(Pengaduan, 2013).

1.8. Metode Penelitian

Adapun langkah-langkah yang akan ditempuh selama melakukan penelitian ini yaitu sebagai berikut:

a. Studi Literatur

Penelitian ini dilakukan dengan melakukan studi kepustakaan yaitu dengan mengumpulkan bahan-bahan referensi yang terkait dengan penelitian, baik melalui buku, artikel, paper, jurnal, makalah, dan mengunjungi beberapa situs yang terdapat pada internet terkait dengan *Sistem Informasi berbasis web dan*

kejahatan cybercrime serta beberapa referensi lain yang dapat menunjang kegiatan penelitian yang dilakukan.

b. Analisis

Tahapan analisis ini dilakukan terhadap model-mode pelaporan secara umum sebagai referensi untuk pembuatan sistem informasi pelaporan cybercrime.

c. Perancangan

Pada tahapan ini peneliti membuat perancangan terkait dengan Sistem Informasi tentang pelaporan cybercrime yang diusulkan.

d. Implementasi

Tahapan implementasi yang dimaksud yaitu mengimplementasikan hasil pembuatan Sistem Informasi untuk pelaporan cybercrime.

e. Testing

Tahapan ini bertujuan untuk mengetahui keberhasilan peneliti dalam pembuatan Sistem Informasi pelaporan Cybercrime.

f. Laporan

Tahapan laporan adalah tahapan akhir dari pelaksanaan penelitian ini, yaitu penyampaian kesimpulan atas hasil setelah Sistem Informasi jadi.

1.9. Sistematika Penulisan

Sistematika penulisan merupakan daftar susunan bab dan subbab dari sebuah penelitian. Laporan penelitian ini disusun dalam sistematika dan berstruktur agar lebih mudah dipahami bagi siapa saja yang membacanya. Sistematika laporan penelitian ini adalah sebagai berikut.

Bab I Pendahuluan

Bab ini memuat latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian yang digunakan dalam penelitian serta sistematika penelitian.

Bab II Landasan Teori

Bab ini memuat teori-teori penunjang yang digunakan sebagai dasar penelitian penyelidikan forensika digital terhadap mesin fotokopi MFP.

Bab III Metodologi Penelitian

Uraian dalam bab ini merupakan penjabaran lebih rinci tentang metode penelitian yang secara garis besar telah disajikan di Bab I (Pendahuluan).

Bab IV Hasil dan Pembahasan

Bagian ini pada dasarnya memuat pengolahan dan analisis data untuk menghasilkan temuan dan pembahasan /analisis dari hasil temuan. Pengolahan data dilakukan berdasarkan prosedur penelitian yang telah diurai di Bab III.

Bab V Kesimpulan dan Saran

Dalam Bab V disajikan penafsiran dan pemaknaan peneliti terhadap hasil analisis temuan penelitian, yang disajikan dalam bentuk kesimpulan penelitian. Serta di kemukakan beberapa saran untuk dilaksanakan guna pengembangan lebih lanjut terkait tugas akhir ini.

Bab II Landasan Teori

2.1. Pengertian Framework

Dalam bidang digital forensic istilah framework dalam bahasa formalnya yang pernah dikemukakan oleh Petar & Maravi merupakan *a structure to support a successful forensic investigation*. secara umum, dilingkungan digita forensic setidaknya ada beberapa istilah terkait dengan langkah-langkah terstruktur dalam proses investigasi diantaranya adalah framework, metodhology, dan forensics process

Secara garis besar, framework tersebut mendeskripsikan tahapan, methodology ataupun model investigasi yang dapat diterapkan dalam mengimplementasikan aktivitas digital forensic. beberapa framework yang ada adalah Generic Computer Forensic Investigation Model (GCFIM) yang diusukan oleh Yussof et.al,The Four Tier Model Ademu et.al,Integrated Digital Forensic Process Model (IDFPM) dari M.D.Kohn serta Integrated Digital Forensics Investigation Framework (IDFIF) dari Rahayu & Prayudi (A.Lutfi & Prayudi, 2015).

2.2. Pengertian Cybercrime

Kejahatan dunia maya (Inggris: cybercrime) adalah istilah yang mengacu kepada tindakan kejahatan dengan gadget atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. di indonesia sendiri kejahatan di bidang IT sudah sering terjadi beberapa di antaranya saat website-website pemerintah yang beberapa kali deface, maupun memanfaatkan celah keamanan joomla (untuk beberapa website pemerintah yang masih menggunakan joomla) dan saat pemilu yang beberapa kali server KPU diserang dari berbagai daerah oleh para hacker, dan baru-baru ini tentang pembobolan ATM dan kartu kredit yang sempat menghebohkan.

Maraknya tindak kejahatan di dunia maya tergantung dari sejauh mana sumber daya baik berupa hardware atau software maupun pengguna teknologi yang bersangkutan mempunyai pengetahuan dan kesadaran tentang pentingnya keamanan di dunia maya, seorang penyedia layanan atau target cybercrime harus mempunyai pengetahuan yang cukup tentang metode yang biasanya seorang cybercrime lakukan dalam menjalankan aksinya.

Pengertian Cybercrime menurut beberapa ahli:

a. Cybercrime sebagai kejahatan dibidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal dalam bukunya yang berjudul *Aspek-aspek pidana di bidang komputer* (menurut: Andi hamzah ,2013).

b. Mendefinisikan Cybercrime sebagai aksi kejahatan yang menggunakan teknologi komputer sebagai komponen utamanya (menurut: Forester dan Morrison).

c. Memberikan definisi cybercrim 9 ng lebih menarik, yaitu : kejahatan dimana tindakan kriminal hanya bisa dilakukan menggunakan teknologi cyber dan terjadi di dunia cyber (M.Yoga.P,2013).

Pengertian Cybercrime menurut beberapa pakar :

- **The U.S. Department of Justice** memberikan pengertian **Computer Crime** sebagai: *"... any illegal act requiring knowledge of Computer technology for its perpetration, investigation, or prosecution".*
- **Organization of European Community Development**, yaitu: *"any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data".*
- **Andi Hamzah dalam bukunya** *"Aspek-aspek Pidana di Bidang Komputer" (1989)* mengartikan **cybercrime** sebagai kejahatan di bidang komputer secara umum dapat diartikan *sebagai penggunaan komputer secara ilegal*.

- **Eoghan Casey** *"Cybercrime is used throughout this text to refer to any crime that involves computer and networks, including crimes that do not rely heavily on computer.*

  Jenis-jenis cybercrime berdasarkan jenis aktivitasnya :

  a. Unauthorized Access to Computer System and Service

     Kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting.

  b. Illegal Contents

     Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain.

  c. Data Forgery

     Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet.

  d. Cyber Espionage

     Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran.

  e. Cyber Sabotage and Extortion

     Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

  f. Offense against Intellectual Property

     Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal,

penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

g. Infringements of Privacy

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

h. Cracking

Kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak system keamaanan suatu system komputer dan biasanya melakukan pencurian, tindakan anarkis begitu merekam mendapatkan akses. Biasanya kita sering salah menafsirkan antara seorang hacker dan cracker dimana hacker sendiri identetik dengan perbuatan negative, padahal hacker adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dapat dipublikasikan dan rahasia.

i. Carding

Adalah kejahatan dengan menggunakan teknologi komputer untuk melakukan transaksi dengan menggunakan card credit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil.

2.3 Pengaduan Pelayanan Publik

Pengaduan atau laporan dapat dilakukan dalam hal terjadinya suatu tindakan yang dilakukan oleh pihak lain dimana tindakan tersebut mengakibatkan ataupun menimbulkan kerugian dipihak lain, dan tindakan yang mengakibatkan kerugian tersebut yang disebut sebuah pelanggaran. Dan pelanggaran ini tidak hanya dilakukan oleh individu secara pribadi atau kelompok, tapi juga dapat terjadi ketika pelaku pelanggaran adalah aparat negara atau pemerintahan, bahkan bagi

kaum profesional pun tidak menutup kemungkinan dapat melakukan pelanggaran dalam melaksanakan profesi yang dijalaninya. Kaum profesional disini seperti halnya dokter atau pengacara, sedangkan pejabat negara atau penyelenggara negara yang dimaksud disini adalah pejabat pemerintah baik pusat maupun daerah, para penegak hukum, dan anggota-anggota komisi negara.
(Mahawisnu tridaya alam,2011)

2.3.1 Sistem Informasi

Data merupakan sebuah nilai atau keadaaan yang berdiri sendiri dan lepas dari konteks apapun,Sementara informasi adalah data yang telah diolah menjadi sebuah bentuk yang berarti penerimanya dan bermanfaat dalam pengambilan keputusan saat ini atau mendatang.dengan melihat dari pengertian data dan informasi di atas, sistem informasi dapat diartikan sebagai suatu alat untuk menyajikan informasi dengan cara sedemikian rupa sehingga bermanfaat bagi penerimanya. tujuannya adalah untuk menyajikan informasi guna pengambilan keputusan para perencanaan, pemrakarsaan, pengorganisasian, pengendalian kegiatan operasi subsistem suatu perusahaan, dan menyajikan sinergi organisasi pada proses. (Al Fatta,2007)

Sistem informasi yang berbasis komputer yang biasa disebut Sistem Informasi Manajemen dalam suatu organisasi terdiri dari komponen-komponen sebagai berikut :

a. Perangkat keras

   Adalah perangkat keras komponen untuk melengkapi masukan,proses, dan keluaran data.

b. Perangkat lunak

   Perangat lunak yaitu program dan instruksi yang diberikan ke komputer.

c. Database

Database adalah kumpulan dari data yang saling berhubungan satu dengan lainnya, tersimpan di perangkat keras komputer dan digunakan perangkat lunak untuk memanipulasinya.

d. Telekomunikasi

Yaitu komunikasi yang menghubungkan antara pengguna sistem dengan sistem komputer secara bersama-sama ke dalam suatu jaringan kerja.

e. Manusia

Manusia merupakan personel dari sistem informasi, meliputi manajer, analisis, programmer, dan operator, serta betanggung jawab terhadap perawatan sistem.

2.3.2 Pengembangan Sistem Informasi

Pengembangan sistem informasi sering disebut proses pengembangan sistem (*System Development*).Terdapat beberapa pendapat yang menjelaskan mengenai definisi dari pengembangan sistem, diantaranya :

a. Pengembangan sistem merupakan suatu proyek yang harus melalui suatu proses pengevaluasian seperti pelaksanaan proyek lainnya. (Amsa, 2008)
b. Pengembangan sistem dapat berarti menyusun sistem yang baru untuk menggantikan sistem yang lama secara keseluruhan atau untuk memperbaiki sistem yang sudah ada. (KAMI, 2008)
c. Pengembangan sistem adalah metode atau prosedur atau konsep atau aturan yang digunakan untuk mengembangkan suatu sistem informasi atau pedoman bagaimana dan apa yang harus dikerjakan selama pengembangan sistem (*algorithm*). Metode adalah suatu cara, teknik sistematik untuk mengerjakan sesuatu (dinu, 2008).

Metodologi pengembangan sistem menggunakan metodologi FAST (Frame The Aplication Of Sistem Thinking).Menurut Whitten (2004) langkah-langkah yang dilakukan adalah sebagai berikut :

a. Definisi Lingkup/ Analisis Awal

Dalam analisis awal ini adalah mengidentifikasi dan menganalisis masalah yang timbul untuk dijadikan bahan untuk dikaji.

b. Analisis masalah.

Analisis masalah mendeskripsikan masalah-masalah tersebut layak untuk dicarikan solusinya.

c. Analisis Kebutuhan

Analisis kebutuhan mendeskripsikan kebutuhan bahan yang dibutuhkan dalam menyelesaikan masalah.

d. Desain logis

Desain logis merupakan persyaratan perancangan sistem dengan menggunakan model-model sistem yang menggambarkan struktur data, proses bisnis, alur data, dan aliran data.

e. Analisis keputusan

Analisis keputusan merupakan sebuah analisis yang dibutuhkan untuk menghasilkan suatu solusi atau keputusan.

f. Desain fisik

Desain fisik mendeskripsikan rancangan tampilan yang akan dibuat dalam sebuah sistem.

g. Pengujian Sistem

Pengujian sistem dilakukan untuk mengetahui apakah program yang dibuat sudah sesuai dengan kebutuhan user.

h. Instalasi atau implementasi

Instalasi program berfungsi untuk menjalankan program secara langsung pada perusahaan.

2.3.3 Karakteristik Sistem Informasi

Sebuah sistem memiliki karakteristik ataupun sift-sifat sebagai berikut (Jogiyanto,1999):

a. Komponen Sistem (System Component)

Suatu sistem terdiri dari sejumlah komponen yang saling bekerjasama membentuk suatu kesatuan. komponen sistem atau elemen sistem berupa suatu kesatuan subsistem atau bagian-bagian dari sistem.

b. Batas Sistem (System Boundary)

Merupakan daerah yang membatasi antara suatu sistem dengan sistem yang lain atau dengan lingkungan luarnya.

c. Lingkungan Luar sistem (System Environment)

Lingkungan luar dari suatu sistem adalah batas luar sistem yang mempengaruhi operasi sistem. lingkungan luar sistem dapat bersifat menguntungkan dan dapat juga bersifat merugikan sistem tersebut.

d. Penghubung sistem (System Interface)

Merupakan media penghubung antara suatu subsistem yang lain dan memungkinkan sumber daya yang mengalir dari suatu subsistem ke subsistem lain. keluaran (ouput) dari suatu subsistem akan menjadi masukan (input) untuk subsistem yang lain dengan melalui penghubung.

e. Masukan Sistem (Input System)

Masukan dapat berupa masukan perawatan (maintenance input) dan masukan sinyal (signal input). Maintenance input adalah energi yang dimasukkan supaya sistem tersebut dapat beroperasi. Signal Input adalah energi yang diproses untuk subsistem yang lain.

f. Pengola Sistem (System Ouput)

Suatu sistem dapat mempunyai suatu bagian pengolah yang akan merubah masukan menjadi keluaran atau sistem itu sendiri sebagai pengolahnya.

g. Sasaran sistem (System Objectives)

Sistem harus mempunyai sasaran. sasaran dari sistem sangat menentukan sekali masukan dibutuhkan sistem dan keluaran yang akan dihasilkan sistem.

2.3.4 Konsep Basis Data

Database merupakan sekumpulan data yang saling terintegrasi satu sama lain dan terorganisasi berdasarkan sebuah skema atau struktur tertentu dan tersimpan pada sebuah hardware komputer. database terdiri dari beberapa tabel (lebih dari suatu tabel) yang saling terorganisir. tabel digunakan untuk menyimpan data dan terdiri atas baris dan kolom. Data tersebut dapat ditampilkan, dimodifikasi,dan dihapus dari tabel. Setiap pemakai

(user) yang diberi wewenang (otoritas) saja yang dapat melakukan akses terhadap data tersebut. (Arief,2006). Basis data memiliki operasi dasar, yaitu;

a. Pembuatan basis data (create database)
b. Penghapusan basis data (drop database)
c. Pembuatan file atau tabel (create tabel)
d. Penghapusan file atau tabel (drop tabel)
e. Penambahan atau pengisian data baru (insert)
f. Pengambilan data (retrie atau search)
g. Pengubahan data (update)
h. Penghapusan data (delete)

2.3.5 HTML

Hyper Text Markup Language (HTML) adalah sebuah *bahasa markah* yang digunakan untuk membuat sebuah halaman web, menampilkan berbagai informasi di dalam sebuah penjelajah web Internet dan pemformatan hiperteks sederhana yang ditulis dalam berkas format ASCII agar dapat menghasilkan tampilan wujud yang terintegerasi. Dengan kata lain, berkas yang dibuat dalam perangkat lunak pengolah kata dan disimpan dalam format ASCII normal sehingga menjadi halaman web dengan perintah-perintah HTML. Bermula dari sebuah bahasa yang sebelumnya banyak digunakan di dunia penerbitan dan percetakan yang disebut dengan SGML (*Standard Generalized Markup Language*), HTML adalah sebuah standar yang digunakan secara luas untuk menampilkan halaman web. HTML saat ini merupakan standar Internet yang didefinisikan dan dikendalikan penggunaannya oleh World Wide Web Consortium (W3C). HTML dibuat oleh kolaborasi Caillau TIM dengan Berners-lee Robert ketika mereka bekerja di CERN pada tahun 1989 (CERN adalah lembaga penelitian fisika energi tinggi di Jenewa).

2.3.6 MySQL

MySQL adalah sebuah implementasi dari sistem manajemen basis data relasioanal (RDBMS) yang didistribusikan secara gratis dibawah lisensi GPL (General Public License). setiap pengguna dapat secara bebas menggunakan MySQL, namun dengan batasan perangkat lunak tersebut tidak boleh dijadikan produk turunan yang bersifta komersial. MySQL sebenarnya merupakan turunan salah satu konsep utama dalam basis data yang telah ada sebelumnya yakni SQL (Structured Query language). SQL adalah sebuah konsep pengoperasian basis data, terutama untuk pemilihan atau seleksi dan pemasukkan data, yang memungkinkan pengoperasian data dikerjakan dengan mudah secara otomatis.

MySQL memiliki beberapa keistimewaan, antara lain :

a. **Portabilitas**. MySQL dapat berjalan stabil pada berbagai sistem operasi seperti Windows, Linux, FreeBSD, Mac Os X Server, Solaris, Amiga, dan masih banyak lagi.
b. **Perangkat lunak sumber terbuka**. MySQL didistribusikan sebagai perangkat lunak sumber terbuka, dibawah lisensi GPL sehingga dapat digunakan secara gratis.
c. **Multi-user**. MySQL dapat digunakan oleh beberapa pengguna dalam waktu yang bersamaan tanpa mengalami masalah atau konflik.
d. **Performance tuning'**, MySQL memiliki kecepatan yang menakjubkan dalam menangani *query* sederhana, dengan kata lain dapat memproses lebih banyak SQL per satuan waktu.
e. **Ragam tipe data**. MySQL memiliki ragam tipe data yang sangat kaya, seperti *signed / unsigned integer, float, double, char, text, date, timestamp,* dan lain- lain.
f. **Perintah dan Fungsi**. MySQL memiliki operator dan fungsi secara penuh yang mendukung perintah Select dan Where dalam perintah (*query*).
g. **Keamanan**. MySQL memiliki beberapa lapisan keamanan seperti level *subnetmask*, nama *host*, dan izin akses *user* dengan sistem perizinan yang

mendetail serta sandi terenkripsi.

h. **Skalabilitas dan Pembatasan**. MySQL mampu menangani basis data dalam skala besar, dengan jumlah rekaman (*records*) lebih dari 50 juta dan 60 ribu tabel serta 5 milyar baris. Selain itu batas indeks yang dapat ditampung mencapai 32 indeks pada tiap tabelnya.

i. **Konektivitas**. MySQL dapat melakukan koneksi dengan klien menggunakan protokol TCP/IP, Unix soket (UNIX), atau Named Pipes (NT).

j. **Lokalisasi**. MySQL dapat mendeteksi pesan kesalahan pada klien dengan menggunakan lebih dari dua puluh bahasa. Meski pun demikian, bahasa Indonesia belum termasuk di dalamnya.

k. **Antar Muka**. MySQL memiliki antar muka (interface) terhadap berbagai aplikasi dan bahasa pemrograman dengan menggunakan fungsi API (*Application Programming Interface*).

l. **Klien dan Peralatan**. MySQL dilengkapi dengan berbagai peralatan yang dapat digunakan untuk administrasi basis data, dan pada setiap peralatan yang ada disertakan petunjuk *online*.

2.3.7 PHP

PHP(Hypertext Preprocessor), merupakan bahasa pemrograman pada sisi server yang memperbolehkan programmer menyisipkan perintah – perintah perangkat lunak web server (apache, IIS, atau apapun) akan dieksekusi sebelum perintah itu dikirim oleh halaman ke browser yang me-*request*-nya, contohnya adalah bagaimana memungkinkannya memasukkan tanggal sekarang pada sebuah halaman web setiap kali tampilan tanggal dibutuhkan. Sesuai dengan fungsinya yang berjalan di sisi server maka PHP adalah bahasa pemrograman yang digunakan untuk membangun teknologi *web application.* (Kevin Yank, 2002).

