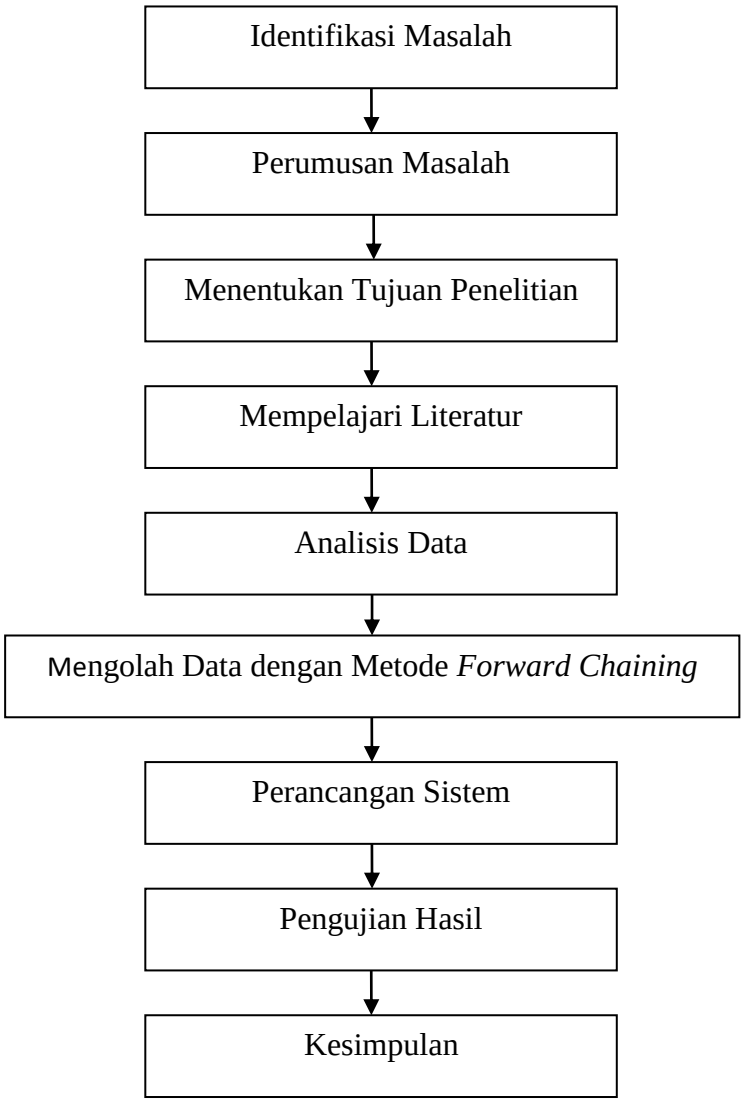
BAB III
METODE PENELITIAN

Metode penelitian pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Data yang telah diperoleh dari penelitian dapat digunakan untuk memahami, memecahkan dan mengantisipasi masalah. Memahami berarti memperjelas suatu masalah atau informasi yang tidak diketahui dan selanjutnya menjadi tahu, memecahkan berarti meminimalkan atau menghilangkan masalah, dan mengantisipasi berarti mengupayakan agar masalah tidak terjadi. (Sugiyono, 2012: 2-3)

3.1 Desain Penelitian

Menurut Sugiyono (2012:297) Metode penelitian dan pengembangan adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut. Metode penelitian dan pengembangan telah banyak digunakan pada bidang-bidang ilmu alam dan teknik. Hampir semua produk teknologi, seperti alat-alat elektronik, kendaraan bermotor, pesawat terbang, kapal laut, senjata, obat-obatan, alat-alat kedokteran, bangunan gedung bertingkat dan alat-alat rumah tangga yang modern diproduk dan dikembangkan melalui penelitian dan pengembangan. Namun demikian metode penelitian dan pengembangan bisa juga digunakan dalam bidang ilmu-ilmu sosial seperti psikologi, sosiologi, pendidikan, manajemen, dan lain-lain.

Penelitian ini menggunakan desain penelitian dengan beberapa tahap proses penelitian seperti yang terlihat pada gambar 3.1



Gambar 3.1 Desain Penelitian
(Sumber: Data Penelitian, 2016)

Berdasarkan gambar diatas berikut penjelasan mengenai langkah-langkah dalam desain Penelitian.

Berikut ini adalah penjelasan dari desain penelitian yang ada pada gambar 3.1 di atas:

1. Identifikasi Masalah

   Didalam tahap ini penelitian diawali dengan melakukan studi pendahuluan untuk mengidentifikasi permasalahan yang berkaitan dengan topik penelitian agar peneliti mendapatkan apa yang sesungguhnya menjadi masalah untuk dipecahkan.

2. Perumusan Masalah

   Didalam tahap ini peneliti merumuskan masalah yang telah didapatkan agar masalah tersebut dapat dijawab dengan baik melalui penelitian.

3. Menentukan Tujuan Penelitian

   Pada tahap ini tujuan penelitian yaitu mengetahui bagaimana sistem pakar mendeteksi tindak pidana *cybercrime* menggunakan metode *forward chaining* berbasis web.

4. Mempelajari Literatur

   Pada tahap ini peneliti mencari dan mempelajari sumber-sumber pengetahuan berupa buku-buku teori, jurnal-jurnal penelitian, dan sumber pustaka otentik lainnya yang berkaitan dengan penelitian, seperti kecerdasan buatan, sistem pakar, tindak pidana *cybercrime, php, mysql* dan *uml*

5. Analisi Data

   Setelah data-data yang berkaitan dengan tindak pidana *cybercrime* didapatkan melalui wawancara dengan pakar tindak pidana *cybercrime* maupun melalui studi literatur yang berhubungan dengan tindak pidana *cybercrime*, kemudian peneliti menganalisa data-data yang dibutuhkan sistem pakar dan dikelompokkan agar lebih mudah melakukan proses pengolahan datanya.