PHP telah menjadi bahasa *scripting* untuk keperluan umum yang pada awalnya hanya digunakan untuk pembangunan web yang menghasilkan halaman web dinamis. Untuk tujuan ini, kode PHP tertanam ke dalam

dokumen sumber *HTML* dan diinterpretasikan oleh server web dengan modul PHP prosesor, yang menghasilkan dokumen halaman web. Sebagai bahasa pemrograman untuk tujuan umum, kode PHP diproses oleh aplikasi penerjemah dalam modus baris - baris perintah modus dan melakukan operasi yang diinginkan sesuai sistem operasi untuk menghasilkan keluaran program dichannel output standar. Hal ini juga dapat berfungsi sebagai aplikasi grafis. PHP tersedia sebagai prosesor untuk server web yang paling modern dan sebagai penerjemah mandiri pada sebagian besar sistem operasi dan komputer *platform.* (wikipedia.org, 2016).

2.3.8 Xampp

Adalah perangkat lunak bebas, yang mendukung banyak sistem operasi, merupakan kompilasi dari beberapa program. Fungsinya adalah sebagai server yang berdiri sendiri (localhost), yang terdiri atas program Apache HTTP Server, MySQL database, dan penerjemah bahasa yang ditulis dengan bahasa pemrograman PHP dan Perl. Nama XAMPP merupakan singkatan dari X (empat sistem operasi apapun), Apache, MySQL, PHP dan Perl. Program ini tersedia dalam GNU General Public License dan bebas, merupakan web server yang mudah digunakan yang dapat melayani tampilan halaman web yang dinamis. Untuk mendapatkanya dapat mendownload langsung dari web resminya.

Bab III Metodologi Penelitian

3.1. Alat dan Bahan Penelitian

Penelitian ini menggunakan alat berupa hardware dan software , sedangkan bahan yang digunakan dalam penelitian ini adalah data-data yang mendukung proses penelitian.

3.1.1. Alat

Alat adalah perangkat yang digunakan dalam pembuatan sistem informasi pelaporan cybercrime ini, terdiri dari 2 bagian yaitu hardware dan software, diantaranya adalah :

a. Hardware (Perangkat keras).

   Pengertian perangkat keras untuk Sistem Informasi pelaporan Cybercrime ini sebenarnya dihubungkan dengan setiap peralatan fisik (physical devices) yang digunakan satu sistem komputer. Perangkat keras yang mendukung didalam pembuatan sistem ini adalah :

   1. Processor Intel Corei3.

      Processor jenis ini digunakan untuk membuat pengguna sistem informasi pelaporan cybercrime ini lebih cepat dalam memproses data.
   2. RAM 2 GB.
   3. Hardd Disk 500 GB.
   4. Monitor 14’’.
   5. Keyboard dan Mouse

b. Software (Perangkat lunak)

   Perangkat lunak untuk komputer bukan hanya satu, dalam terminologi komputer perangkat lunak sebenarnya ada tiga jenis, yaitu: *Operating system, special system support program, dan aplication software.* berdasarkan catatan di iatas, perangkat lunak sistem informasi pelaporan Cybercrime adalah:

1. Sistem operasi Windows 7 X86
2. XAMPP tools versi 5 20
3. Text editor (Macromedia Dreamweaver 8)
4. Web browser
5. Corel draw X5 dan Adobe photoshop CS 5

3.1.2. Bahan Penelitian

Bahan penelitian merupakan entitas yang menjadi objek yang diolah atau diberi perlakuan-perlakuan tertentu, pengolahan atau perlakuan tersebut akan menghasilkan fenomena-fenomena yang dapat diamati, yang selanjutnya digunakan sebagai bahan kajian dalam penelitian (pedoman skripsi ilmu komputer UPI, 2007). Tidak hanya objek yang bersifat riil saja yang dijadikan bahan penelitian, objek berupa informasi yang bersifat abstrak pun dapat dijadikan bahan penelitian.

3.2 Waktu dan Tempat penelitian

3.2.1. Waktu penelitian

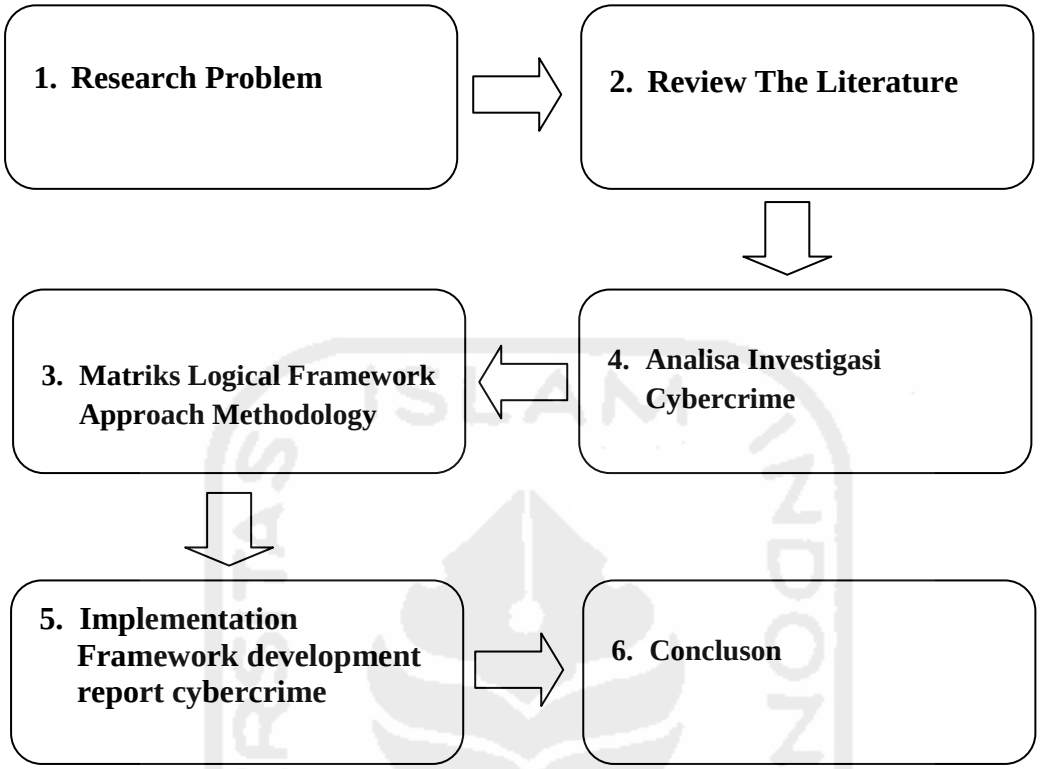
Penelitian ini dilakukan mulai bulan Agustus sampai bulan Desember 2016.

3.2.2. Tempat penelitian

Tempat penelitian dilakukan di Polda Yogyakarta.

3.3. Metode Penelitian

Pada bab ini menjelaskan cara penelitian dimana terdapat rincian tentang urutan langkah-langkah yang dibuat secara sistematis, logis sehingga dapat dijadikan pedoman yang jelas dan mudah untuk menyelesaikan permasalahan, analisis hasil dan kesulitan-kesulitan yang dihadapi. Urutan langkah-langkah



Gambar 3.1 Metodologi Penelitian

3.3.1 *Identifying Research Problem*

Identifying Research Problem merupakan langkah awal yang dilakukan untuk memperoleh dan menentukan topik penelitian yang akan diteliti lebih lanjut. Pada tahapan ini dimulai dengan melihat berbagai fenomena, kejadian dan informasi yang didapatkan dengan berbagai cara.

Dalam hal ini, New Model for Cyber Crime Investigation Procedure (Oleh: Yong-Dal Shin,2011). sehingga perlu dilakukan beberapa pengujian terhadap New Model for Cyber Crime Investigation Procedure itu dengan tujuan untuk mengetahui segala kekurangan yang ada pada *framework* tersebut.

3.3.2. *Review the literarure*

Diharapkan mampu menggali seluruh informasi yang terkait dengan permasalahan yang akan diteliti dan obyek yang menjadi tujuan penelitian. *Reviewing the literarure* ini memberikan dasar bagi arah penelitian yang

akan dilakukan serta menjadi awal pemikiran bagi setiap peneliti sehingga penelitian yang dilakukan dapat dijadikan acuan kembali dikemudian hari.

Reviewing the literarure yang dilakukan disini adalah dengan cara melakukan pencarian dasar-dasar teori dan penemuan dari penelitian yang telah diakukan sebelumnya. Teori-teori yang terkait dengan permasalahan penelitian Investigation Cyber Crime yang berhubungan dengan Forensika Digital serta dan khususnya tentang Pengembangan Framework pelaporan penelitian yang menggabungkan beberapa model evaluasi berusaha digali dan dirangkumkan secara singkat sesuai dengan kebutuhan dalam penelitian ini. *Reviewing the literarure* dilakukan dengan membaca, merangkum, kemudian menuliskannya kembali dengan metode yang sudah ditentukan. Teori diperoleh dari jurnal dan melalui publikasi-pulikasi jurnal nasional dan internasional.

3.3.3. Analisis Matriks *Logical framework approach*

Ada beberapa kegiatan yang dilakukan dalam melakukan analisis *Logical framework approach* ini. Diantaranya yaitu menyusun matrik logframe sebagai perencanaan seluruh kegiatan evaluasi yang dilakukan. Yang kemudian nantinya matrik logframe akan dirinci kembali menjadi beberapa bagian matrik sehingga didapat alur evaluasi yang terstruktur untuk mencapai tujuan yang telah ditetapkan.

Matrik logframe evaluasi merupakan matrik dari seluruh aktivitas evaluasi yang dilakukan. Matrik ini tersusun dari empat elemen dasar yaitu hubungan antara tujuan (goals), sasaran (purpose), keluaran (outputs), dan kegiatan (activities).

Matrik ini juga menjadi landasan kegiatan apa saja yang dilakukan untuk menjalankan evaluasi terhadap *framework* sehingga dapat menghasilkan *framework* yang telah memenuhi seluruh ketentuan dalam SNI 27037:2014 dan layak untuk digunakan. Adapun bentuk matriks yang direncanakan akan dianalisis yaitu seperti pada tabel 3.3.2 dibawah ini.

Deskripsi Kegiatan	**Indikator**	**Verivikasi Indikator**	**Asumsi**
Goal/Tujuan			
Purpos/Sasaran			
Outputs/Keluaran			
Activites/Aktfitas			

3.3.4 Implementation Framework development report cybercrime

Menurut wikipedia, Kerangka kerja (framework) adalah suatu struktur konseptual dasar yang digunakan untuk memecahkan atau menangani suatu masalah kompleks. Istilah ini sering digunakan antara lain dalam bidang perangkat lunak untuk menggambarkan suatu desain sistem perangkat lunak yang dapat digunakan kembali, serta dalam bidang manajemen untuk menggambarkan suatu konsep yang memungkinkan penanganan berbagai jenis atau entitas bisnis secara homogen. Sedangkan dalam Kamus Oxford mendefinisikan Frameworks sebagai "struktur pendukung atau yang mendasari".

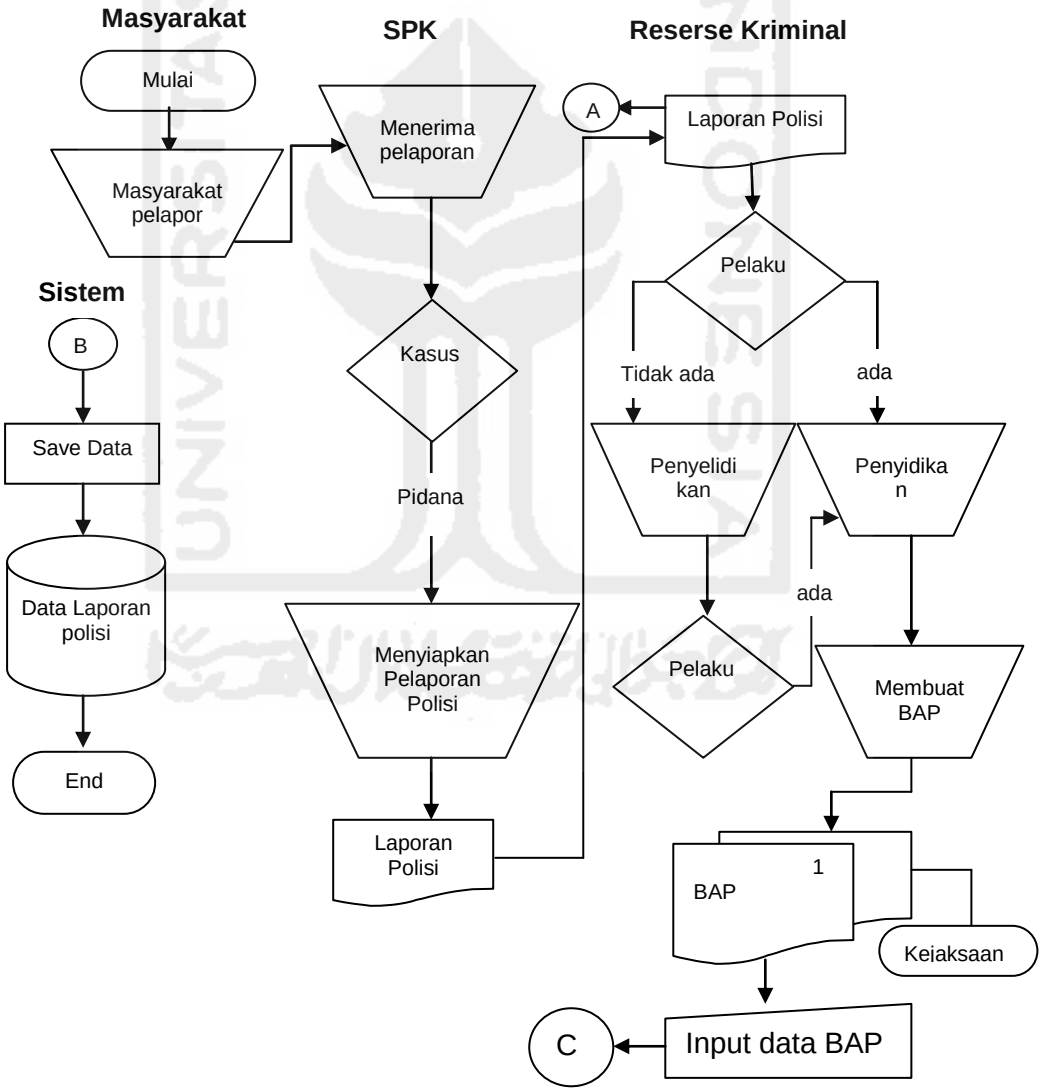
Framework komputer forensik dapat didefinisikan sebagai struktur untuk mendukung kesuksesan dalam penyelidikan forensik. Ini berarti dapat disimpulkan bahwa tujuan yang ingin dicapai oleh ahli forensic hasilnya harus sama dengan orang lain yang juga melakukan penyelidikan yang sama. Sebuah framework juga tergantung pada sejumlah struktur.

Adapun tahapan untuk Implementasi Pengembangan Framework Pelaporan Cyber crime adalah sebagai berikut:

3.3.4.1 Framework Pelaporan yang sebelumnya sudah ada

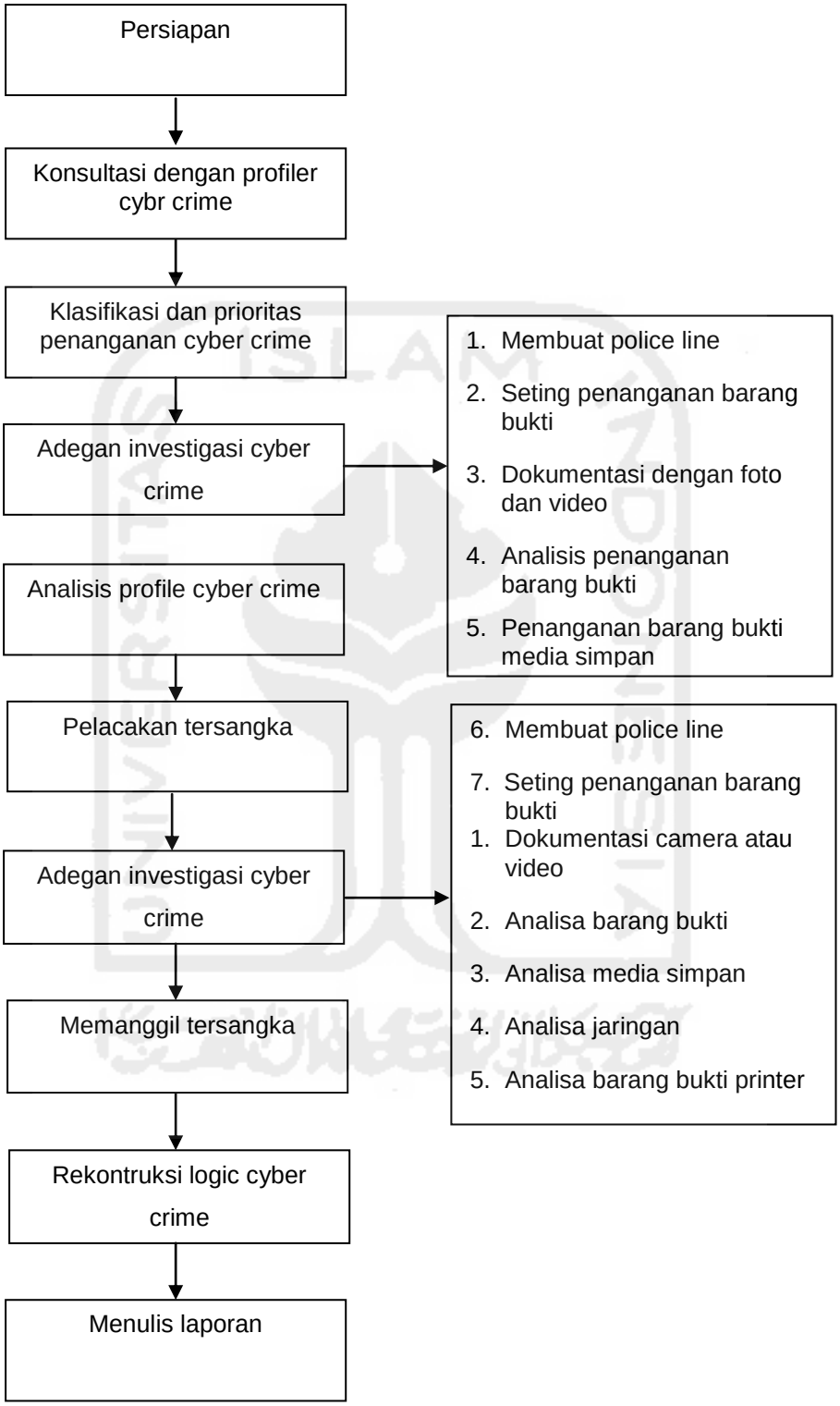
a. Tahapan pelaporan Tindak Kriminal dikepolisian

Tahapan yang dikembangkan oleh peneliti sebelunya yang ditulis oleh Tiur Gantini dan Peter Iman Paskal Mendrofa yaitu tahapan dalam mempercepat pembuatan yaitu laporan berkas tindak pidana kriminal. Laporan dari masyarakat tentang tindak criminal ke pihak kepolisian.



Gambar a. Tahapan pelaporan tindak Kriminal di kepolisian

b. Tahapan New Model Investigation Cyber Crime



Gambar b. Framework SOP (Standar Operasinal Procedure) New model investigation Cyber crime

Dari framework pelaporan diatas perbedaannya yaitu untuk Framework pelaporan tindak kriminal secara umum untuk korban mulai dari melapor kepada pihak kepolisian sampai dengan proses penyidikan secara detail setelah itu diserahkan kepada pihak kejaksaaan tapi untuk Framework New model cybercrime yaitu pelaporan dari pihak intern kepolisian setelah menerima laporan dari korban dan diteruskan kepada penyidik yaitu kejahatan yang berhubungan dengan Teknologi Informasi dan Komunikasi dan alur yang dibahas pada proses Investigasi dari penyidik dalam penanganan alat bukti kejahatan cybercrime.

3.3.4.2 Tahapan Pelaporan Cyber crime yang berjalan di Kepolisian

Saat ini sistem Pelaporan yang berjalan dikepolisian, mulai dari tingkat Polsek, polres, Polda sampai tingkat pusat khususnya yang berhubungan dengan pelaporan kejahatan Cybercrime masih menjadi satu dengan tindak kejahatan kriminal yang umum dan cara pelaporan yang masih Konvensional, sebagai contoh Masyarakat yang mengalami korban kejahatan kriminalitas datang kekantor kepolisian membawa bukti foto copy atau dokumen yang berkaitan dengan tindak pidana atau kasus yang dilaporkan atau diadukan pelapor membuat surat penyataan yang menyatakan bahwa laporan tersebut belum pernah dilaporkan atau ditangani oleh polisi. laporan atau pengaduan diserahkan dari siaga Ops kepada kepolisian yang piket. piket reskrimsus membawa laporan pengaduan ke Bagian Bin Opsonal untuk di register dan oleh Kabag Bin Opsnal ditelaah dan dipelajari kemudian diteruskan ke Kasubdit atau penyidik kemudian Kasubdit mendisposisikan meneruskan ke salah satu unit dalam lingkungan kerja satuan fungsinya untuk menangani atau diproses laporan tersebut setelah laporan diterima oleh Kanit atau tim penyidik yang ditugaskan untuk menangani laporan tersebut membuat rencana penyelidikan dan penyidikan serta melakukan penilaian terhadap laporan yang diterima paling lama 3 (tiga) hari setelah diterima Laporan Polisi, penyidik membuat SP2HP format A1. setelah itu pemohon pelapor datang lagi kekantor kepolisian untuk mengambil jawaban surat

permohonannya tersebut. hal ini memakan waktu yang cukup lama atau bisa dikatakan penggunaan waktu yang tidak efesien.

Dari permasalahan yang terjadi tentang laporan pengaduan dari masyarakat kepihak kepolisian yang masih secara konvensional, maka dibuatlah sistem pelaporan yang terbaru untuk memberikan kemudahan kepada pihak publik, serta mempermudah masyarakat dalam penyampaian pengaduan ke kepolisian yang cepat dan akurat.

Gambar 3.3.4.2. Alur pelaporan Cyber crime yang yang dibuat sendiri oleh Polda Yogyakarta dan berkoordinasi dengan kejati DIY.

KEPOLISIAN NEGARA REPUBLIK INDONESIA DAERAH ISTIMEWA YOGYAKARTA DIREKTORAT RESERSE KRIMINAL KHUSUS SUBDIT	NOMOR SOP : SOP/IX/2016 Ditreskrimus TANGGAL PEMBUATAN : 30 SEPTEMBER 2016 TANGGAL REVIS I: 30 SEPTEMBER 2016 TANGGAL PENGESAHAN : 30 SEPTEMBER 2016 DISAHKAN OLEH : DIREKTUR RESERSE KRIMINAL ANTONIUS PUJIANTO,S.H KOMISARIS BESAR POLISI NRP 62060946
	Nama SOP : pendistribusian LP dan Aduan dari pelapor

NO	URAIAN KEGIATAN	PELAKSANA			
		BANUM	KASUBDIT	KANIT	PENYIDIK/PENYIDIK PEMBANTU
1	2	3	4	5	6
1	Penyampaian laporan polisi dari bag binops ke Banum Subdit II Ditreskrimsus				
2	Penerimaan LP dan/atau aduan oleh Banum				
3	Penyampaian LP dan/atau aduan kepada Kasubdit				
4	Pembuatan Disposisi penanganan dari Kasubdit ke Kanit				
5	Jika Kasubdit berhalangan Kanit dapat langsung ditangani. mendisposisikan kepada Unit untuk ditangani				
6	Banum meregistrasi hasil disposisi Kasubdit ke buku Register				
7	Hasil Disposisi Kasubdit di Registrasi oleh Kanit				
8	Kanit mendistribusikan ke Penyidik				

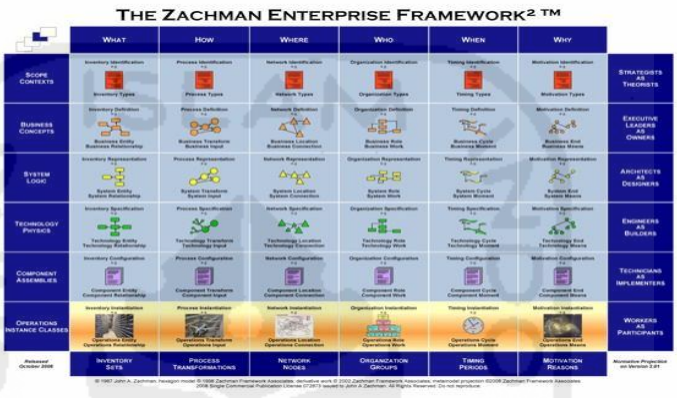
KETERANGAN

ARAH GIAT — ALTERNATIF GIAT

MULAI GIAT — LANJUT HALAMAN

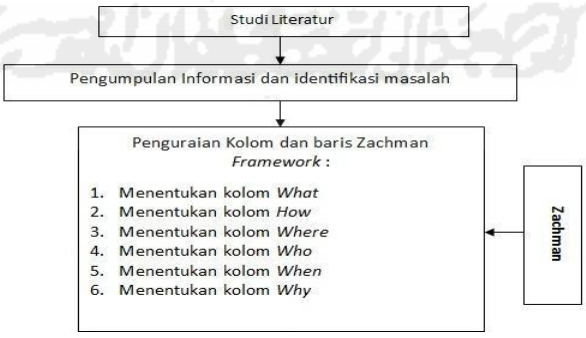
GIAT — AKHIR GIAT

Dalam penelitian Pengembangan Framework pelaporan Cybercrime menggunakan Metode Zachman Framework merupakan salah satu metode EAP yang banyak digunakan diseluruh dunia dalam perancangan sistem dimana didalam metode ini perencanaan dilakukan dengan langkah-langkah yang sistematis, mudah dipahami dan dapat dijadikan control untuk pengembangan sistem informasi ke depan.



Gambar 3.1. Framework Zachman

Dalam penelitian ini metode yang digunakan untuk menganalisa perancangan sistem adalah menggunakan framework Zachman yang akan dijabarkan dalam masing-masing kolomnya yang terdiri dari What, How, Where, Who, When dan Why. Pada penelitian ini yang akan dijabarkan hanya dari sudut pandang User dan Administrator.



Gambar 3.2 Alur Penelitian

Berdasarkan hasil pengumpulan data maka selanjutnya akan dilakukan proses pemetaan masalah kedalam kerangka Zachman untuk menghasilkan rancangan sistem yang dibutuhkan. Setelah peta masalah didapatkan maka selanjutnya masalah-masalah tersebut akan disusun dalam kerangka matrik Zachman. Setelah matrik Zachman diperoleh maka masing-masing baris dan kolom pada matrik tersebut akan diuraikan satu persatu.

Berikut adalah penjabaran dari matrik Zachman dari hasil penelitian :

a. Kolom What

   Menjelaskan tentang data yang dapat disajikan dari sudut pandang User dan Administrator .

b. Kolom How

   Kolom ini membahas tentang proses yang terjadi pada Pelaporan Cyber crime di Polda Yogyakarta.

c. Kolom Where

   Kolom ini membahas tentang lokasi bisnis utama tempat sitem informasi berada beserta infrastruktur dan konfigurasinya.

d. Kolom Who

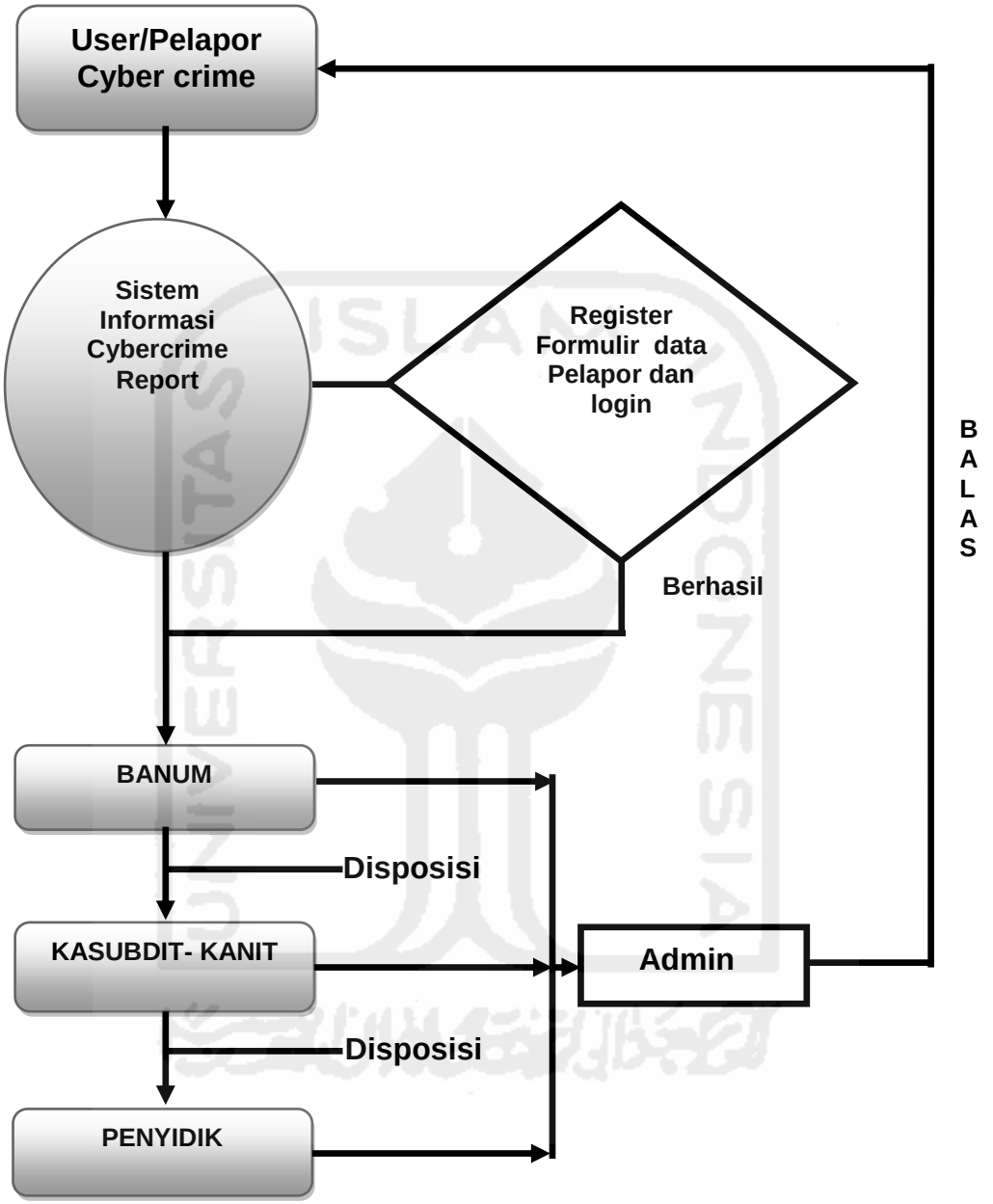
   Kolom ini membahas tentang sumber daya manusia yang berperan penting dalam proses pelaporan Cyber crime di Polda Yogyakarta.

e. Kolom When

   Kolom ini membahas tentang kejadian atau kegiatan beserta jadwalnya. Kegiatan utama yang akan dibahas adalah yang berkaitan dengan pelaporan Cyber crime.

f. Kolom Why

   Menjabarkan tentang tujuan, motivasi dan inisiatif serta batasan-batasan yang ditetapkan berkaitan dengan Sistem informasi yang akan dibangun.

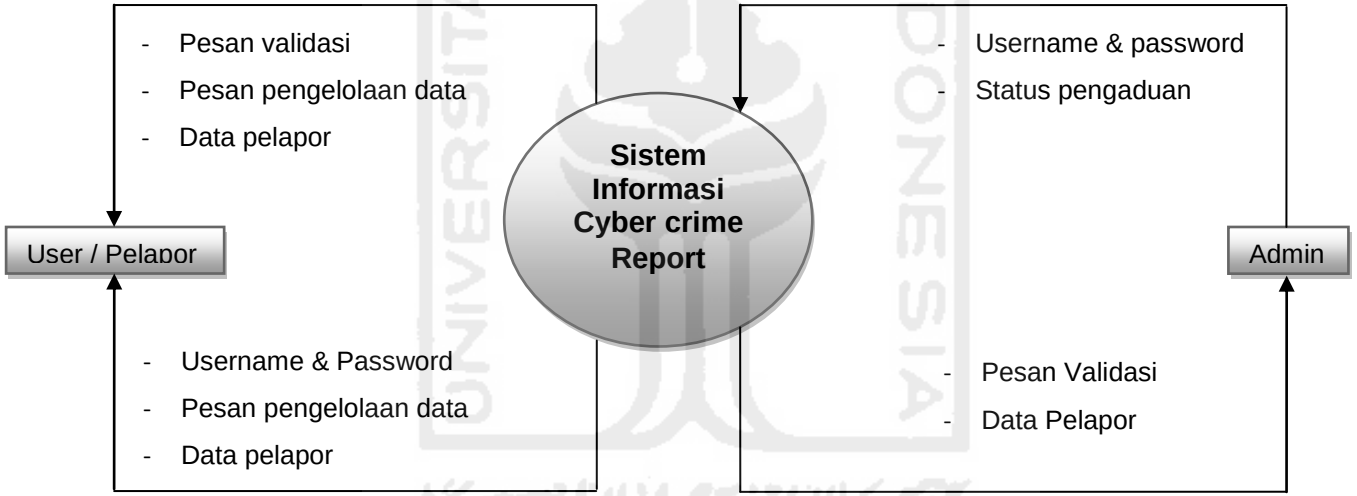


Gambar 3.3.4.3 Alur pelaporan yang diusulkan

3.3.5 Diagram Konteks

3.3.5.1 DFD Level 0

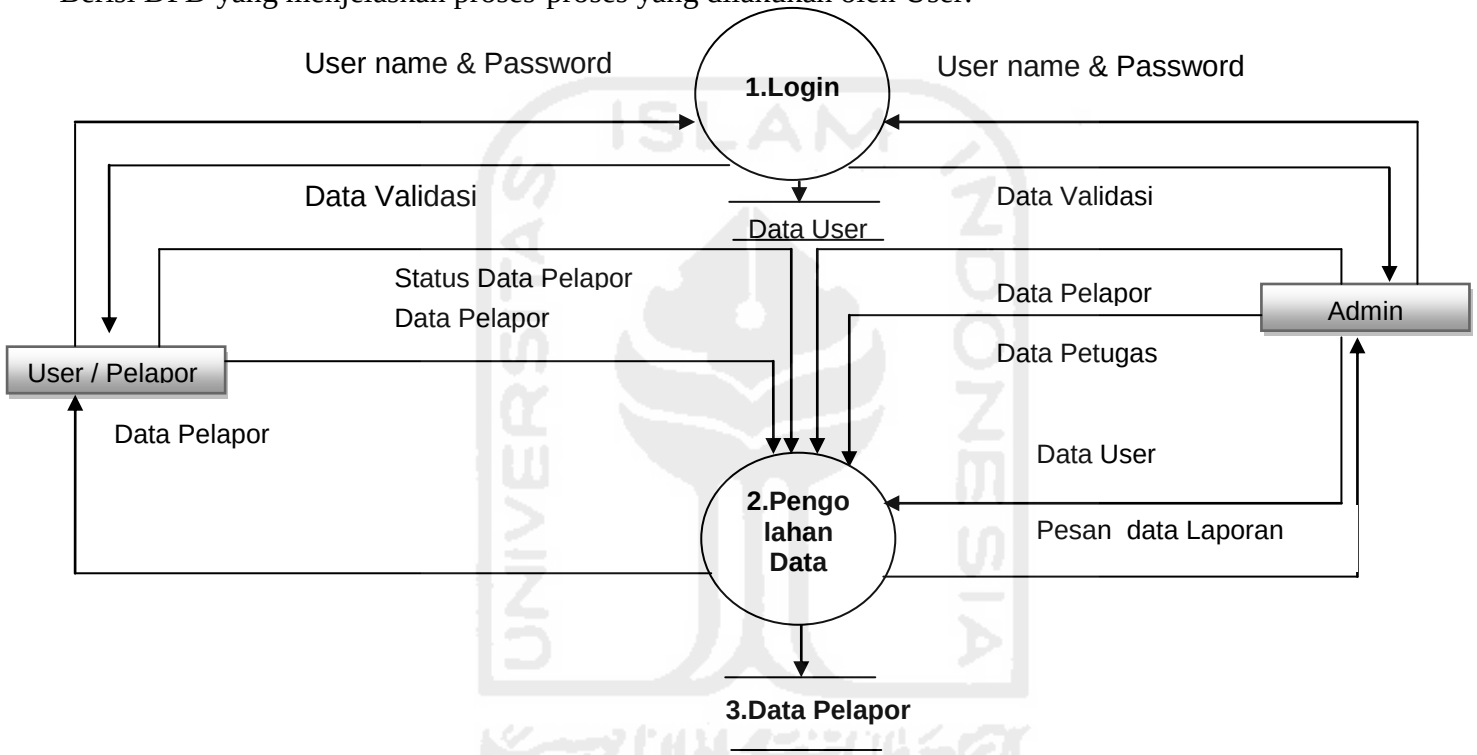
Diagram level 0 atau yang bisa disebut konteks diagram menggambarkan secara keseluruhan proses yang ada pada sistem dengan kesatuan luar yang ada pada sistem. Berikut gambar 1 DFD level 0 Sistem Informasi Pelaporan Cyber crime.



Gambar 3.6.3.1. DFD Level 0

3.3.5.2 DFD Level 1 Input User

Berisi DFD yang menjelaskan proses-proses yang dilakukan oleh User.

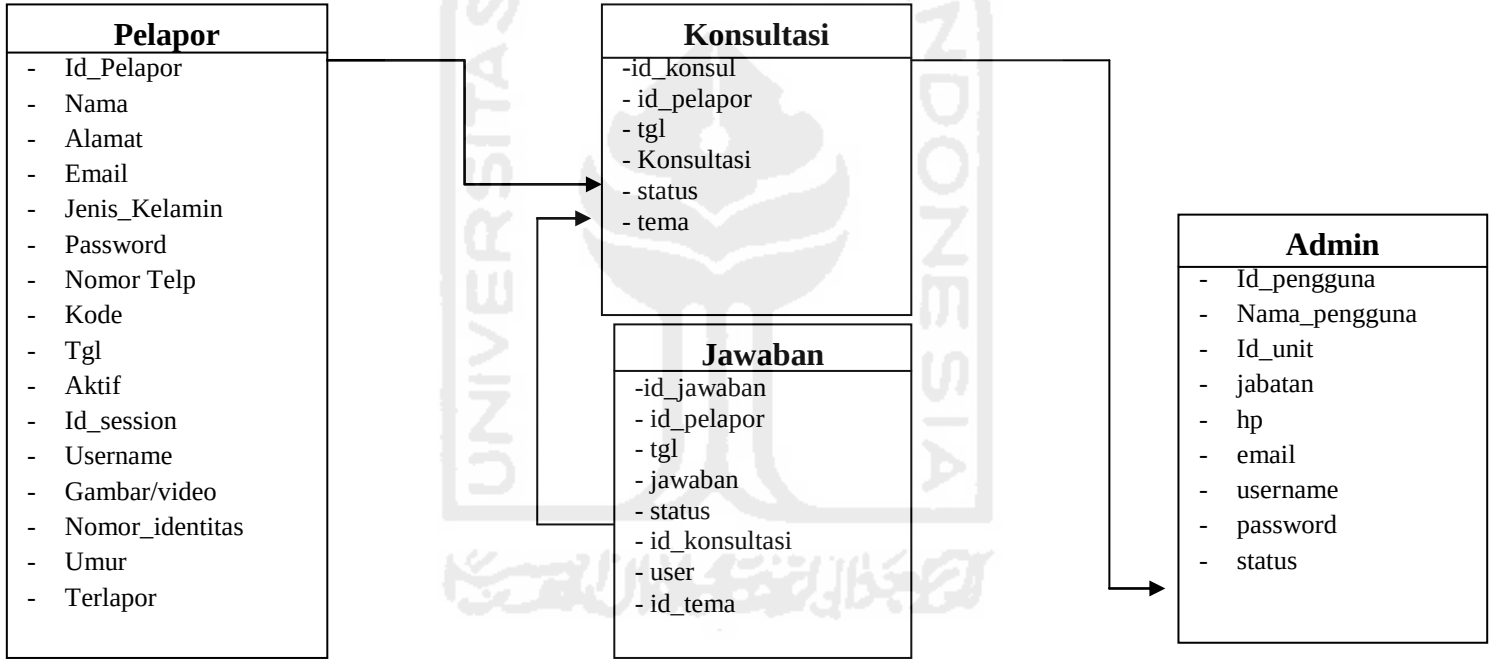


Gambar 3.6.3.2 DFD Level 1

3.3.6 Perancangan Basis Data

Perancangan basis data merupakan perancangan yang digunakan untuk pembuatan dan penyimpanan data ke dalam system terdiri dari beberapa *file database*.