6. Mengolah data dengan metode *Forward Chanining*

   Setelah data-data yang telah dianalisa kemudian diolah menggunakan metode *forward chaining* untuk membuat kaidah (*rule*) yang akan digunakan saat sistem pakar melakukan penelusuran sebelum menyimpulkan hasil.

7. Perancangan Sistem

   Pada tahap ini peneliti melakukan kegiatan perancangan mulai dari desain basis pengetahuan, desain *uml*, desain database, desain antar muka yang akan digunakan untuk mendeteksi tindak pidana *cybercrime* berdasarkan data yang ada.

8. Pengujian Hasil

   Didalam tahap ini bertujuan untuk meminimalisir kesalahan dan memastikan keluaran yang dihasilkan sesuai dengan yang diinginkan. Sistem ini diuji dengan membandingkan hasil deteksi pakar dengan hasil deteksi sistem untuk melihat apakah sistem berjalan dengan baik.

9. Kesimpulan

   Tahap terakhir dalam penelitian ini yaitu menyimpulkan hasil penelitian yang berisi jawaban terhadap rumusan masalah berdasarkan data-data yang ada. Peneliti juga memberikan saran yang penting untuk membantu dalam memecahkan permasalahan yang ada.

3.2 Pengumpulan Data

Pengumpulan data merupakan langkah yang dilakukan peneliti untuk mendapatkan data-data yang berkaitan dengan tindak pidana *cybercrime* untuk mendukung penelitian yang sedang dilakukan. Teknik pengumpulan data yang dilakukan dalam penelitian ini adalah:

1. Wawancara

   Wawancara digunakan sebagai teknik pengumpulan data apabila peneliti ingin melakukan studi pendahuluan untuk menemukan permasalahan yang harus diteliti, dan juga apabila peneliti ingin mengetahui hal-hal dari responden yang lebih mendalam dan jumlah respondennya sedikit/kecil (Sugiyono, 2012:137). Untuk mendapatkan data-data yang berkaitan dengan penelitian, peneliti melakukan wawancara langsung dengan Bapak Tyas Satria Manggala, S.STP yang bekerja sebagai Penata Tingkat I/III d, Kabid Penyelenggaraan E-Goverment di Kantor Dinas Komunikasi dan Informatika (Kominfo) lantai 7 (tujuh) Gedung Wali Kota Batam.

2. Studi Literatur

   Peneliti melakukan studi literatur dengan mengumpulkan, membaca, dan memahami referensi teoritis yang berasal dari buku-buku, jurnal-jurnal penelitian dan sumber pustaka otentik lainnya yang berkaitan dengan penelitian.

3.3 Operasional Variabel

Variabel penelitian pada dasarnya adalah segala sesuatu yang berbentuk apa saja yang ditetapkan oleh peneliti untuk dipelajari sehingga diperoleh informasi dan kesimpulannya (Sudaryono, 2015:16).

Variabel yang digunakan dalam penelitian ini adalah Tindak pidana *cybercrime*. *Cybercrime*didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi computer yang berbasasis pada kecanggihan perkembangan teknologi internet. Terdapat beberapa bagian yang mempengaruhi tindak pidana *cybercrime* sekaligus menjadi indikator tindak pidana *cybercrime*.

Tabel 3.1 Variabel dan Indikator

Variabel	Indikator
Tindak Pidana *Cybercrime*	Informasi Ilegal
	Akses Ilegal
	Intersepsi Ilegal
	Gangguan Terhadap Data
	Gangguan Terhadap Sistem
	Penyalahgunaan Perangkat

Sumber: Data Penelitian, (2016)

3.4 Metode Perancangan Sistem

Perancangan sistem bisa digambarkan dalam suatu bagan alir yang menjelaskan keseluruhan proses yang dilakukan. Jika ada data riil yang diambil, jelaskan kapan, di mana, dan bagaimana data yang diambil. Kalau dengan wawancara, jelaskan siapa aja yang kita wawancarai. Jika menggunakan

kuesioner, jelaskan inti pertanyaan dalam kuesioner tersebut. Jika data diambil melalui pengamatan, jelaskan bagaimana melakukannya (Sudaryono, 2015:230).

3.4.1 Desain basis pengetahuan

Sebelum melakukan desain basis pengetahuan, peneliti telah melakukan proses akuisisi pengetahuan dengan mengumpulkan pengetahuan dan fakta dari sumber-sumber yang tersedia. Sumber pengetahuan dan fakta diperoleh melalui wawancara dengan pakar tindak pidana *cybercrime* dan studi literatur tentang materi yang berkaitan dengan tindak pidana *cybercrime*. Sumber pengetahuan dan fakta yang didapat berupa data-data yang berhubungan dengan tindak pidana *cybercrime*, sanksi-sanksi tindak pidana *cybercrime* berdasarkan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pengetahuan dan fakta tersebut ditampilkan dalam Tabel Indikator (Tabel 3.2), Tabel Kejahatan (Tabel 3.3), Tabel Ciri-ciri Kejahatan (Tabel 3.4), dan Tabel Aturan (Tabel 3.5).