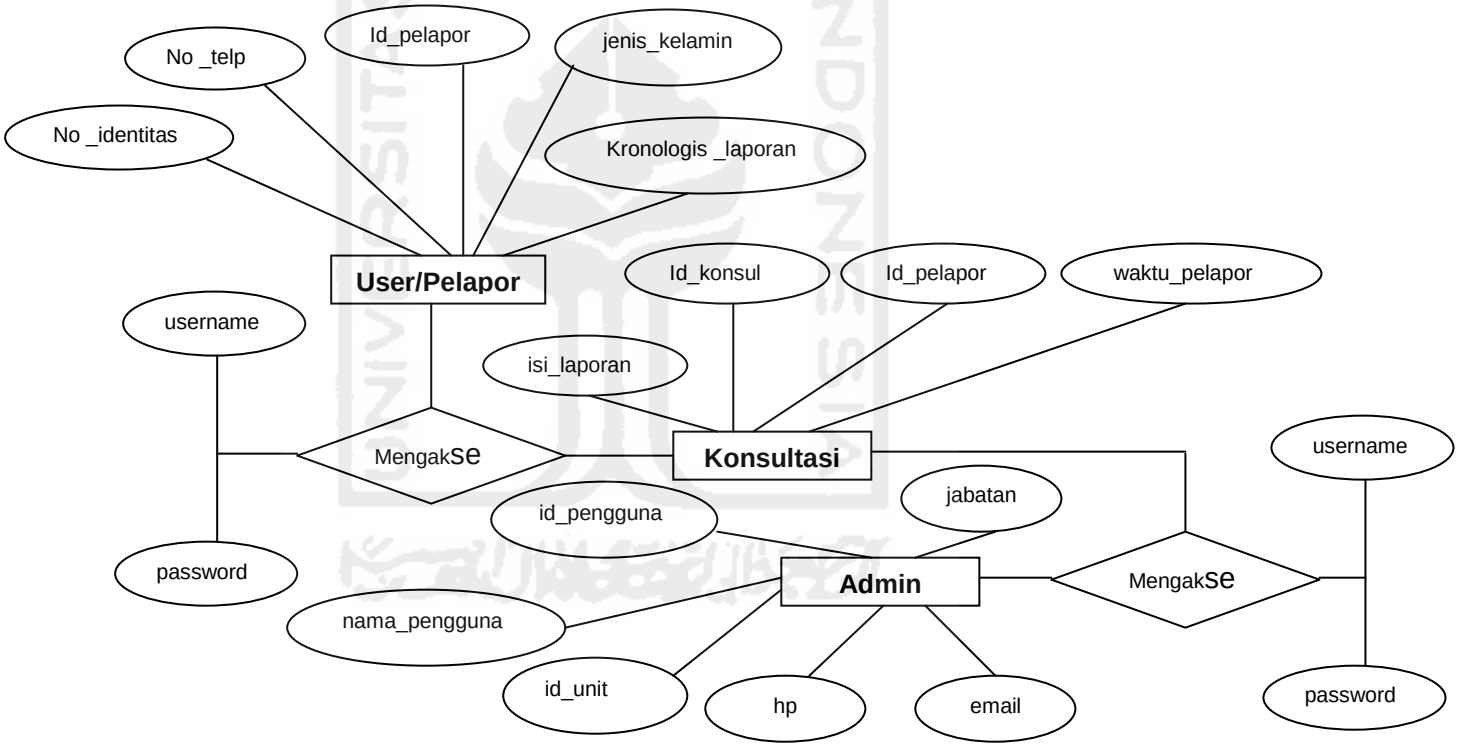
3.3.5.1 Tabel Relasi



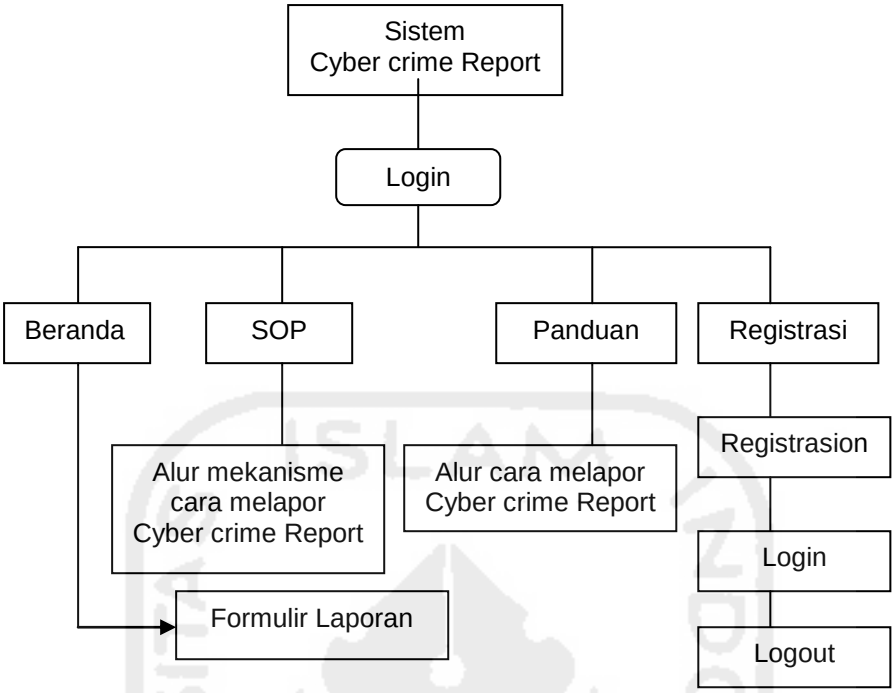
Gambar 3.3.4.3 Tabel Relasi

3.3.6.2 Model Data Konseptual (Diagram ER-D)

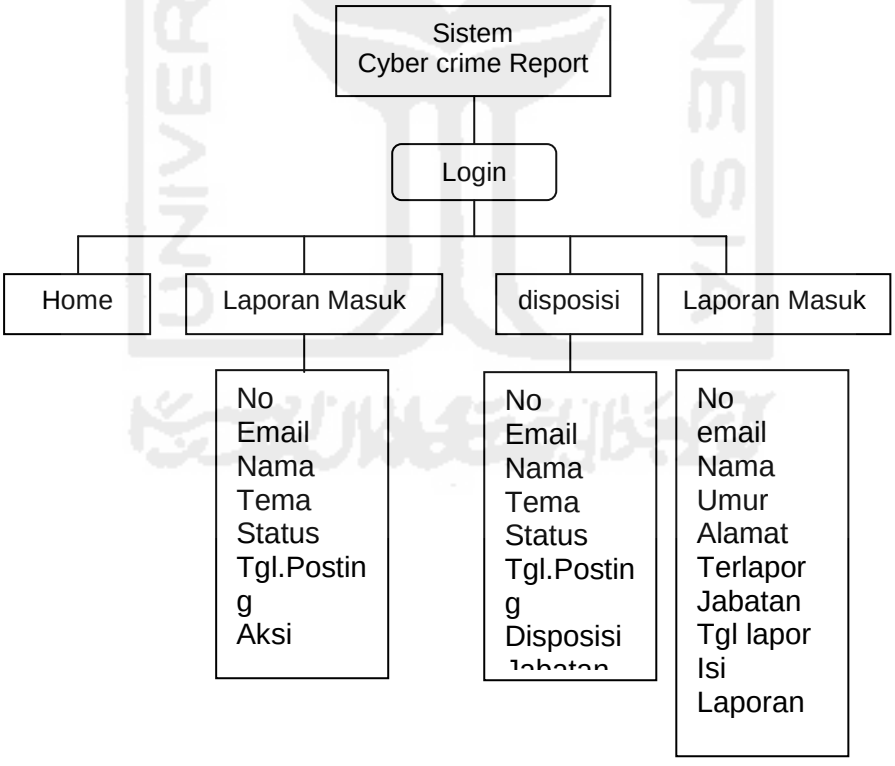
ERD merupakan suatu model untk mejelaskan hubungan antar data dalam basis data berdasarkan objek-objek dasar data yang mempunyai hubungan antar relasi. ERD dapat memodelkan struktur data dan hubungan antar data, untuk menggambarkannya digunakan beberapa notasi dan symbol. Untuk diagram ER-D nya dapat dilihat pada gambar di bawah ini :



3.4 Perancangan Struktur Menu



Gambar 3.4 Struktur Menu User/Pelapor



3.4. Gambar Struktur Menu Admin/ Kepolisian

3.5 Pengujian Sistem

Pada Pengembangan Framework pelaporan cybercrime ini menggunakan metode pengujian *black box testing* dilakukan dengan cara menguji beberapa aspek sistem dengan sedikit memperhatikan struktur logika internal sistem. Sistem dikatakan dapat berfungsi dengan baik yaitu pada saat input diberikan dan output memberikan hasil sesuai dengan spesifikasi sistem yang dibuat. Berikut pengujian dapat dilihat pada tabel:

Tabel 3.5 Pengujian sistema

NO	Skenario Pengujian	Test Case	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
1	Masuk ke Sistem cyber-crimereport.cf Mengosongkan semua isian data login,lalu langsung mengisikan Form Laporan	Nama,Identitas,Email,No HP,Umur,Jenis kelamin,Alamat,terlapor, Uraian singkat kejadian	Sistem akan menolak akses registrasi pesan *"mohon Form Laporan isi dulu atau sudah didaftarkan"*menerima akses registrasi dan menampilkan terimakasih *"andaberhasil sudah registrasi di system Cyber-crimereport.cf"* username dan password ke email	Sesuai harapan	Valid

NO	Skenario Pengujian	Test Case	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
2	Login Ke Email untuk mendapatkan Username dan Password untuk login ke Cyber-crimereport.cf	Username dan Password email	Sistem akan menerima akses login email dan membuka Inbox/kotak surat masuk melihat akun yang berisi "Username dan Password"	Sesuai harapan	Valid
3	Menginputkan Username dan Password di menu Register Login	Username: cahkra2010@gmail.com Password:4864375575872 2c2616413	Sistem akan menerima register login dan menampilkan menu member yaitu Laporan(Lembar konsultasi Subjek laporan dan Pesan),testimony(Form Testimoni),Log out dan Edit Profil (Nama,Alamat,Email,No HP, Jenis kelamin,Password baru, browse Foto.	Sesuai harapan	Valid

NO	Skenario Pengujian	Test Case	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
4	Klik Menu PANDUAN	PANDUAN cara melapor pada cyber-crimerepor.cf	Menampilkan cara melaporkan dari USER pada system	Sesuai harapan	Valid
5	Klik Menu SOP	SOP pada pelaporan dikepolisian	Menampilkan pada Sistem tentang SOP di Kepolisian	Sesuai harapan	Valid
6	Login ke ADMIN umum cyber-crimereport.cf/admin web	Username:Admin Password:beauty123	Sistem akan menolak akses login apabila username dan password yang diisikan salah.sistem akan menerima akses login dan kemudian menampilkan menu data Laporan dari user yang berisi nama,hal laporan,status,tanggal posting dan isi laporan	Sesuai harapan	Valid

NO	Skenario Pengujian	Test Case	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
7	Login ke ADMIN person BANUM	Username: 1 Password:1	Sistem akan menolak akses login apabila username dan password yang diisikan salah.sistem akan menerima akses login dan kemudian menampilkan menu Home,Laporan masuk,dispoisi, data laporan dan Log out	Sesuai Harapan	Valid
8	Login ke ADMIN person KASUBDIT(UNIT PERTAMA)	Username:pertama Password:pertama	Sistem akan menolak akses login apabila username dan password yang diisikan salah.sistem akan menerima akses login dan kemudian menampilkan menu Home,Laporan masuk,dispoisi dan Log out	Sesuai harapan	Valid

NO	Skenario Pengujian	Test Case	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
9	Login ke ADMIN person KASUBDIT(UNIT KEDUA)	Username:kedua Password: Kedua	Sistem akan menolak akses login apabila username dan password yang diisikan salah.sistem akan menerima akses login dan kemudian menampilkan menu Home,Laporan masuk,dispoisi dan Log out.	Sesuai harapan	Valid
10	Login ke ADMIN person PENYIDIK PERTAMA	Username:penyidik pertama Password:penyidik pertama	Sistem akan menolak akses login apabila username dan password yang diisikan salah.sistem akan menerima akses login dan kemudian menampilkan menu Home,Laporan masuk,dispoisi dan Log out.	Sesuai harapan	Valid

NO	Skenario Pengujian	Test Case	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
11	Login ke ADMIN person PENYIDIK KEDUA	Username:penyidik kedua Password:penyidik kedua	Sistem akan menolak akses login apabila username dan password yang diisikan salah.sistem akan menerima akses login dan kemudian menampilkan menu Home,Laporan masuk,dispoisi dan Log out.	Sesuai harapan	Valid

Proses pengujian pada penelitian ini melibatkan pengembang, pengguna dan Administrator melakukan pengujian untuk memastikan sistem berjalan dengan baik sesuai proses yang ditentukan.pengguna yang melakukan proses penggujian dengan cara mencoba menggunakan sistem ini untuk memberikan evaluasi dalam bentuk kritik dan saran terhadap sistem yang sudah dibuat.hasil evaluasi dari pengguna dijadikan pertimbangan bagi pengembang untuk ditindaklanjuti dalam proses perbaikan sistem.

Bab IV Hasil dan Pembahasan

Bab ini, akan membahas tentang hasil analisis yang dilakukan terhadap apa yang diperoleh, ditinjau secara kualitatif. Berdasarkan hasil evaluasi dan perbaikan yang dilakukan maka akan dapat dihasilkan sebuah *framework* hasil perbaikan yang telah memenuhi ketentuan dan layak untuk digunakan dalam melakukan Investigasi Cybercrime.

4.1 Review the literature

Ada beberapa model untuk penyelidikan Investigasi Cyber Crime dalam literatur.

4.1.1. Lee Model Ilmiah Crime Scene Investigation

Lee et al. (2001) mendiskusikan ilmiah penyelidikan TKP sebagai suatu proses. Model ini TKP investigasi, tidak dengan proses investigasi penuh. Saya mengidentifikasi empat langkah dalam proses.

Pengakuan **a**dalah langkah pertama, di mana barang atau pola yang terlihat menjadi potensibukti. penyidik harus tahu baik apa yang harus dicari dan di mana dapat ditemukan. Pengakuan mengarah ke dua sub-kegiatan: dokumentasi dan pengumpulan dan pengamanan.

Identifikasi berbagai jenis bukti adalah langkah berikutnya. Ini melibatkan klasifikasi bukti, dan satu sub-kegiatan, perbandingan. Fisik, biologi, kimia, dan sifat lain dari barang bukti yang dibandingkan dengan standar yang dikenal yang.

Individualisasi mengacu menentukan apakah barang bukti yang mungkin adalah unik sehingga bahwa mereka mungkin terkait dengan individu atau peristiwa tertentu. Dalam hal ini, barang-barang harus dievaluasi dan diinterpretasikan.

Rekonstruksi melibatkan menyatukan output dari bagian-bagian awal dari proses, dan informasi terkait lainnya yang peneliti .

4.1.2. Casey (2000)

menyajikan model untuk pengolahan dan memeriksa bukti-bukti digital.

langkah-langkah berikut:

1. Pengakuan
2. Pengamanan, koleksi, dan dokumentasi
3. Klasifikasi, perbandingan, dan individualisasi
4. Rekonstruksi

4.1.3. Forensik pertama Digital Research (Palmer, 2001)

Menghasilkan model yang menetapkan langkah-langkah untuk analisis forensik digital dalam proses linear. Langkah-langkahnya sebagai berikut:

1. Identifikasi
2. Pengamanan
3. Koleksi
4. Pemeriksaan
5. Analisis
6. Presentasi
7. laporan

4.1.4 Reith, Carr dan Gunsch (2002)

Menggambarkan model yang sampai batas tertentu yang berasal dari model DFRWS. Langkah-langkah dalam model mereka adalah:

1. Identifikasi
2. Persiapan Strategi
3. Pendekatan
4. Pengamanan
5. Koleksi
6. Pemeriksaan
7. Analisis
8. Presentasi
9. Kembali Bukti

4.1.5. Yong-Dal Shin

Mengusulkan model baru untuk prosedur investigasi Cyber Crime adalah sebagai berikut :

1. Tahap Persiapan Investigasi
2. Konsultasi dengan pihak Cyber Crime
3. Klsifikasi Cyber Crime
4. Analisys Cyber crime
5. Pelacakan tersangka
6. Adegan investigasi Cyber Crime
7. Memanggil tersangka
8. Rekontruksi
9. Menulis laporan

Table 4.1 Comparison of activities in the models discussed

Activity in New model	Lee et al	Casey	DRFWS	Reith et al	Yong-Dal shin
Awareness				√	√
Authorisation					
Planning				√	√
Notification					
Search/Identification	√	√	√	√	√
Collection	√	√	√	√	√
Transport					
Storage					
Examination	√	√	√	√	√
Hypothesis	√		√	√	√
Presentation	√		√	√	√
Proof/Defence			√		
Dissemination					

4.2 Analisis Matriks Logical framework approach

Kegiatan yang dilakukan dalam melakukan analisis *Logical framework approach* ini yaitu menyusun matrik logframe sebagai perencanaan seluruh kegiatan evaluasi yang dilakukan. Yang kemudian nantinya matrik logframe akan dirinci kembali menjadi beberapa bagian matrik sehingga didapat alur evaluasi yang terstruktur untuk mencapai tujuan yang telah ditetapkan.

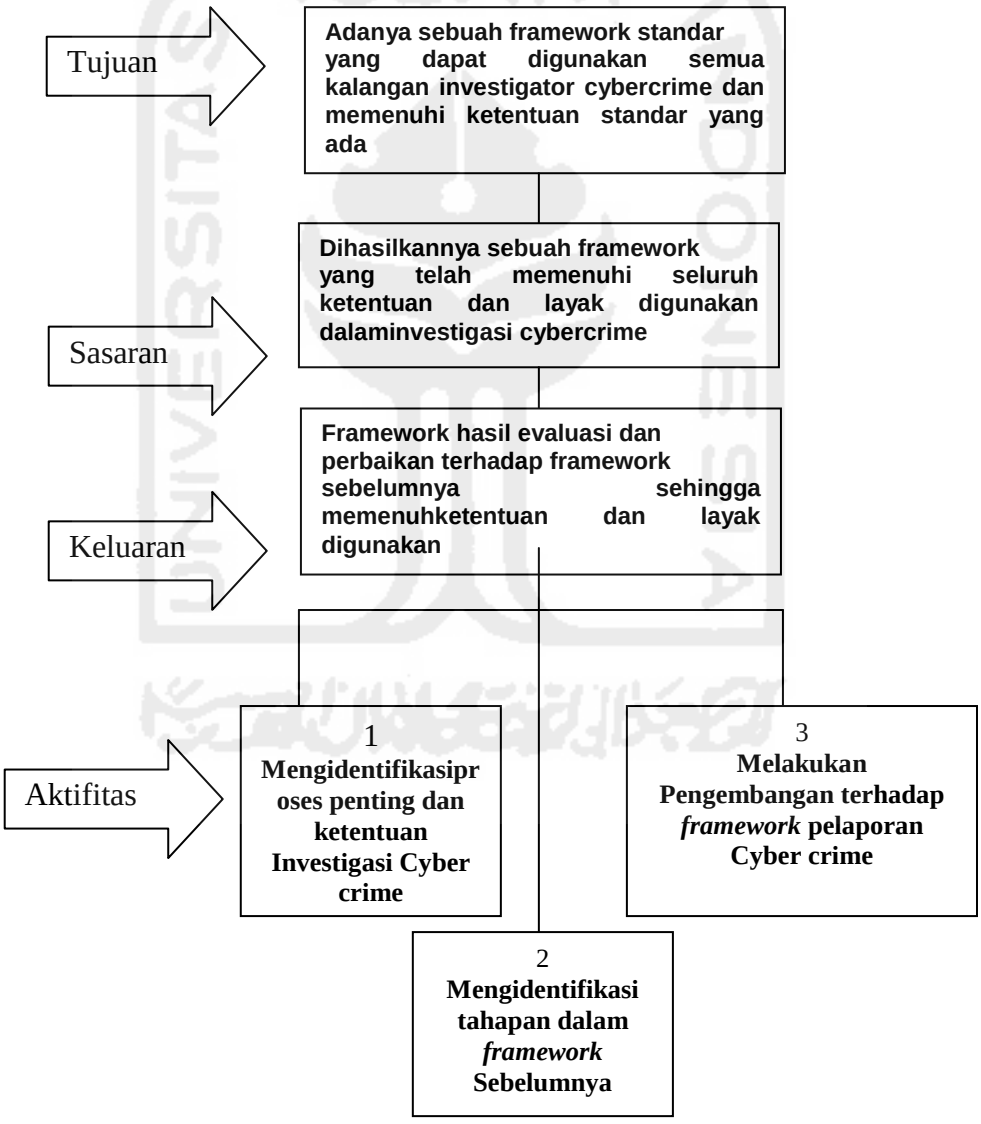
Matrik logframe evaluasi merupakan matrik dari seluruh aktivitas evaluasi yang dilakukan. Matrik ini tersusun dari empat elemen dasar yaitu hubungan antara tujuan *(goals)*, sasaran *(purpose)*, keluaran *(outputs)*, dan kegiatan *(activities)*. Matrik ini juga menjadi landasan kegiatan apa saja yang dilakukan untuk menjalankan evaluasi terhadap *framework* sehingga dapat menghasilkan *framework* yang telah memenuhi seluruh ketentuan dan layak untuk digunakan.

Table 4.2 Analisis Matriks *Logical framework approach*

Deskripsi Kegiatan	**Indikator**	**Verifikasi Indikator**	**Asumsi**
Tujuan Adanya sebuah Pengembangan *framework* dapat digunakan semua kalangan masyarakat yang mengalami kejahatan Cyber crime untuk melaporkan kepada pihak yang berkompeten	*Framework* standar yang dapat digunakan oleh user yang mengalami kejahatan Cyber crime	- Memenuhi seluruh ketentuan dalam standar - Layak untuk digunakan dalam pelaporan cyber crime	Standar yang memang digunakan untuk investigasi Cyber crime

Deskripsi Kegiatan	**Indikator**	**Verifikasi Indikator**	**Asumsi**
Sasaran Dihasilkanny a sebuah pengembanga n *framework* yang telah memenuhi seluruh ketentuan	*Framework* yang telah memenuhi ketentuan	- Memenuhi seluruh ketentuan dalam investigasi Cyber crime - Layak untuk digunakan dalam investigasi Cyber crime	Tidak ada
Keluaran *Framework* hasil evaluasi dan pengembanga n terhadap *framework* sebelumnya sehingga memenuhi ketentuan dan layak digunakan	*Framework* hasil pengembangan dan evaluasi terhadap *framework* sebelumnya	- Memenuhi seluruh ketentuan dalam invetigasi Cybe crime - Layak untuk digunakan dalam investigasi Cyber crime	Tidak ada
Aktivitas 1.Mengidenti fikasi proses penting dan ketentuan	1. Daftar kegiatan proses penting dalam investigasi cybercrime	1. Dokumen *2.Framework* investigasi yang bersumber dari jurnal dan paper 3.Hasil evaluasi terhadap *framework* baru	Semua aktivitas harus dilakukan dan menggunakan teori pendukung sehingga hasil kegiatan tidak subjektif.
2.Mengidenti fikasi tahapan dalam *framework* Sebelumnya	2.Mengidentifik asi tahapan dalam *framework* sebelumnya		
3.Melakukan pengembangan terhadap *framework* Pelaporan Cyber crime	*3.Framework* yang telah diperbaikiuntuk emenuhi ketentuan		

Dari hasil pembuatan rencana evaluasi berdasarkan tabel tersebut, maka dapat digambarkan pohon kegiatan evaluasi berurutan dari pohon yang paling atas merupakan tujuan akhir yang mau dicapai, kemudian sasaran, keluaran, dan terakhir aktivitas yang dilakukan seperti gambar dibawah ini. Dari aktivitas yang dilakukan, maka akan mencapai keluaran yang diharapkan, dari keluaran, akan mencapai sasaran, dan terakhir dari sasaran akan mencapai tujuan akhir. Hal ini merupakan hirarki berpikir dari *Logical framework approach*.



Gambar 4.1 Pohon kegiatan evaluasi yang dilakukan

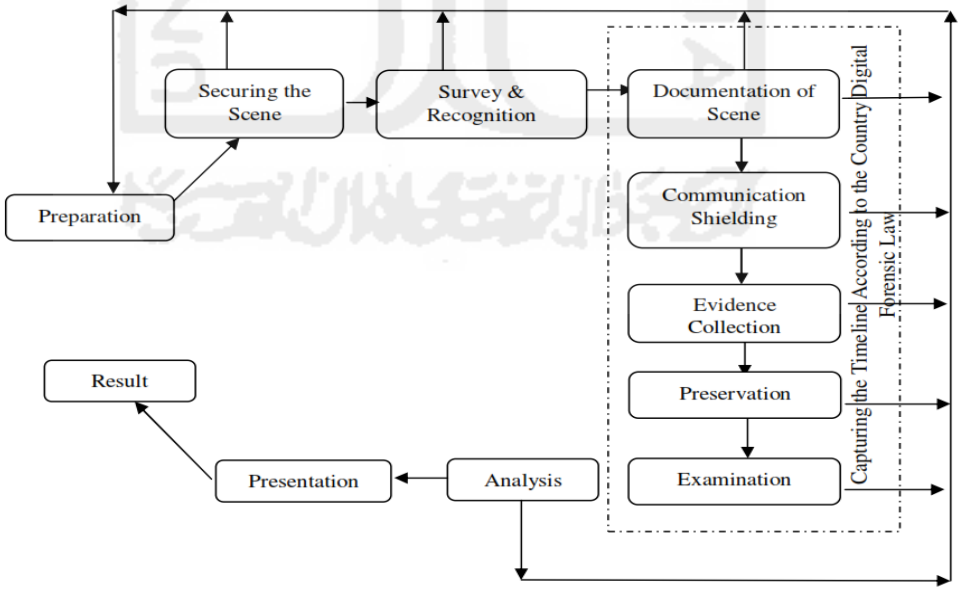
4.3 Analisa Investigasi Cybercrime

Pada tahapan ini, akan dilakukan evaluasi terhadap 4 jenis *framework* yang bersumber dari jurnal dan paper Tentang Investigasi Forensika Digital yang berdekatan dengan Investigasi Cyber crime. dengan hasil identifikasi proses penting yang terdapat dalam. Evaluasi dilakukan dengan membandingkan hasil identifikasi proses penting dalam apakah sudah ada atau belum dalam tahapan *framework* investigasi maupun penjelasan dari tahapan tersebut.

Oleh karena itu dilakukan juga identifikasi terlebih dahulu terhadap tahapan dan penjelasan tahapan tiap *framework* tersebut. Setelah identifikasi terhadap tahapan, dibuat juga tabel matriks logframe terhadap tiap *framework* untuk memetakan *framework* dan mengetahui indikator serta terminologi yang digunakan untuk setiap tahapan *framework*. Sehingga ketika evaluasi dilakukan, istilah terminologi yang digunakan sudah sama.

4.3.1. Systematic Digital Forensic Investigation Model

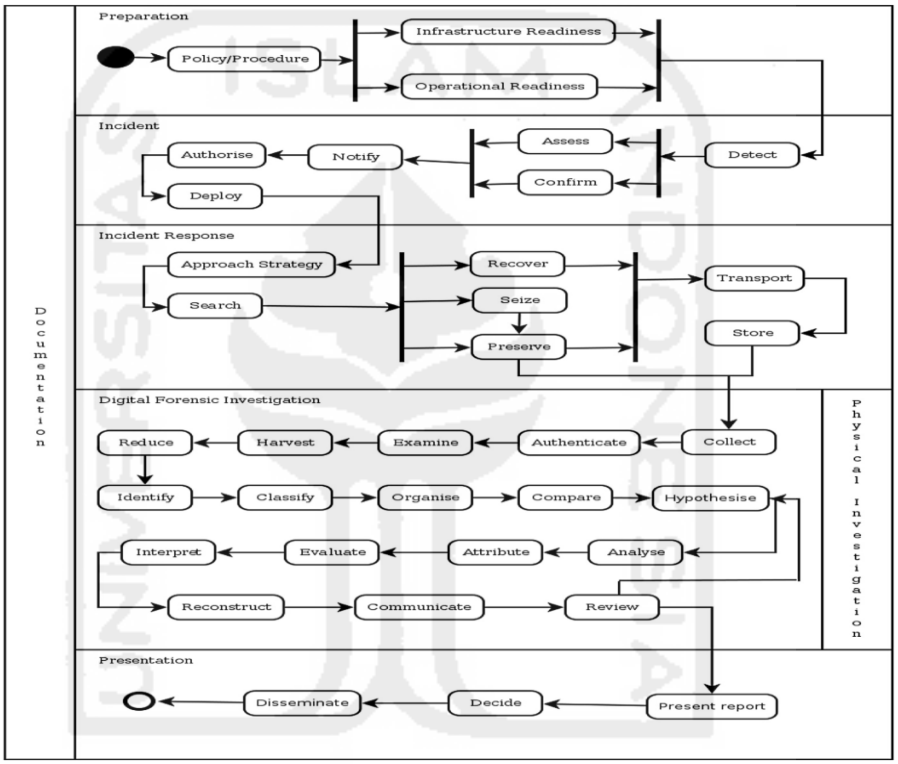
Framework ini dikembangkan oleh (Agarwal et al., 2011) dengan melakukan analisis terhadap 4 jenis *framework* investigasi dan mengembangkannya menjadi sebuah *framework* investigasi yang bersifat sistematis. Ilustrasi *Framework* tersebut dapat dilihat pada



Gambar 4.3.1 Systematic Digital Forensic Investigation Model

4.3.2 Integrated Digital Forensic Process Model

Framework ini diusulkan oleh (Kohn et al., 2013) dengan nama *framework Integrated Digital Forensic Process Model. Framework* ini dibangun dengan menganalisis 6 jenis *framework* dari tahun 2001 sampai 2009 yang kemudian dijadikan landasan untuk mengembangkan sebuah *framework* baru. Ilustrasi *Framework* tersebut dapat dilihat pada Gambar 4.4.2 dibawah ini.

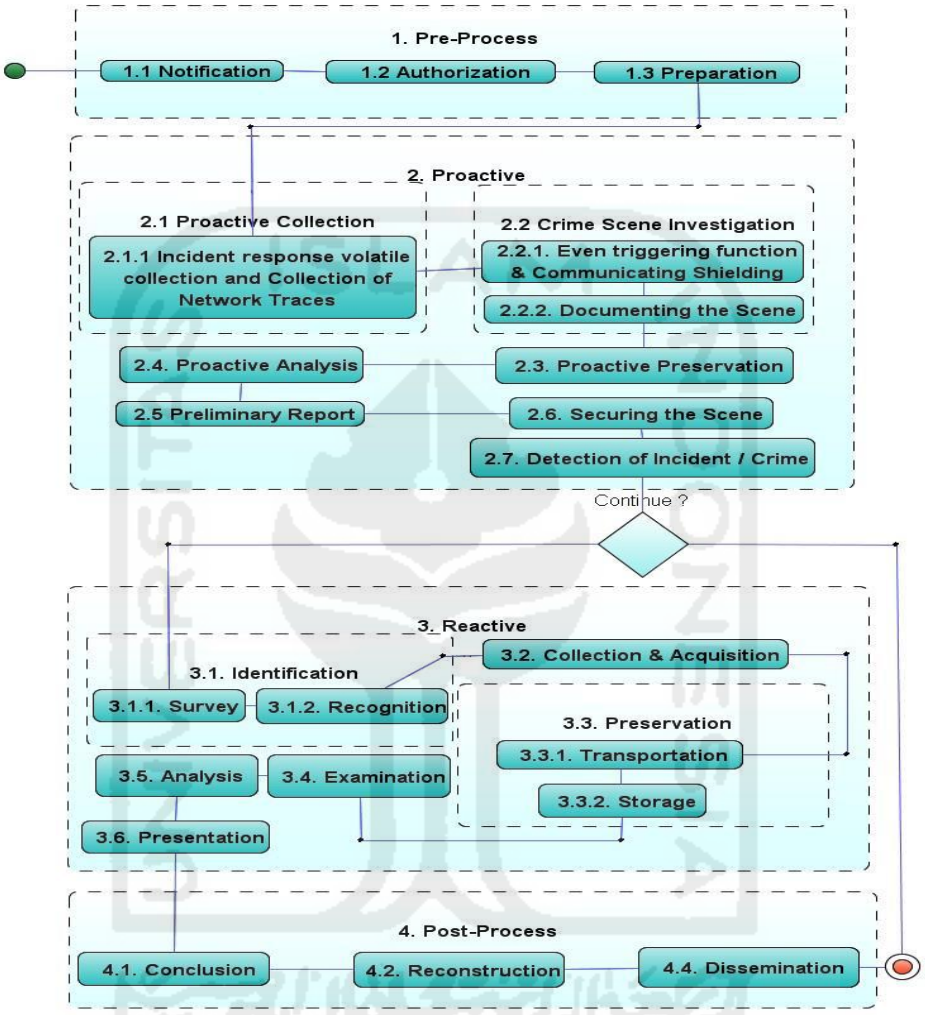


Gambar 4.3.2 Integrated Digital Forensic Process Model

4.3.3 Integrated Digital Forensics Investigation *Framework*s

Framework ini diusulkan oleh (Rahayu & Prayudi, 2014) dengan nama *framework Integrated Digital Forensics Investigaton Frameworks (IDFIF).Framework* ini dibangun dengan menganalisis 6 jenis *framework* sebagai landasan pengembangan sebuah *framework* baru dan mengakomodir keenam *framework* tersebut dengan

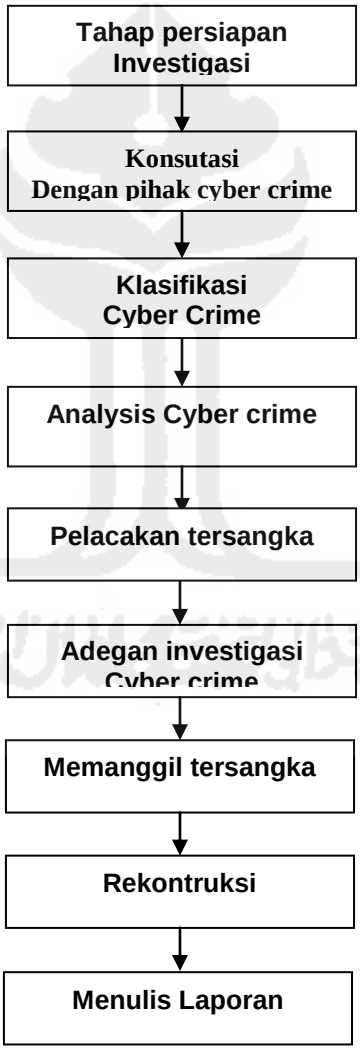
menggunakan metode sequential logic. Ilustrasi *Framework* tersebut dapat dilihat pada Gambar 4.4.3 dibawah ini.



Gambar 4.3.3 Integrated Digital Forensics Investigation *Framework*s

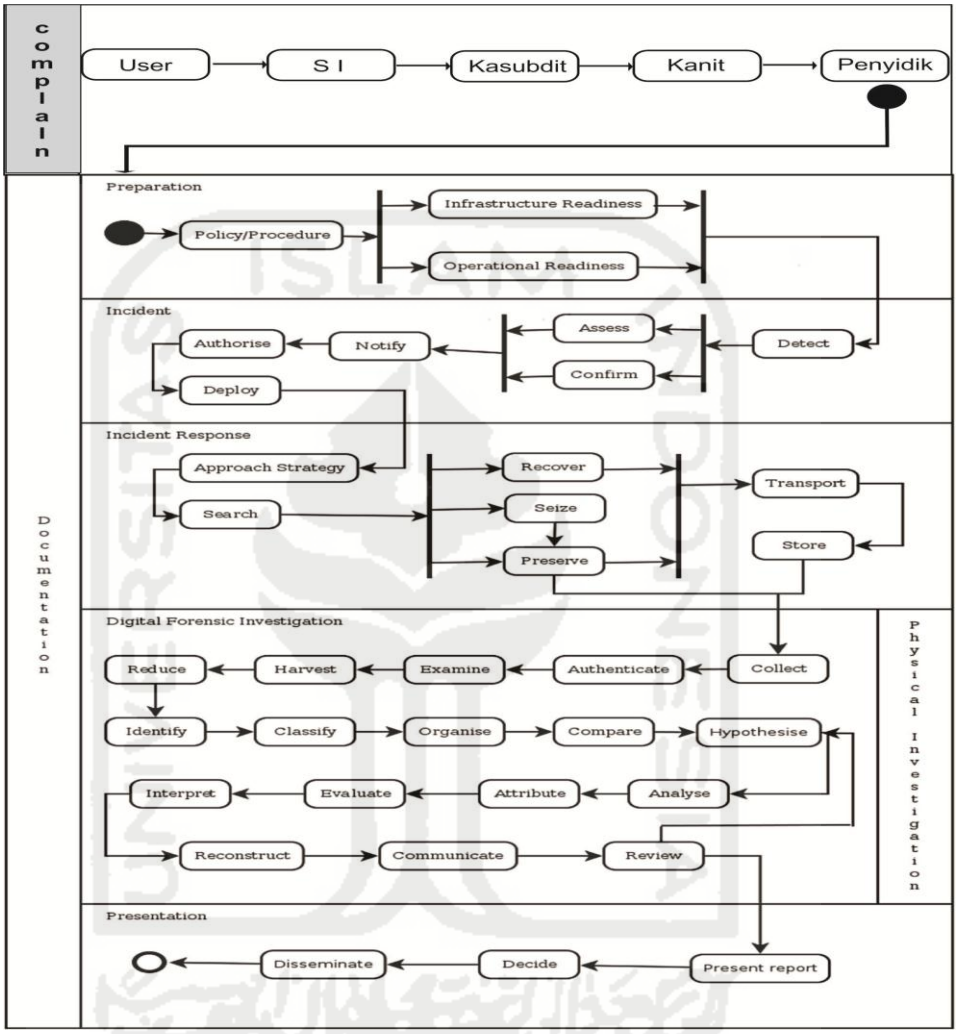
4.3.4 Analisa Framework Investigasi Forensika Digital

Investigasi kejahatan cyber yang di tulis oleh Yong-Dal Shin sebagai berikut: Readines phase, Consulting with crime profiler ,cyber klasifikasi kejahatan dan prioritas keputusan penyelidikan, cyber TKP investigasi, Cyber crime classification and investigation priority decision, damaged(victim) cyber crime scene investigation, analysis by profiler, suspect tracking, injurer cyber crime scene investigation, suspect summon, cyber crime logical recontruction, writing report. Gambar dibawah adalah SOP (Standar Operasinal Procedure) Pelaporan Cyber crime yang diusulkan. Untuk informasi lebih lanjut mengenai prosedur penyelidikan adalah sebagai berikut :



Gambar 4.3.4 Framework New Model Investigasi Forensika Digital

Dari ke empat tahapan tentang Investigasi Forensika Digital dan tentang Investigasi Cyber crime, maka disini penulis akan menambahkan tahapan untuk pelaporan/ complain kepada pihak yang berkompeten.



Gambar 4.4.5 Pengembangan Framework Investigasi cyber crime

Keterangan :

: Tahapan

: Tahapan Asli

4.4 Implementasi Pengembangan Framework Pelaporan Cyber crime

Skenario implementasi Framework pelaporan cybercrime dengan menggunakan sistem informasi berbasis web terdiri dari Pelapor korban dari cybercrime sebagai user dan Admin sebagai penerima dan membalas laporan, melihat data pelapor, menampilkan data orang yang melapor dalam setiap bulan dan menampilkan data orang yang melapor yaitu dari pihak kepolisian.