Tabel 3.2 Tabel Indikator

Kode	Nama Indikator
IND01	Informasi Ilegal
IND02	Akses Ilegal
IND03	Intersepsi Ilegal
IND04	Gangguan Terhadap Data
IND05	Gangguan Terhadap Sistem
IND06	Penyalahgunaan Perangkat

Sumber: Data Penelitian (2016)

Pada (Tabel 3.3) di bawah terdapat beberapa dari Kode Kejahatan, Jenis Kejahatan, serta Sanksi-sanksi dari Kejahatan *Cybercrime.*

Tabel 3.3 TabelKejahatan *Cybercrime*

Kode Kejahatan	Jenis Kejahatan	Sanksi Kejahatan
K01	KejahatanAsusila	1. Dijerat Pasal 27 ayat 1: Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksenya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan. 2. Sanksi Pidana Pasal 45 ayat 1: Pidana penjara paling lama 4 Tahun dan Denda paling banyak Rp 750 juta.
K02	Kejahatan Perjudian	1. Dijerat Pasal 27 ayat 2: Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksenya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar perjudian. 2. Sanksi Pidana Pasal 45 ayat 1: Pidana penjara paling lama 4 Tahun dan Denda paling banyak Rp 750 juta.
K03	Kejahatan Penghinaan dan Pencemaran Nama Baik	1. Dijerat Pasal 27 ayat 3: Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksenya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar penghinaan dan/atau pencemaran nama baik. 2. Sanksi Pidana Pasal 45 ayat 1: Pidana penjara paling lama 4 Tahun dan Denda paling banyak Rp 750 juta.
K04	Kejahatan Pemerasan dan Pengancaman	1. Dijerat Pasal 27 ayat 4: Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksenya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar pemerasan dan/atau pengancaman. 2. Sanksi Pidana Pasal 45 ayat 1: Pidana penjara paling lama 4 Tahun dan Denda paling banyak Rp 750 juta.
K05	Kejahatan Penipuan dan Berita Bohong	1. Dijerat Pasal 28 ayat 1: Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. 2. Sanksi Pidana Pasal 45 ayat 2: Pidana penjara

Tabel 3.3 Lanjutan

		paling lama 6 Tahun dan Denda paling banyak Rp 1 miliar.
K06	Kejahatan Berita Kebencian dan Permusuhan	1. Dijerat Pasal 28 ayat 2: Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA). 2. Sanksi Pidana Pasal 45 ayat 2: Pidana penjara paling lama 6 Tahun dan Denda paling banyak Rp 1 miliar.
K07	Kejahatan Ancaman Kekerasan dan Menakut-nakuti	1. Dijerat Pasal 29: Setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakuti-nakuti yang ditujukan secara pribadi. 2. Sanksi Pidana Pasal 45 ayat 3: Pidana penjara paling lama 4 Tahun dan Denda paling banyak Rp 750 juta.
K08	Kejahatan Akses Komputer Orang Tanpa Izin	1. Dijerat Pasal 30 ayat 1: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun. 2. Dijerat Pasal 30 ayat 2: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik. 3. Dijerat Pasal 30 ayat 3: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. 4. Sanksi Pidana Pasal 46 ayat 1: Pidana penjara paling lama 6 Tahun dan Denda paling banyak Rp 600 juta 5. Sanksi Pidana Pasal 46 ayat 2: Pidana penjara paling lama 7 Tahun dan Denda paling banyak Rp 700 juta. 6. Sanksi Pidana Pasal 46 ayat 3: Pidana penjara paling lama 8 Tahun dan Denda paling banyak Rp 800 juta.
K09	Kejahatan Penyadapan	1. Dijerat Pasal 31 ayat 1: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum

Tabel 3.3 Lanjutan

		melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain. 2. Dijerat Pasal 31 ayat 2: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan. 3. Sanksi Pidana Pasal 47: Pidana penjara paling lama 10 Tahun dan Denda paling banyak Rp 800 juta.
K10	Kejahatan Cracker	1. Dijerat Pasal 32 ayat 1: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik. 2. Dijerat Pasal 32 ayat 2: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak. 3. Dijerat Pasal 32 ayat 3: Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagimana mestinya. 4. Sanksi Pidana Pasal 48 ayat 1: Pidana penjara paling lama 8 Tahun dan Denda paling banyak Rp 2 miliar. 5. Sanksi Pidana Pasal 48 ayat 2: Pidana penjara paling lama 9 Tahun dan Denda paling banyak Rp 3 miliar.

Tabel 3.3 Lanjutan

		6. Sanksi Pidana Pasal 48 ayat 3: Pidana penjara paling lama 10 Tahun dan Denda paling banyak Rp 5 miliar.
K11	Kejahatan Hacker	1. Dijerat Pasal 33: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya. 2. Sanksi Pidana Pasal 49: Pidana penjara paling lama 10 Tahun dan Denda paling banyak Rp 10 miliar.
K12	Kejahatan Abuse	1. Dijerat Pasal 34 ayat 1a: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33. 2. Dijerat Pasal 34 ayat 1b: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu yang ditujukan agar sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33. 3. Sanksi Pidana Pasal 50: Pidana penjara paling lama 10 Tahun dan Denda paling banyak Rp 10 miliar.
K13	Kejahatan Pemalsuan Data	1. Dijerat Pasal 35: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik. 2. Sanksi Pidana Pasal 51 ayat 1: Pidana penjara paling lama 12 Tahun dan Denda paling banyak Rp 12 miliar.

Sumber: Data Penelitian (2016)

Sistem pakar ini yang menggunakan metode *Forward Chaining* pada penelitian ini digunakan untuk mendeteksi tindak pidana *Cybercrime*. Untuk data jenis-jenis kejahatan *Cybercrime* bisa di lihat pada (Tabel 3.4) di bawah ini.