4.4.1. Tampilan Sistem Informasi Cyber crime Report

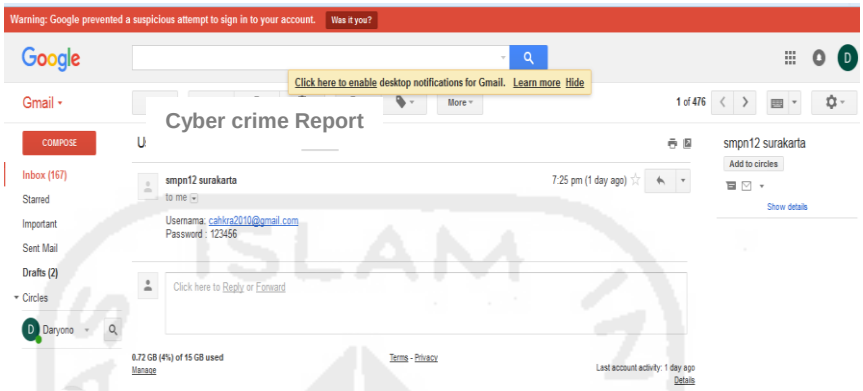
Pelapor menuliskan alamat situs www.cyber-crimereport.cf, dan tampil halaman depan seperti gambar dibawah ini:

4.4.1.1 Registrasi User Pelapor

Gambar 4.4.1 Tampilan Register User Pelapor

Setelah tampil halaman situs halaman paling depan, pilih ke menu registration untuk register menjadi member seperti tampilan gambar dibawah didepan.

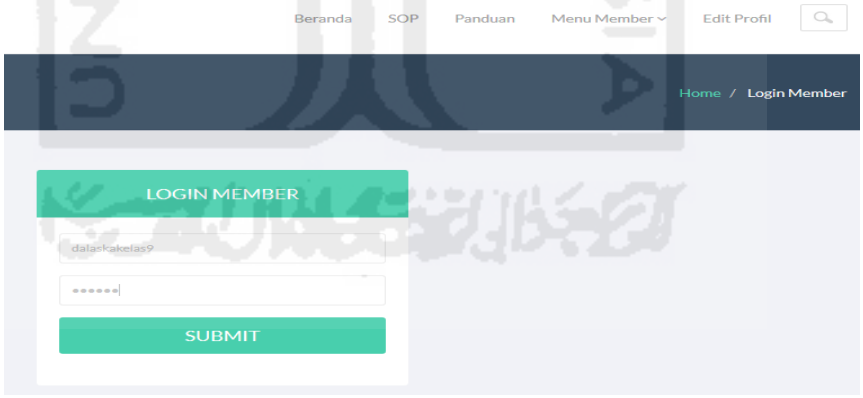
4.4.1.2. Mendapatkan Username dan Password melalui Email



Gambar 4.4.2 Tampilan Register User Pelapor

Setelah berhasil register tahap selanjutnya akan mendapatkan username dan password dari system yang akan dikirim ke alamat email user saat mendaftar seperti gambar diatas.

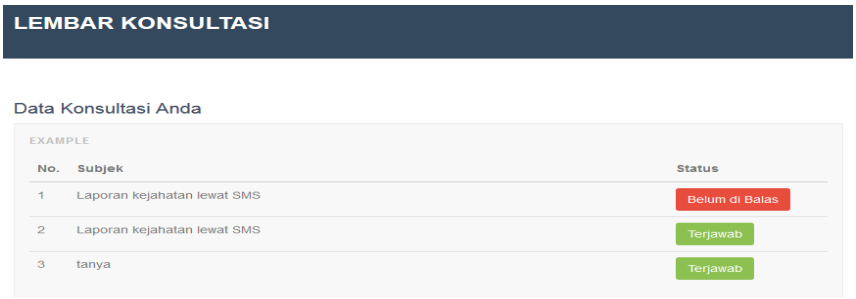
4.4.1.3. Berhasil melakukan registrasi user login menjadi member



Gambar 4..4.1.3 Login menjadi member

Tahap selanjutnya klik menu registration ke sub menu login untuk melapor kesistem seperti gambar diatas.

4.4.1.4. Lembar konsultasi yaitu user melakukan Lapor pada sistem informasi kepada Kepolisian



Gambar 4..4.1.4 Lembar Konsultasi pelapor ke Polisi/ Administrator

Setelah berhasil login ke sistem tahap selanjutnya yaitu ketahap untuk lapor ke polisian lewat sistem dengan mengisikan Subjek kejadian dan Isi Pelaporan dan disertai dengan file barang bukti setelah itu klik kirim tampilanseperti gambar diatas.

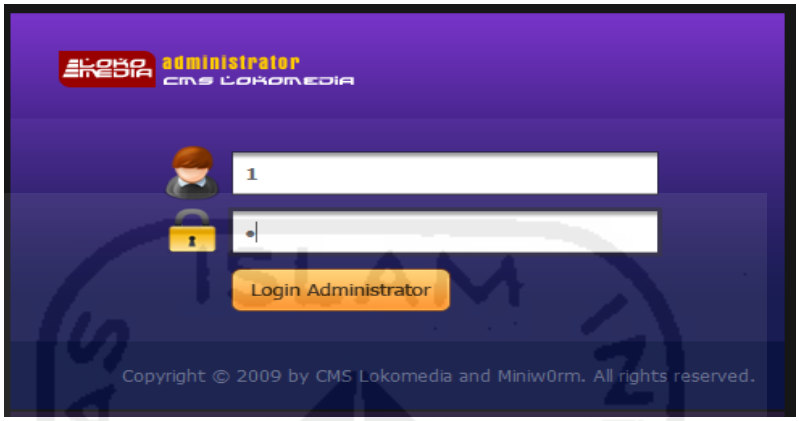
4.4.1.5 Balasan dari Administrator Kepolisian kepada User pelapor

Gambar 4..4.1.5 Lembar Balasan dari Administrator/ polisi Ke Pelapor

Setelah laporan berhasil dikirim akan masuk masuk ke system administrator bagian Umum yaitu kepolisian dan akan mendapatkan balasan seperti pada gambar didepan.

4.4.1.6. Tampilan Sistem Informasi Administrator Kepolisian ada tiga Administrator yaitu pertama BANUM, kedua KASUBDIT/KANIT dan PENYIDIK

BANUM melakukan login pada Sistem



Gambar 4..4.1.6 Login menjadi member Administrator/ Polisi Sebagai BANUM

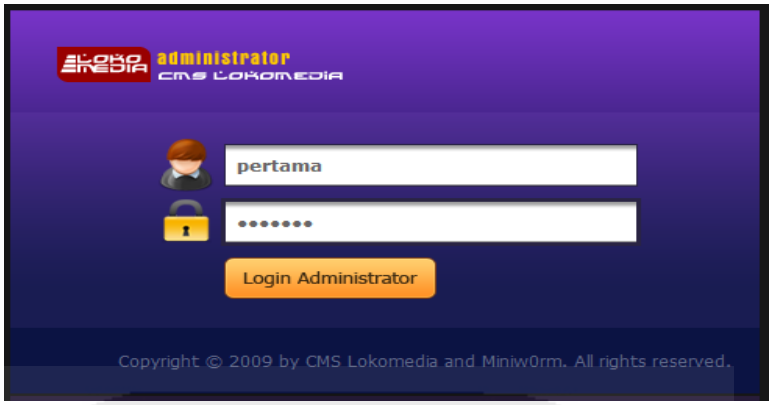
Tampilan gambar diatas adalah login Administrator Bagian umum/BANUM untuk melihat laporan dari User.

4.4.1.7. Melihat data pelapor yang masuk, yang berhak lihat data pelapor dan melakukan Disposisi Ke KASUBDIT / KANIT

Gambar 4.4.1.7 Administrator/ Polisi BANUM Melihat data Pelapor

Administrator BANUM melihat laporan yang terdiri dari menu Laporan masuk, Disposisi dan Data pelapor seperti gambar di atas.

4.4.1.8. KASUBDIT melakukan login pada Sistem



Gambar 4..4.1.8 Login menjadi member Administrator/ Polisi Sebagai KASUBDIT

Setelah laporan dari User diterima oleh Administrator bagian umum tahap selanjutnya yaitu BANUM akan melakukan Disposisi yang laporan akan diteruskan ke Bagian Adminstrator Bagian KASUBDIT, dan gambar diatas adalah login Administrator KASUBDIT untuk melihat data Laporan dari BANUM.

4.4.1.9. Melihat data pelapor yang masuk, yang berhak lihat data pelapor, Membalas ke USER Pelapor melakukan Disposisi Ke PENYIDIK

Gambar 4.4.1.9 Administrator/ Polisi KASUBDIT Melihat data Pelapor

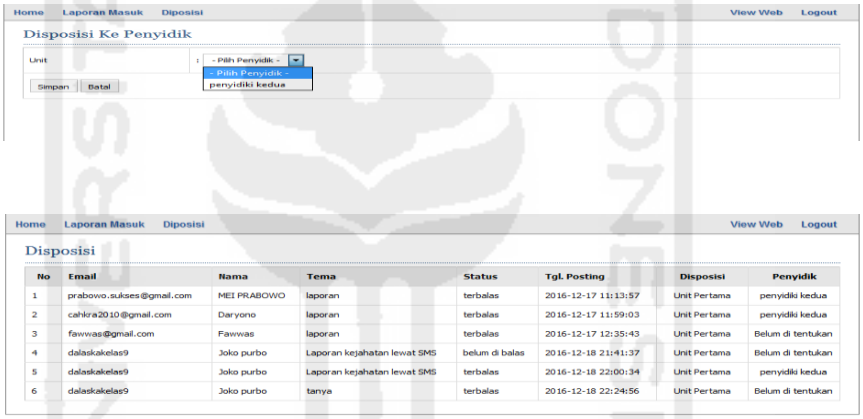
LEMBAR - DISPOSISI

Dari	: Kasubdit	Tanggal Terima	: 19 Januari 2017
Nomor Surat	: 0005	Klasifikasi	: Penipuan lewat SMS
Tanggal Surat	: 14 Januari 2017	Nomor Agenda	: 0005
Jam Terima	: 08:57:07		
Perihal	: Kejahatan cyber		

Kepada Yth.	Isi Disposisi
Unit Pertama	

Gambar diatas adalah surat disposisi dari Kasubdit ke penyidik

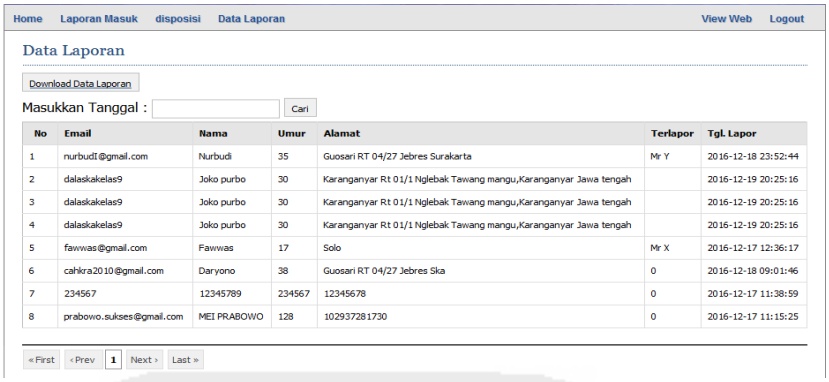
Setelah Administrator KASUBDIT berhasil login, tahap selanjutnya yaitu melihat laporan dari disposisi BANUM yang terdiri dari menu Laporan masuk yang berisi Nama email, Nama pelapor, Tema, Status, Tanggal posting dan aksi seperti gambar diatas.



Gambar 4.4.1.9 Administrator/ Polisi KASUBDIT Disposisi ke penyidik

Gambar di depan adalah tampilan menu disposisi yang akan ditujukan ke penyidik untuk melakukan Investigasi atas laporan yang diminta oleh user.

4.4.1.10. KASUBDIT juga bisa untuk melihat data serta mengunduh Data pelapor pada Sistem



Gambar 4.4.1.10 Gambar Administrator/ Polisi KASUBDIT melihat data Pelapor

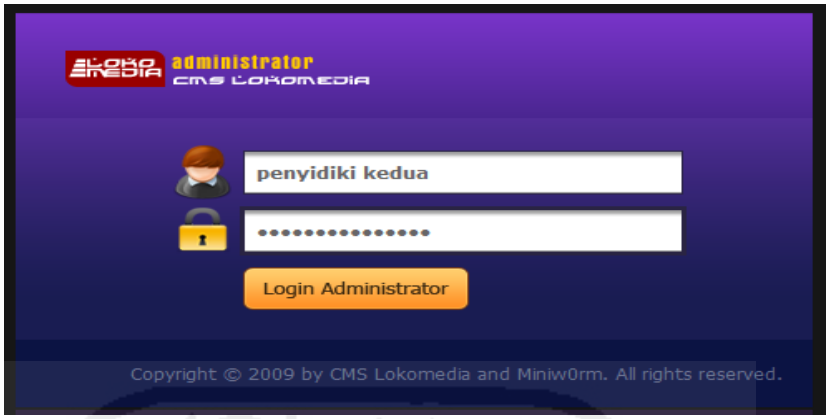
Tampilan diatas adalah menu dari Kasubdit yang berisi menu laporan data dari User, Menu disposisi apakah sudah dilakukan disposisi atau belum, Serta menu untuk download data yang sudah masuk.

4.4.1.11. Melihat data pelapor yang masuk, yang berhak lihat data pelapor, Membalas ke USER Pelapor melakukan Disposisi Ke PENYIDIK

Gambar 4.4.1.11 Gambar Administrator/ Polisi Login KANIT melihat data pelapor

Tampilan gambar didepan adalah Administrator Kanit, sebagai pegganti Kasubdit apabila Kasubdit berhalangan hadir, dan dapat menerima dan melakukan disposisi laporan yang masuk dari user.

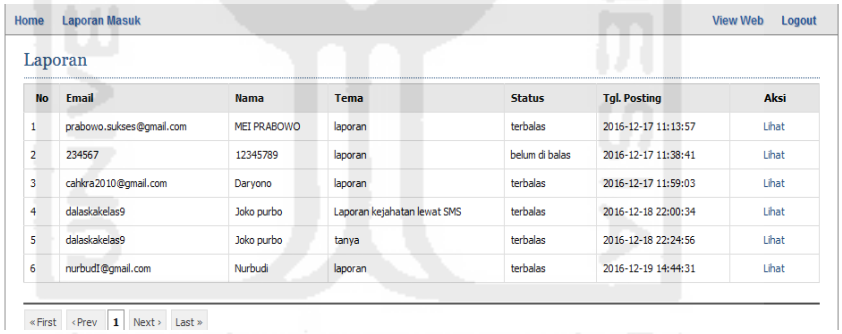
4.4.1.12. PENYIDIK melakukan login pada Sistem



Gambar 4.4.1.12 Administrator/ Polisi Login Sebagai PENYIDIK

Tampilan gambar diatas adalah login Administrator penyidik untuk melihat laporan data masuk yang telah diterima Kasubdit/ Kanit laporan dari User.

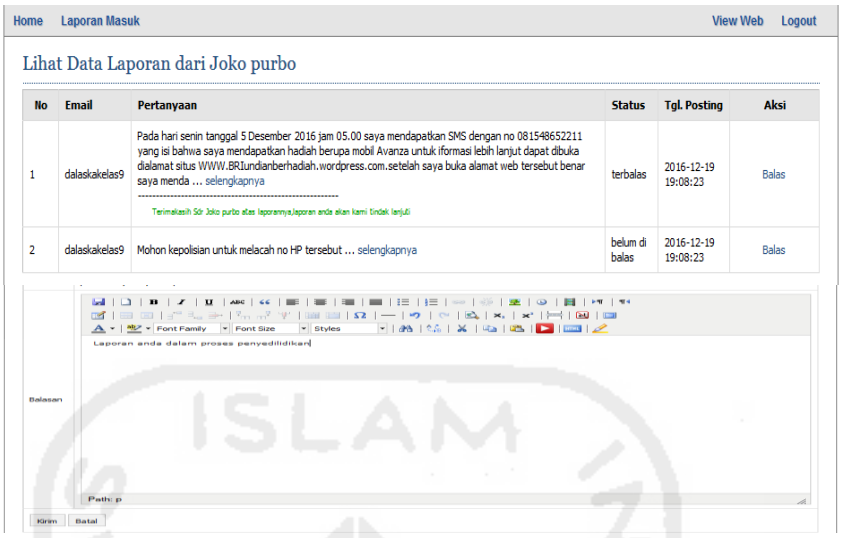
4.4.1.13. Melihat data pelapor yang masuk, yang berhak lihat data pelapor, Membalas ke USER Pelapor melakukan Disposisi Ke PENYIDIK



Gambar 4.4.1.13 Administrator/ Polisi PENYIDIK Melihat data Laporan

Tampilan gambar di depan adalah menu Laporan masuk yang diterima oleh penyidik untuk melakukan proses Investigasi yang diterima dari disposisi Kasubdit yang berisi data pelapor dan Isi laporan serta bukti screenshot.

4.4.1.14. Membalas kepada USER tentang kasus yang ditangani oleh PENYIDIK



Gambar 4.4.1.14 Administrator/ Polisi PENYIDIK membalas laporan

Tampilan gambar diatas adalah proses penyidik melakukan balasan kepada kasubdit tentang hasil proses Investigasi yang telah dilakukan oleh penyidik.

3

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Kesimpulan yang dapat simpulkan dari penelitian yang telah dilakukan adalah :

1. Dengan adanya Perancangan sebuah pengembangan Framework dapat menghasilkan sebuah Sistem Informasi pelaporan Cyber crime.
2. Setelah melakukan wawancara dengan pihak kepolisian khususnya yang menangani Cyber crime, untuk model pelaporan dari masyarakat yang menjadi korban Cyber crime masih menggunakan model konvensional. maka disini penulis memberikan kontribusi membuat Framework pelaporan cybercrime berbasis web guna membantu masyarakat untuk lebih cepat dan mudah dalam pelaporan kepada pihak yang berkompeten khususnya yang menangani Cyber crime dan pihak kepolisian untuk memberikan layanan kepada publik lebih cepat.

5.2 Saran

Saran yang mungkin berguna bagi penelitian selanjutnya, antara lain:

Mengembangkan model Framework yang lain seperti Proses Investigasi Cybercrime dan Framework berbasis Sistem Informasi pelaporan kepada pihak yang berkompeten.

DAFTAR PUSTAKA

Akhmad Sobirin.*Upaya Polda Daerah Istimewa Yogyakarta dalam mengungkap kejahatan penipuan Online, Skripsi*,Tahun 2012,Yogyakarta.

Andika Agus Slameto.2013.*Penerapan zachman framework dalam merancang system pelaporan kerusakan Komputer*,Seminar Nasional Teknologi Informasi dan Multimedia, Tahun 2013,Yogyakarta.

Budi Siswanto.2012.*Sistem Aplikasi Pencatatan Tindak Kejahatan pada polsek tegal selatan berbasis web*,Transient Vol 1 No 3 Semarang.

Cahyana.2008.*Perluya Cyberlaw dalam menghadapi dan menanggulangi kejahatan Dunia Maya*,Buletin hukum perbankan dan Kebanksentralan,Vol 6 Nomor 1.

David Wall.*Crime and Internet*.2001.London and Newyork,Routledge.
Dheny wahyudi.*Perlindungan Hukum Terhadap Korban Kejahatan Cybercrime di Indonesia*, Jurnal ,Jambi.

Dyah Ayu Mustikowati.*Pembangunan Sistem Informasi Pendataan Rumah Tangga Miskin Kecamatan Tulakan Kabupaten Pacitan*,Journal Speed,Vol 5 No.3 Tahun 2013.Pacitan.

Fajar Masya.2012 *Sistem Pelayanan Pengaduan Masyarakat pada Divisi* Humas Polri Berbasis Web.SNATI 15-16 Juni 2012.Jakarta.

Hari Murti,*Cybercrime*.2005Jurnal Teknologi Informasi dan Komunikasi Vol X ,Semarang.
I Made Dharmawan Setiadi.*Sistem Informasi Geografis Pemetaan Tingkat Pertumbuhan Penduduk Berbasis Web*.Merpati Vol.3 No.3 Desember 2015.Bali.