Tabel 3.4 Tabel Ciri-ciri Kejahatan *Cybercrime*

Kode Ciri-ciri Kejahatan	Ciri-ciri Kejahatan
CK01	Pelaku melakukan tindak pidana *cybercrime* kesusilaan
CK02	Pelaku menyebarkan video porno seseorang ke dunia maya
CK03	Membuat video porno seseorang itu dapat di akses oleh publik
CK04	Pelaku melakukan aktivitas Perjudian
CK05	Pelaku melakukan aktivitas perjudian secara online disitus web
CK06	Pelaku mengirim berupa komentar dengan unsur penghinaan ke pengguna lain di sosial media
CK07	Pelaku mempublikasikan identitas seseorang yang bersifat fitnah di dunia maya
CK08	Pelaku mengirim pesan yang berisi pemerasan atau pengancaman terhadap pihak tertentu di dunia maya
CK09	Pelaku meminta sejumlah uang dan mengancam menyebarkan photo vulgar seseorang
CK10	Pelaku menyebarkan informasi atau berita bohong yang dapat menyesatkan seseorang
CK11	Pelaku melakukan tindak penipuan yang dapat merugikan seseorang dalam transaksi jual beli online
CK12	Pelaku mengirim informasi yang dapat menyebabkan permusuhan
CK13	Pelaku mengirim status atau informasi di media sosial yang dapat menyebabkan individu atau sekelompok orang terpengaruh permusuhan antar golongan
CK14	Pelaku mengancam dan menakut-nakuti kepada seseorang di sosial media
CK15	Pelaku mengirim informasi atau dokumen kepada seseorang yang bersifat teror yang dapat meresahkan seseorang
CK16	Pelaku mengakses komputer atau sistem elektronik seseorang dengan cara apapun
CK17	Pelaku mengakses sistem seseorang untuk memperoleh informasi yang diinginkan
CK18	Pelaku menerobos atau menjebol sistem pengamanan komputer seseorang dengan cara apapun
CK19	Pelaku melakukan penyadapan akses komunikasi seseorang

Tabel 3.4 Lanjutan

CK20	Pelaku melakukan penyadapan akses komunikasi seseorang baik yang tidak menyebabkan perubahan maupun menyebabkan perubahan atau penghentian informasi
CK21	Pelaku memindahkan atau mentransfer dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak dengan cara apapun
CK22	Pelaku merusak, mengurangi atau menyembunyikan informasi atau dokumen elektronik milik orang lain
CK23	Pelaku mengirim software atau virus sistem seseorang
CK24	Pelaku melakukan tindakan yang membuat terganggunya sistem seseorang agar tidak bekerja sebagaimana mesti
CK25	Pelaku menyediakan perangkat keras atau perangkat lunak untuk memfasilitasi kejahatan *cybercrime*
CK26	Pelaku menjual kata sandi atau kode akses dengan tujuan memfasilitasi kejahatan *cybercrime*
CK27	Pelaku melakukanpemalsuandokumen atau informasimilikperusahaan atau instansidengancara apapun
CK28	Pelaku memanipulasidatatersebutsehinggaseolah-olahdianggapdata yangotentik

Sumber: Data Penelitian (2016)

Data aturan ini disusun untuk memudahkan penelitian ini dalam menyusun kaidah yang akan digunakan sebagai basis pengetahuan dalam sistem pakar pada penelitian ini. Susunan data aturan bisa di lihat pada (Tabel 3.5) di bawah ini:

Tabel 3.5 Tabel Aturan

Kode Indikator	Kode Kejahatan	Ciri-ciri Kejahatan
IND01	K01	CK01,CK02,CK03
IND01	K02	CK04,CK05
IND01	K03	CK06,CK07
IND01	K04	CK08,CK09
IND01	K05	CK10,CK11
IND01	K06	CK06,CK12,CK13
IND01	K07	CK08,CK14,CK15
IND02	K08	CK16,CK17,CK18
IND03	K09	CK16,CK17,CK19,CK20
IND04	K10	CK16,CK21,CK22
IND05	K11	CK16,CK23,CK24
IND06	K12	CK25,CK26
IND04	K13	CK16,CK27,CK28

Sumber: Data Penelitian (2016)

Berdasarkan data aturan yang telah disusun, maka kaidah yang akan digunakan dalam sistem pakar dan tabel keputusannya adalah sebagai berikut:

1. Kaidah: IF CK01 *AND* CK02 *AND* CK03 *THEN* K01
2. Kaidah: IF CK04 *AND* CK05 *THEN* K02
3. Kaidah: IF CK06 *AND* CK07 *THEN* K03
4. Kaidah: IF CK08 *AND* CK09 *THEN* K04
5. Kaidah: IF CK10 *AND* CK11 *THEN* K05
6. Kaidah: IF CK06 *AND* CK12 *AND* CK13 *THEN* K06
7. Kaidah: IF CK08 *AND* CK14 *AND* CK15 *THEN* K07
8. Kaidah: IF CK16 *AND* CK17 *AND* CK18 *THEN* K08
9. Kaidah: IF CK16 *AND* CK17 *AND* CK19 *AND* CK20 *THEN* K09
10. Kaidah: IF CK16 *AND* CK21 *AND* CK22 *THEN* K10
11. Kaidah: IF CK16 *AND* CK23 *AND* CK24 *THEN* K11
12. Kaidah: IF CK25 *AND* CK26 *THEN* K12
13. Kaidah: IF CK16 *AND* CK27 *AND* CK28 *THEN* K13

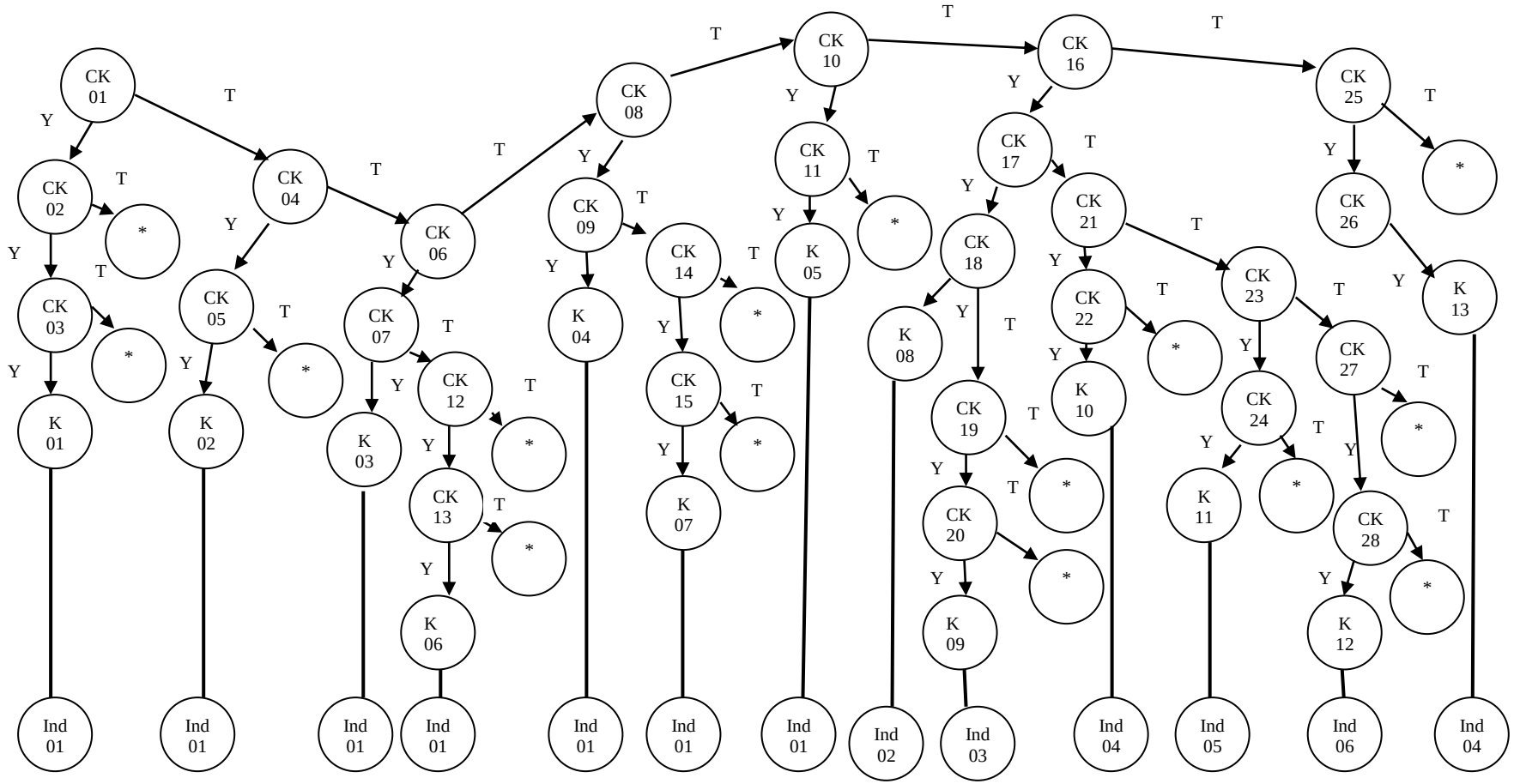
Berdasarkan data aturan atau kaidah keputusan yang telah di susun di atas, terdapat ciri-ciri kejahatan*cybercrime* atau kasus-kasus kejahatan*cybercrime* maka disimpulkan suatu hasil atau keputusan berupa pasal-pasal atau sanksi-sanksi tindak pidana *cybercrime* berdasarkan Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berlaku.

Tabel 3.6 Tabel Keputusan

Bagian				Ind 01				Ind 02	Ind 03	Ind 04	Ind 05	Ind 06	Ind 04
Ciri-Ciri Kasus	K 01	K 02	K 03	K 04	K 05	K 06	K 07	K 08	K 09	K 10	K 11	K 12	K 13
CK01	√												
CK02	√												
CK03	√												
CK04		√											
CK05		√											
CK06			√			√							
CK07			√										
CK08				√			√						
CK09				√									
CK10					√								
CK11					√								
CK12						√							
CK13						√							
CK14							√						
CK15							√						
CK16								√	√	√	√		√
CK17								√	√				
CK18								√					
CK19									√				
CK20									√				
CK21										√			
CK22										√			
CK23											√		
CK24											√		
CK25												√	
CK26												√	
CK27													√
CK28													√

Sumber: Data Penelitian (2016)

Berdasarkan Tabel 3.6 Tabel Keputusan diatas menunjukkan ciri-ciri kejahatan atau kasus-kasus kejahatan untuk mendapatkan suatu hasil atau keputusan dari penelitian ini. Berdasarkan maka pohon keputusan adalah sebagai berikut:



Gambar 3.2 Pohon Keputusan
(Sumber: Data Penelitian, 2016)

Data ciri-ciri kasus ditentukan sebagai keadaan awal dalam sistem pakar ini saat melakukan penelusuran sebelum memperoleh keputusan atau kesimpulan. Proses penelusuran selanjutnya tergantung bagaimana jawaban yang diberikan pengguna. Jika pengguna memberikan jawaban "Benar", maka penelusuran menuju simpul kiri pada level berikutnya dan jika pengguna memberikan jawaban "Tidak", maka penelusuran menuju simpul kanan pada level berikunya, begitu seterusnya sampai penelusuran menemukan simpul "K (Kode Kejahatan)" atau simpul *****. Simpul "K (Kode Kejahatan)" berasosiasi dengan simpul "IND (Indikator)" yang berarti bahwa simpul "K (Kode Kejahatan)" tersebut bagian dari "IND (Indikator)". Simpul ***** merupakan simpul yang berarti tidak menghasilkan kesimpulan tertentu. Pada sistem pakar ini, jika penelusuran menemukan simpul * maka sistem akan kembali melakukan penelusuran mulai dari keadaan awal.