Jane Kernan and Heather J.Ruskin.*Cybercrime and Privacy Issues*.2012.Ercim News.
Masya, F., Simanjuntak, F. M., Informasi, S., Ilmu, F., Universitas, K., Buana, M., … Publik, I. (2012). *Sistem Pelayanan Pengaduan Masyarakat Pada Divisi Humas* (Vol. 2012).

M.Zainal Abidin. *Perancangan Sistem Informasi Layanan Pelanggan PLN Berbasis Website pada PLN Rayon Ampera*, Jurnal,palembang.
Michael Barama.2011,Elektronik Sebagai Alat Bukti Dalam Cybercrime,Karya ilmiah,Manado.

Mohammad Yazdi.2012.*Implementasi Web-Service Pada Sistem Pelayanan Perijinan Terpadu satu Atap di Pemerintahan Kota Palu*.Semantik,Palu Sulawesi tengah.
Pengaduan, A., Untuk, M., Pegawai, I., Pelaporan, P., & Web, B. (2013). *INTERNAL PEGAWAI PUSAT PELAPORAN DAN ANALISIS TRANSAKSI KEUANGAN (PPATK) BERBASIS WEB, 7(08).*

Putu Agus Eka Wilantara. *Pengembangan Sistem SMS Pengaduan Menggunakan SMS gateway untuk meningkatkan Kinerja PNPM Mandiri Perdesaan Kabupaten Buleleng Berbasis Web*.Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika.Volume 3,Juli 2014.Bali.

Radiant Victor Imbar. Perancangan Sistem Informasi pelayanan Medis Rawat Jalan Poliklinik Kebidanan dan Kandungan pada RSUD kota Batam,Jurnal Sistem Informasi,Vol 7,No.1,Maret 2012.Bandung.

Rahayu, Y. D. (2014). *Konsep Integrated Digital Forensics Investigation Framework(IDFIF) Sebagai Standar Perbandingan Framework Investigasi.* Sleman, Yogyakarta: Universitas Islam Indonesia.

Rahayu, Y. D., & Prayudi, Y. (2014). Membangun Integrated Digital Forensics Investigation Framework(IDFIF) Menggunakan Metode Sequential Logic. *Seminar Nasional Teknologi Informasi dan Komunikasi(Sentika).*

Roy Rendra Wijaya.*Perancangan dan Pengembangan Sistem Pelaporan Terpadu Sistem Informasi Puskesmas (SPT SIMPUS)dengan Metode BPR*,Jurnal Ilmiah Kursor,Vol 5 No 2,Juli 2009,Madura.

Seamus O Ciardhuain. An Extended Model of Cybercrime Investigations, Internationa Journal of Digital Evidence,2004.

Shalahudin A.P.Djafar.*Perancangan Sistem Informasi Admisi Program PascaSarjana Universitas Sam Ratulangi*.E-Journal Teknik Informatika,Volume 4,No.2 Tahun 2014,Manado.

Suci Sitoresmi.*Efektifitas Sistem Informasi Layanan Aspirasi dan Pengaduan Online Rakyat (LAPOR!)Pada Unit Kerja Presiden bidang Pengawasan dan Pengendalian Pembangunan (UKP4)*.Skripsi.2013.Depok.

Tiur gantini,Peter Iman Paskal Mendrofa.Pembuatan Perangkat Lunak Pengelolaan data Kasus Perkara di Kepolisian Resor Kota bandung Barat. Jurnal Informatika Vol 6 No 1 Juni 2010.

Vindy Agus Setiawan.2011,Naskah *Publikasi, Analisis dan Perancangan Sistem Informasi Simpan Pinjam pada LKM Gerembeng Bali,*Yogyakarta.

Yong-Dal shin.2011, *New Model for Cyber Crime Investigation Procedure.Dept*.Of IT & Cyber Police,Youngdong University,Rep.of Korea.

Yudi Prayudi.2007.*Antisipasi Cybercrime Menggunakan Teknik KomputerForensik*,SNATI,Yoyakarta.

Yudie Irawan.2011.*Perancangan Sistem Informasi Perpustakaan Berbasis Web Application*,Tesis ,Semarang.

Lampiran

Pengembangan Framework Pelaporan Cyber crime dengan Sistem Informasi Berbasis Web dengan menggunakan Motode Zahman Framework.

Tabel .Matriks Zahman Sistem Pelaporan Cybercrime

Abstraksi/ Perspektif	DATA WHAT (Things)	FUNCTION How (Process)	NETWORK Where (Location)	PEOPLE Who (people)	TIME When (Time)	MOTIVATION Why (Motivation)
Planer/Contextuak (Scope)	Data pelaporan kepolisian,SDM	Proses pelaporan cybercrime dikepolisian	Polda yogyakarta bag Cybercrime	Korban cybercrime, Kepolisian	Input laporan cybecrime,lihat laporan ,balas laporan	Visi dan misi kepolisian
Owner/Conceptual (Bussines Model)	Flowmap dan Use case system	Physical data flow activity diagram	Desain alur system pelaporan cybercrime	Programer, desiner,administrator dan operator	Time schedule pembangunan proyek siste informasi	Alasan pengadaan system informasi

A. Perspektif Planner

Baris pertama pada Zachman Framework ini sering disebut dengan arsitektur kontekstual. Pada arsitektur ini didefinisikan model bisnis fungsional secara global dan berbagai requirement external organisasi.

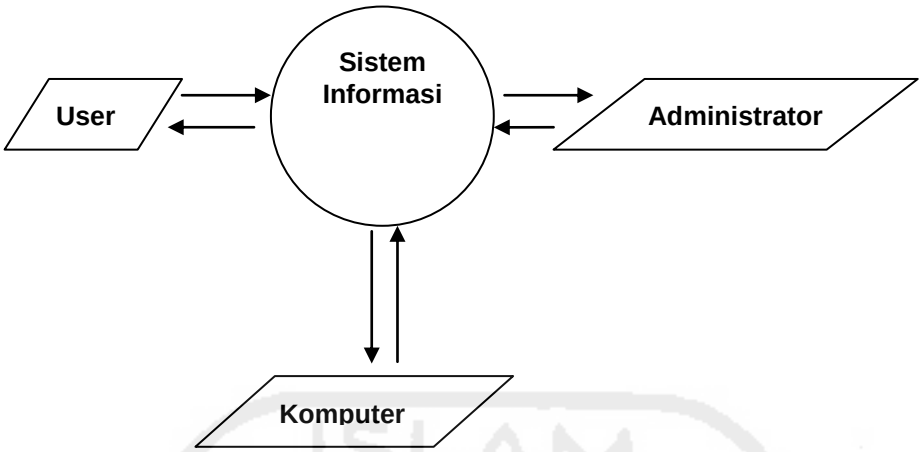
Mendeskripsikan visi, misi, kontek, batas, dan arsitektur sistem. Sering disebut sebagai black box, karena kita dapat melihat input dan output, namun tidak dapat melihat detail pekerjaannya. Baris ini sering disebut baris konteks.

1. What

Ini menerangkan tentang data-data atau entitas yang berkaitan dengan Sistem informasi pelaporan Cyber crime di Polda Yogyakarta. Dari hasil analisis, data-data tersebut dikelompokkan menjadi 2 bagian, yaitu :

a. Data Sumber Daya Manusia, yaitu merupakan data-data pemakai yang menggunakan System informasi ini (User,Yaitu orang yang mengalami korban kejahatan digital dan Administrator,Yaitu pihak kepolisian yang menerima laporan dari User).

b. Data komputer, yaitu data tentang komputer yang digunakan sebagai obyek penelitian.



2. How

Ini membahas tentang proses-proses yang terjadi pada Pelaporan Sistem Informasi di Polda Yogyakarta.

Proses utama yang terjadi adalah proses pelaporan dan penerimaan pelaporan kejahatan Digital.

a. Prosedur pelaporan Cyber crime

1) Register menjadi Member

2) Mengisi form pelaporan yang telah disediakan oleh sistem.

b. Prosedur Penerimaan Laporan Cyber crime dari User

1) Register menjadi member Administrator

2) Login menjadi member Administrator

3) Administrator bagian umum melihat data laporan dari User

4) Administrator bagian umum mendisposisikan ke Kasubdit yang menangani Cybercrime

5) Administrator Subdit unit Cybercrime menerima disposisi dari Bagian umum dan laporan akan diteruskan ke penyidik untuk dilakukan Investigasi lebih lanjut dan setelah itu menjawab laporan dari User.

3. Where

Kolom ini membahas tentang pola bisnis utama yaitu dimana pelaporan cybercrime dari Masyarakat atau User Kepada Polda Yogyakarta khususnya Kasubdit yang menangani Cybercrime.

4. Who

Kolom ini membahas tentang Sumber daya manusia yang berperan penting dalam proses pelaporan dan penanganan Cybercrime Di Polda Yogyakarta. Berikut ini adalah orang-orang yang berperan penting dalam proses tersebut :

a. Bagian Umum (Administrator)

b. Unit pertama (Administrator Kasubdit pertama)

c. Unit Kedua (Administrator Kasubdit kedua)

d. Penyidik pertama (Administrator Penyidik pertama)

e. Penyidik kedua (Administrator Penyidik kedua)

5. When

Pada kolom ini dijelaskan tentang kegiatan-kegiatan yang terjadi di Sistem Pelaporan Polda Yogyakarta khususnya Kasubdit Cybercrime. Untuk kegiatan utama yang akan dibahas adalah yang berkaitan dengan pelaporan cybercrime

Dari User sebagai pelapor dan Administrator sebagai Penerima Laporan.

Adapun kegiatan-kegiatan User tersebut adalah :

a. Form register member baru
b. Form Laporan kepada pihak kepolisian
c. Menu cara Panduan
d. Menu SOP Pelaporan

Adapun kegiatan-kegiatan Administrator tersebut adalah :

a. Form Pengguna Sistem
b. Data Pelaporan dan Isi Laporan
c. Form Disposisi Laporan
d. Menu balas kepada User

6. Why

Pada kolom ini dijelaskan tentang visi dan misi secara umum pada Polda Yogyakarta.

a. Visi

“Terwujudnya postur polri yang jujur, Disiplin, Komunikatif, cinta kasih dan selalu bersyukur sebagai pelindung , pengayom, dan pelayan masyarakat yang terpercaya dalam memelihara kamtibmas dan menegakkan hokum kepolisian daerah Istimewa Yogyakarta “

b. Misi

1. Memberikan perlindungan, pengayoman dan pelayanan secara mudah, tanggap dan responsive, dan tidak diskriminatif agar masyarakat bebas dari segala bentuk gangguan fisik dan psikis.

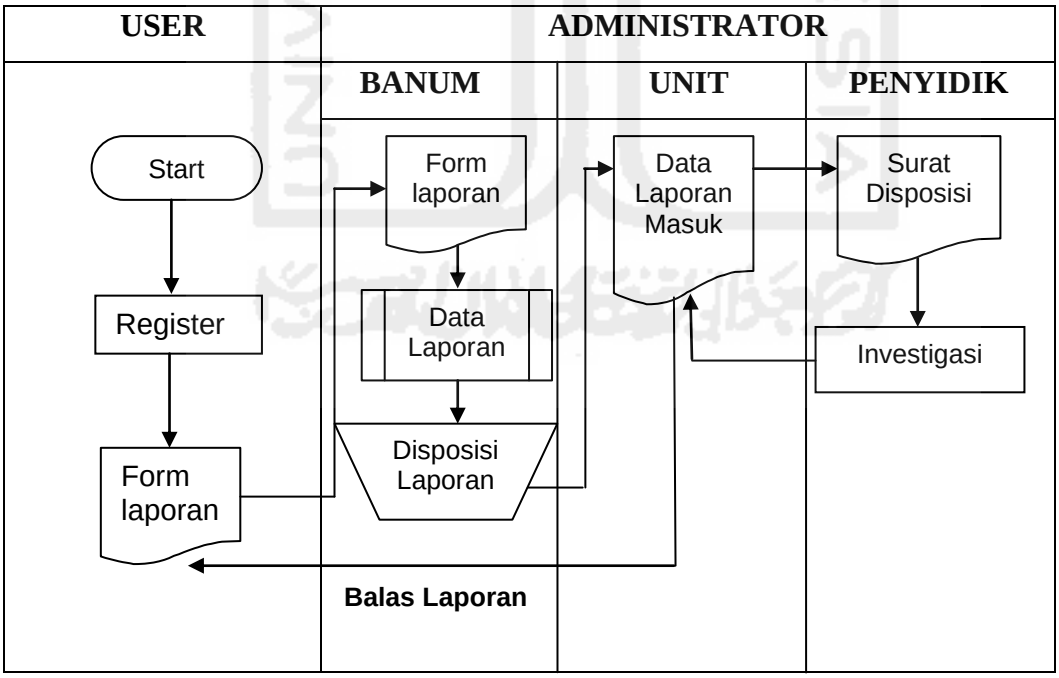
2. Memelihara keamanan dan ketertiban masyarakat sepanjang waktu di seluruh wilayah hukum Kepolisian Daerah Istimewa Yogyakarta, Serta memfasilitasi keikutsertaan masyarakat dalam memelihara kamtibmas dengan mengembangkan Community Policing.

B. Perspektif *Owner*

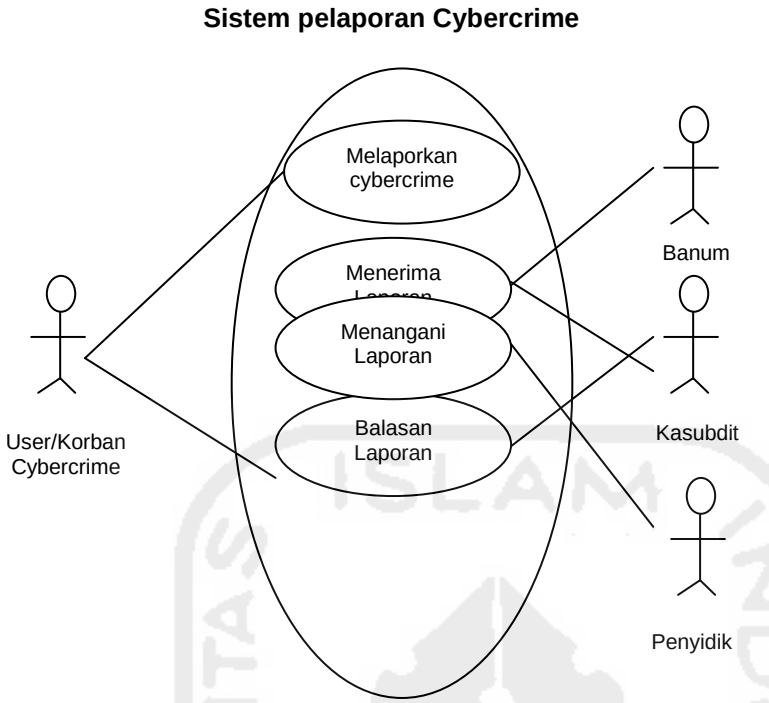
Dalam perspektif ini akan dijabarkan kolom-kolom zachman dari sudut pandang pemilik atau orang yang paling bertanggung jawab terhadap organisasi, dimana dalam penelitian ini yang bertanggung jawab terhadap Pelaporan Cybercrime khususunya di Polda Yogyakarta. Dari sudut pandang ini *owner* akan menyampaikan usulan sebuah sistem dan bagaimana sistem tersebut dapat digunakan dalam gambaran yang masih sederhana. *Owner* hanya melihat bagaimana nanti sistem ini akan berjalan, siapa saja orang-orang yang dibutuhkan untuk membangun sistem dan apa tujuan sistem dibangun.

1. What

Bagian ini menjelaskan bagaimana cara entitas yang sudah ditentukan pada erspektif *Planner* berhubungan dalam menjalankan proses pada sistem pelaporan kerusakan komputer. Pada gambar 2 menggambarkan bagaimana proses terjadi.



Gambar Flowmap proses laporan cybercrime



Gambar. Use case system

2. How

Kolom ini menjabarkan tentang proses yang terjadi pada diagram yang dibuat pada kolom *what.* Proses-proses tersebut adalah :

Kolom ini menjabarkan tentang proses yang terjadi pada diagram yang dibuat pada kolom *what.* Proses-proses tersebut adalah :

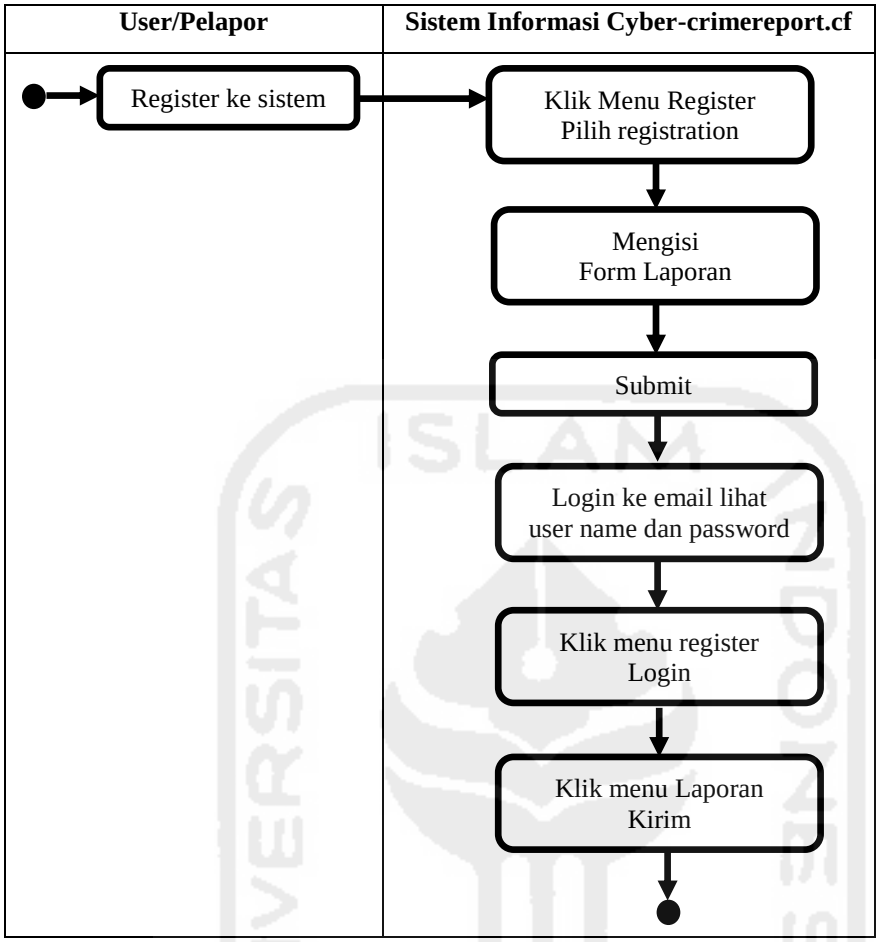
a. User Korban Cybercrime melaporkan pada system Cyber-crimereport.cf.

b. Admin Banum menerima laporan dari User korban cybercrime dan melakukan diposisi kepada Kasubdit kebagian unit.