3.4.2 Struktur Kontrol (Mesin Inferensi)

Mesin inferensi dalam sistem pakar ini menggunakan metode penelusuran *forward chaining*. Langkah-langkah yang digunakan dalam proses penelusurannya adalah sebagai berikut:

1. Mengajukan pertanyaan tentang kasus-kasus tindak pidana *cybercrime* oleh pengguna internet (*user*).
2. Menyimpan sementara jawaban pengguna tentang kasus-kasus tindak pidana *cybercrime* ke dalam memori sementara

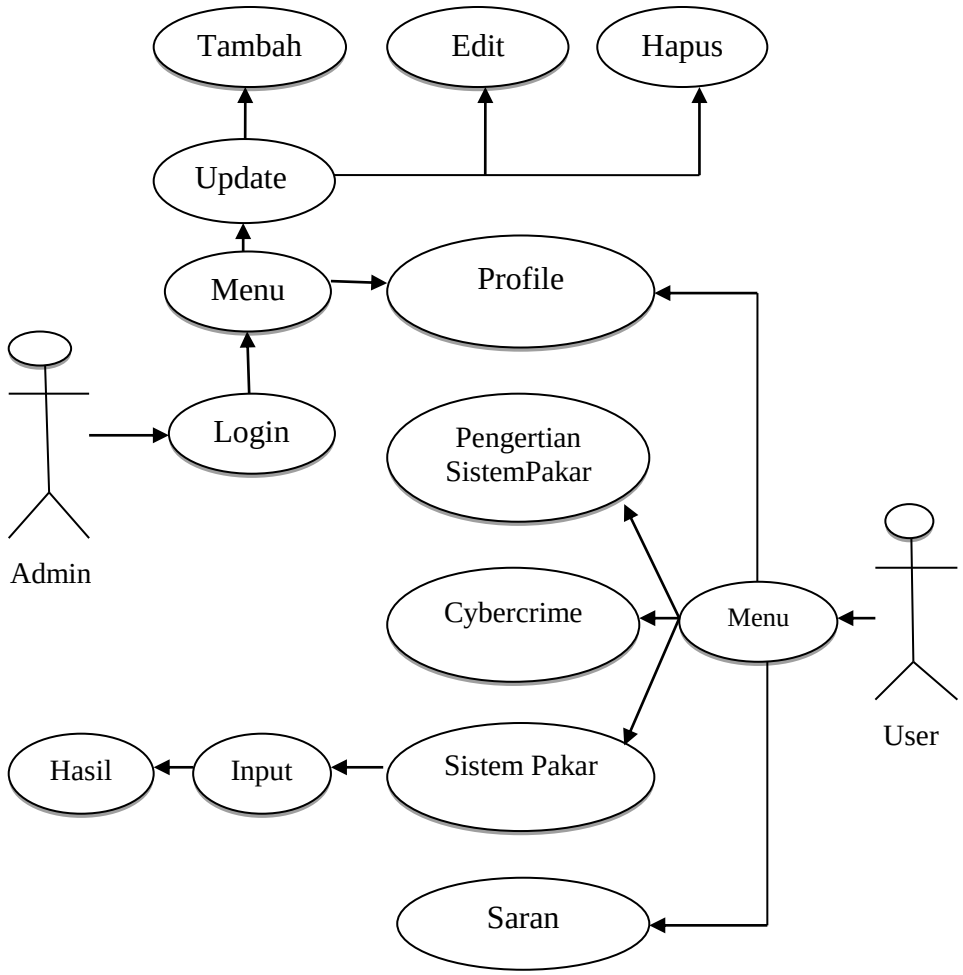
3. Memeriksa gejala-gejala yang ada dengan aturan yang telah dibuat, jika ada konklusi yang cocok maka simpan hasil kedalam memori tetap, jika belum memenuhi konklusi apapun, ulangi
4. Menampilkan hasil kasus-kasus serta sanksi-sanksi tindak pidana *cybercrime*

3.4.3 Desain UML (*Unifield Modeling Languange*)

1. *Use case Diagram*

Use case diagram menjelaskan aktor-aktor yang terlibat dengan perangkat lunak yang dirancang untuk sistem pakar dalam penelitian ini beserta proses-proses di dalamnya.

Berikut ini adalah gambar *user case* diagram *admin* dan *user:*



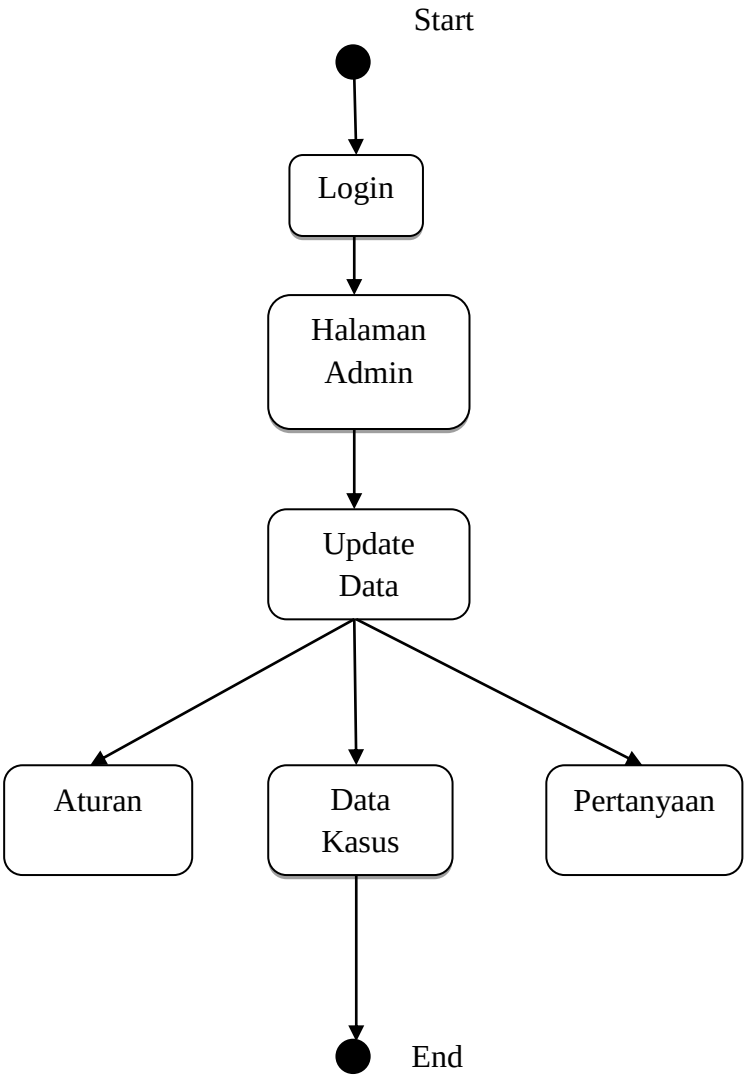
Gambar 3.3 Diagram *Use Case Admin* dan *User*
(Sumber**:** Data Penelitian, 2016)

Use case diagram menjelaskan admin dan user yang terlibat denganaktor-aktor perangkat lunak yang dirancang untuk sistem pakar dalam penelitian ini beserta proses-proses di dalamnya.

2. *Activity Diagram*

Activity diagram menggambarkan aliran aktifitas dari sebuah sistem, yang dirancang untuk sistem pakar.

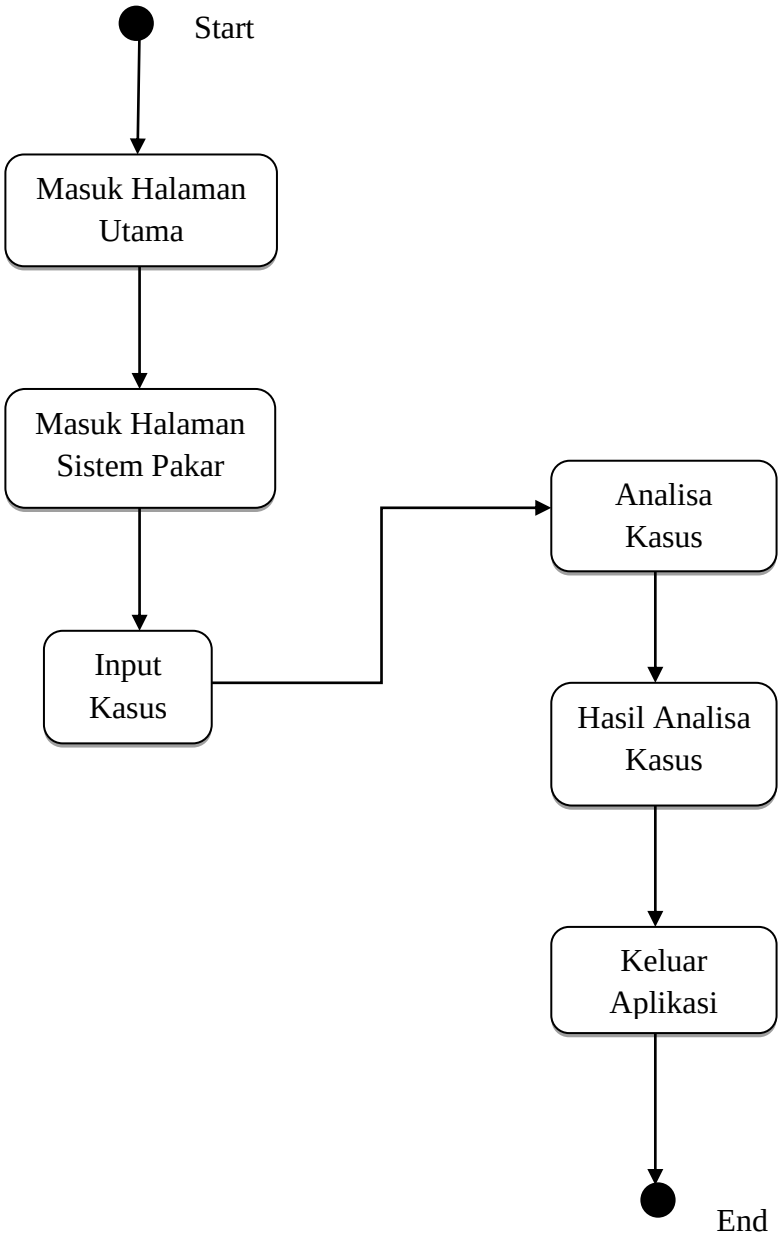
a. *Activity diagram admin*



Gambar 3.4 *Activity diagram admin*
(Sumber: Data Penelitian 2016)

Activity diagram admin diatas menggambarkan suatu aliran aktifitas dari sebuah sistem yang dirancang untuk sistem pakar dalam penelitian ini.