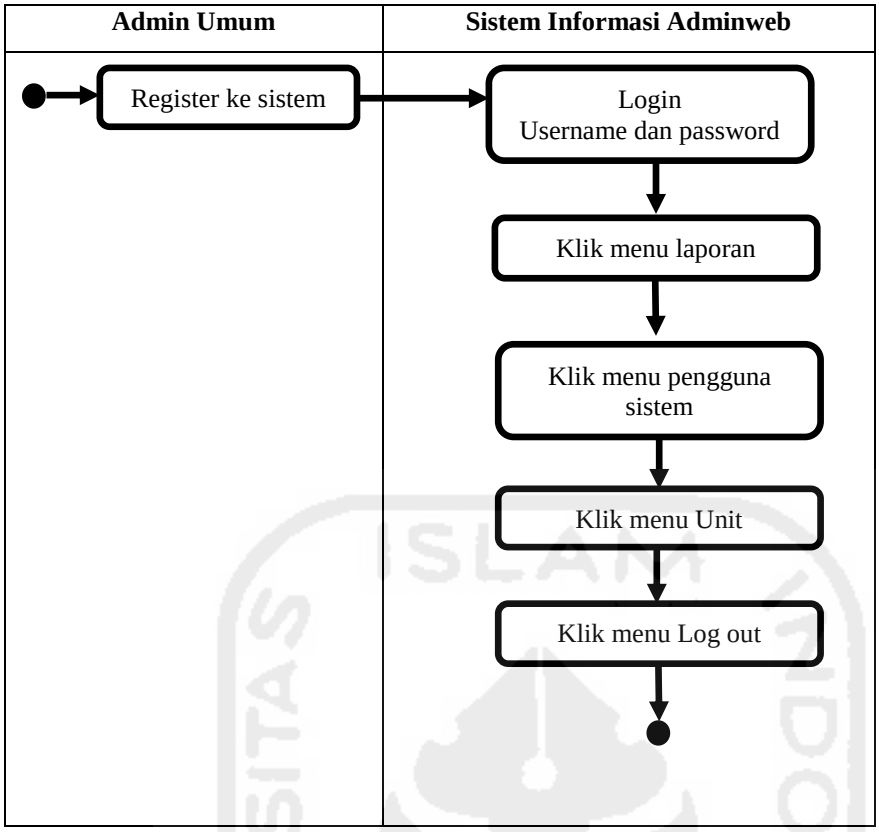
c. Admin Kasubdit menerima laporan disposisi dari Banum dan akan meneruskan disposisi ke bagian penyidik untuk dilakukan proses investigasi, apabila dari laporan dari user korban cybercrime benar terjadi kejahatan kasubdit akan membalas laporan ke User.

d. Admin penyidik bertugas menerima laporan dari Kasubdit (Unit) untuk melakukan proses investigasi cybercrime dari pelapor.

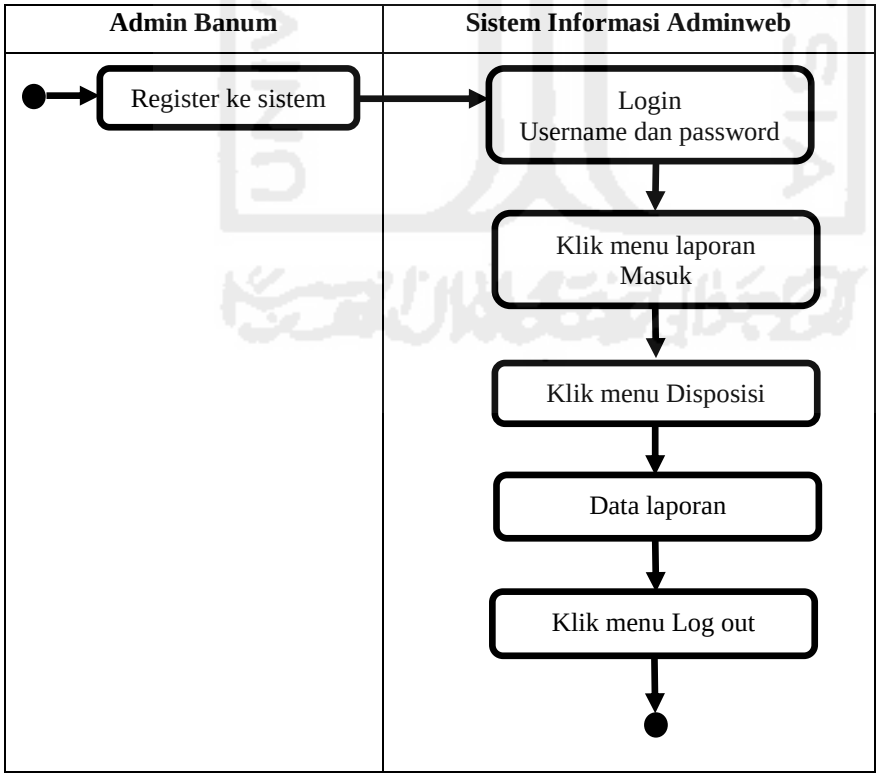
Berikut ini adalah gambaran proses yang terjadi pada sistem informasi pelaporan Cybercrime



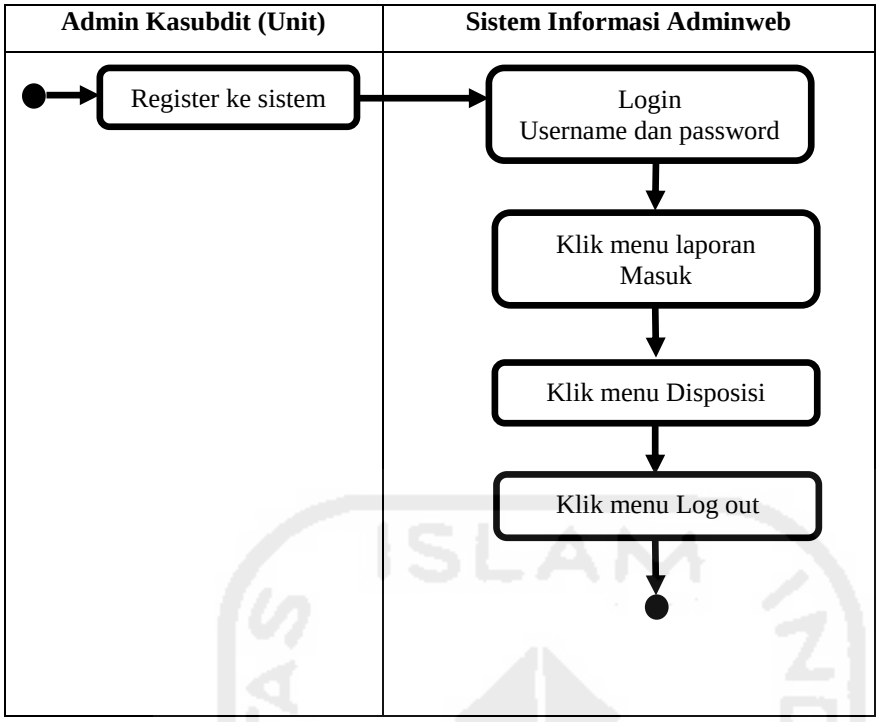
Gambar Activity diagram User/Pelapor



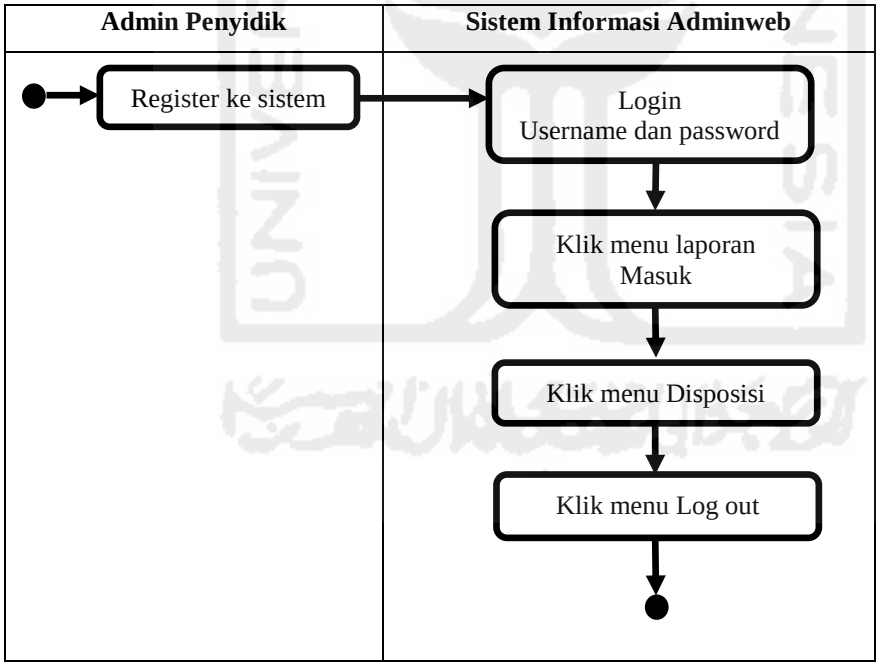
Gambar Activity diagram Admin umum



Gambar Activity diagram Admin Banum



Gambar Activity diagram Admin Kasubdit (Unit)



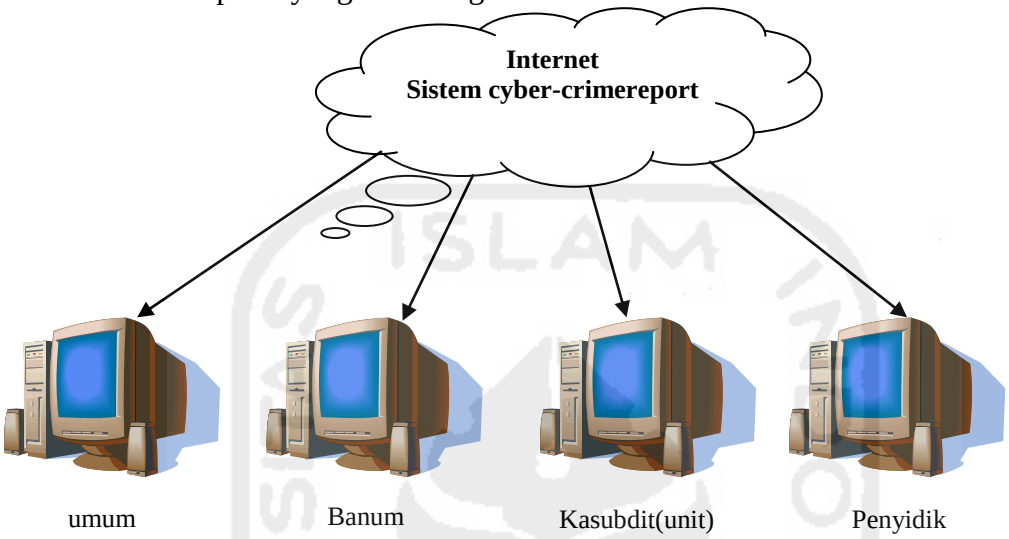
Gambar Activity diagram Admin Penyidik

dari proses diatas sudah dapat dilihat apa yang dilakukanmasing-masing entitas. Oleh karena itu tiap entitas akan diberi batasan-batasan seperlunya dalam menggunakan sistem informasi ini.

3. Where

Bagian ini menjelaskan tentang dimana system informasinya akan ditempatkan. Sistem informasi pelaporan Cybercrime akan ditempatkan didalam jaringan

Internet Kantor bagian cybercrime Polda Yogyakarta sehingga diharapkan dapat diakses dari seluruh komputer yang ada dibagian kantor tersebut.



4. Who

Pada bagian ini menjelaskan siapa saja sumber daya manusia yang akan ditugaskan oleh *owner* untuk pembangunan dan mengelola sistem informasi. Personel tersebut antara :

a. Pengelola komputer

b. Admin operator umum

c. Administrator Banum

d. Administrator Kasubdit (Unit)

e. Penyidik

5. When

Pada bagian ini dijelaskan tentang jadwal atau *time schedule* untuk membangun sistem informasi pelaporan Cybercrime pada Kasubdit Cybercrime Polda Yogyakarta yang akan ditentukan oleh pihak *owner* kemudian akan didelegasikan ke tim yang akan melaksanakan proyek. Tabel 2 dibawah ini adalah *time schedule* yang disusun.

Tabel.Time schedule Rencana Proyek

NO	Rencana kegiatan	Target output	November				Desember			
1	Persiapan proyek	Observasi masalah dan Penetapan jadwal proyek								
2	Fase analisis dan penerapan Framework Kedalam sistem	- Pengambilan data - Menetukan kebutuhan system - Membuat prototype permasalahan dengan metode Zahman dengan penetuan What,How,Where,Who,When,Why dengan penyelesaian masalahnya								
3	Implementasi									

6. Why

Pada kolom ini dijelaskan tentang tujuan yang ingin dicapai oleh bagian Sistem pelaporan Cybercrime yang terkait dengan adanya sistem informasi. Adapun tujuan-tujuannya adalah

a. Ingin merubah yang dari pelaporan konvensinal, dibuat secara digital untuk memudahkan pelapor dan kepolisian secara mudah dan cepat.

b. Ingin membuat manajemen pelaporan yang lebih baik di kepolisian khusunya yang menangani cybercrime.

KUESIONER PENGUJIAN SISTEM CYBER-CRIMEREPORT.CF

Nama : …….
Pekerjaan : …….
Instansi : …….

Berilah Tanda (X) pada jawaban yang sesuai

1. Apakah tampilan dari Sistem Pelaporan Cyber crime yang didesain untuk masyarakat yang mengalami kejahatan cyber Menarik?
   a. Sangat setuju
   b. setuju
   c. Cukup setuju
   d. Tidak setuju
   e. Sangat tidak setuju
2. Apakah Sistem ini memudahkan anda untuk melapor kepihak kepolisian?
   a. Sangat setuju
   b. setuju
   c. Cukup setuju
   d. Tidak setuju
   e. Sangat tidak setuju
3. Apakah Sistem ini dapat menyajikan informasi kejahatan Cyber sesuai dengan kebutuhan?
   a. Sangat setuju
   b. setuju
   c. Cukup setuju
   d. Tidak setuju
   e. Sangat tidak setuju
4. Apakah Sistem ini sudah layak untuk dipakai?
   a. Sangat setuju
   b. Setuju
   c. Cukup setuju
   d. Tidak setuju
   e. Sangat tidak setuju
5. Apakah aplikasi Sistem informasi Pelaporan Cyber crime dapat dijalankan dengan baik?
   a. Sangat setuju
   b. Setuju
   c. Cukup setuju
   d. Tidak setuju
   e. Sangat tidak setuju
6. Apakah aplikasi Sistem informasi pelaporan cybercrime ini mudah untuk digunakan?
   a. Sangat setuju
   b. Setuju
   c. Cukup setuju
   d. Tidak setuju
   e. Sangat tidak setuju
7. Apakah jenis dan ukuran pada Sistem mendukung kenyamanan pengguna Aplikas?
   a. Sangat setuju
   b. Setuju
   c. Cukup setuju

d. Tidak setuju
e. Sangat tidak setuju

8. Apakah intruksi Sistem sederhana dan dapat dimengerti oleh pengguna?
   a. Sangat setuju
   b. Setuju
   c. Cukup setuju
   d. Tidak setuju
   e. Sangat tidak setuju
9. Apakah setiap menu dalam aplikasi dapat berjalan dengan baik dan sesuai fungsinya?
   a. Sangat setuju
   b. Setuju
   c. Cukup setuju
   d. Tidak setuju
   e. Sangat tidak setuju
10. Apakah keseluruhan performa aplikasi berjalan dengan baik?
    a. Sangat setuju
    b. Setuju
    c. Cukup setuju
    d. Tidak setuju
    e. Sangat tidak setuju

HASIL KUESIONER

NO	PERTANYAAN	SS	S	C	TS	STS
1	Apakah tampilan dari Sistem Pelaporan Cyber crime yang didesain untuk masyarakat yang mengalami kejahatan cyber Menarik?	5	11	0	0	0
2	Apakah Sistem ini memudahkan anda untuk melapor kepihak kepolisian?	9	7	0	0	0
3	Apakah Sistem ini dapat menyajikan informasi kejahatan Cyber sesuai dengan kebutuhan?	3	9	4	0	0
4	Apakah Sistem ini sudah layak untuk dipakai?	3	9	4	0	0
5	Apakah aplikasi Sistem informasi Pelaporan Cyber crime dapat dijalankan dengan baik?	4	7	4	0	0
6	Apakah aplikasi Sistem informasi pelaporan cybercrime ini mudah untuk digunakan?	7	5	3	0	0
7	Apakah jenis dan ukuran pada Sistem mendukung kenyamanan pengguna Aplikas?	4	8	4	0	0
8	Apakah intruksi Sistem sederhana dan dapat dimengerti oleh pengguna?	7	8	1	0	0
9	Apakah setiap menu dalam aplikasi dapat berjalan dengan baik dan sesuai fungsinya?	4	9	2	0	0
10	Apakah keseluruhan performa aplikasi berjalan dengan baik?	1	11	3	0	0

Keterangan : Data ini di ambil dari setiap perwakilan sebagai user yaitu mahasiswa di Universitas Slamet riyadi dan Administrator yaitu di Polda Yogyakarta Dari pengolahan data dibawah, Hasil pengujian system cyber-crimereport.cf Layak digunakan.

Correlations

		P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	Total
P1	Pearson Correlation	1	.101	.293	-.056	.319	.570*	.206	.342	.371	.293	.619*
	Sig. (2-tailed)		.710	.271	.836	.229	.021	.445	.195	.157	.271	.011
	N	16	16	16	16	16	16	16	16	16	16	16
P2	Pearson Correlation	.101	1	.345	-.215	.000	.241	.261	-.568*	.157	-.207	.173
	Sig. (2-tailed)	.710		.191	.424	1.000	.368	.328	.022	.561	.442	.522
	N	16	16	16	16	16	16	16	16	16	16	16
P3	Pearson Correlation	.293	.345	1	.115	.109	.078	.422	-.269	.332	.289	.483
	Sig. (2-tailed)	.271	.191		.670	.688	.774	.104	.313	.209	.278	.058
	N	16	16	16	16	16	16	16	16	16	16	16
P4	Pearson Correlation	-.056	-.215	.115	1	.566*	.270	-.365	.280	.372	.577*	.483
	Sig. (2-tailed)	.836	.424	.670		.022	.312	.164	.294	.156	.019	.058
	N	16	16	16	16	16	16	16	16	16	16	16
P5	Pearson Correlation	.319	.000	.109	.566*	1	.572*	-.129	.396	.574*	.490	.750**
	Sig. (2-tailed)	.229	1.000	.688	.022		.021	.634	.129	.020	.054	.001
	N	16	16	16	16	16	16	16	16	16	16	16
P6	Pearson Correlation	.570*	.241	.078	.270	.572*	1	.000	.314	.433	.545*	.746**
	Sig. (2-tailed)	.021	.368	.774	.312	.021		1.000	.236	.094	.029	.001

	N	16	16	16	16	16	16	16	16	16	16	16
P7	Pearson Correlation	.206	.261	.422	-.365	-.129	.000	1	-.170	.370	.211	.313
	Sig. (2-tailed)	.445	.328	.104	.164	.634	1.000		.528	.158	.433	.238
	N	16	16	16	16	16	16	16	16	16	16	16
P8	Pearson Correlation	.342	-.568*	-.269	.280	.396	.314	-.170	1	-.047	.592*	.342
	Sig. (2-tailed)	.195	.022	.313	.294	.129	.236	.528		.862	.016	.195
	N	16	16	16	16	16	16	16	16	16	16	16
P9	Pearson Correlation	.371	.157	.332	.372	.574*	.433	.370	-.047	1	.332	.751**
	Sig. (2-tailed)	.157	.561	.209	.156	.020	.094	.158	.862		.209	.001
	N	16	16	16	16	16	16	16	16	16	16	16
P10	Pearson Correlation	.293	-.207	.289	.577*	.490	.545*	.211	.592*	.332	1	.747**
	Sig. (2-tailed)	.271	.442	.278	.019	.054	.029	.433	.016	.209		.001
	N	16	16	16	16	16	16	16	16	16	16	16
Total	Pearson Correlation	.619*	.173	.483	.483	.750**	.746**	.313	.342	.751**	.747**	1
	Sig. (2-tailed)	**.011**	**.522**	.058	.058	**.001**	**.001**	.238	.195	**.001**	**.001**	
	N	16	16	16	16	16	16	16	16	16	16	16

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

UJIVALIDITAS

Dengan α = 5% = 0,05
Soal yang valid nomor 1, 5,6,9, 10 (warna hitam tebal) karena p < 0,05

UJI RELIABILITAS

Reliability Statistics

Cronbach's Alpha	N of Items
.748	10

Instrumen dikatakan reliabel karena nilai alpha cronbach = 0,748 > 0,6

Case Processing Summary

		N	%
Cases	Valid	16	84.2
	Excluded[a]	3	15.8
	Total	19	100.0

a. Listwise deletion based on all variables in the procedure.

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
P1	36.81	11.629	.522	.717
P2	37.19	13.363	.065	.761
P3	37.56	11.596	.305	.745
P4	37.13	11.983	.350	.735
P5	37.38	9.850	.624	.689
P6	37.13	9.717	.612	.691
P7	37.38	12.650	.148	.762
P8	37.00	12.533	.182	.757
P9	37.31	9.696	.619	.689
P10	37.50	11.200	.677	.700

ISLAM
UNIVERSITAS
INDONESIA