b. Activity diagram user

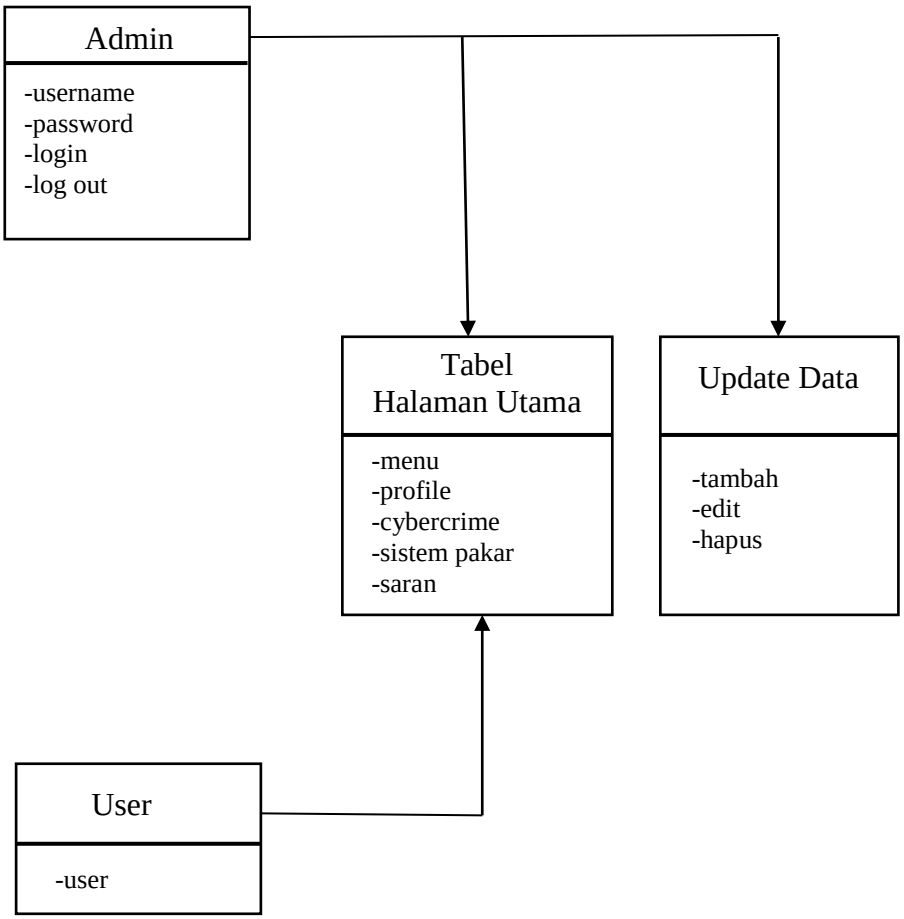


Gambar 3.5 *Activity diagram user*
(Sumber: Data Penelitian 2016)

*Activity diagram user*diatas menggambarkan suatu aliran aktifitas dari sebuah sistem yang dirancang untuk sistem pakar dalam penelitian ini.

3. *Class Diagram*

Class diagram menggambarkan struktur sistem pakar tindak pidana *cybercrime*. Berikut ini adalah gambar *class diagram:*



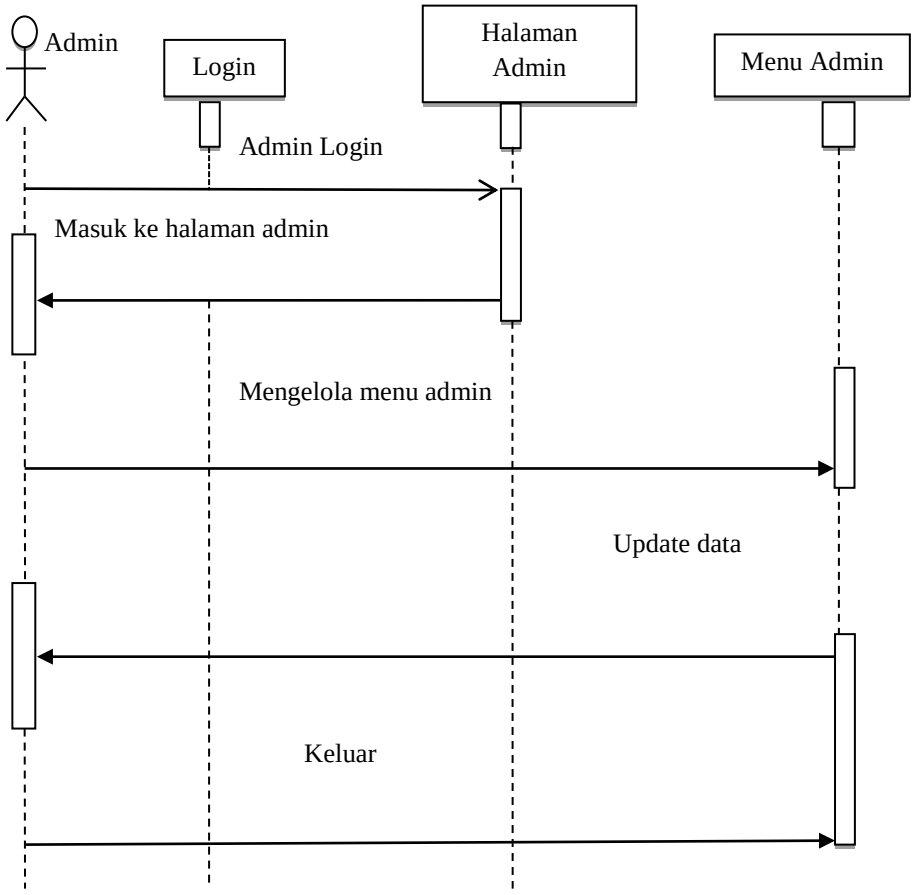
Gambar 3.6 *Class diagram*
(Sumber: Data Penelitian 2016)

Class diagram diatas saling berkaitan antara admin dan user untuk menggambarkan struktur sistem pakar tindak pidana *cybercrime*untuk sistem pakar dalam penelitian ini.

4. *Sequence Diagram*

Sequence diagram yang menggambarkan interaksi antar obyek dan mengindikasikan diantara obyek tersebut.

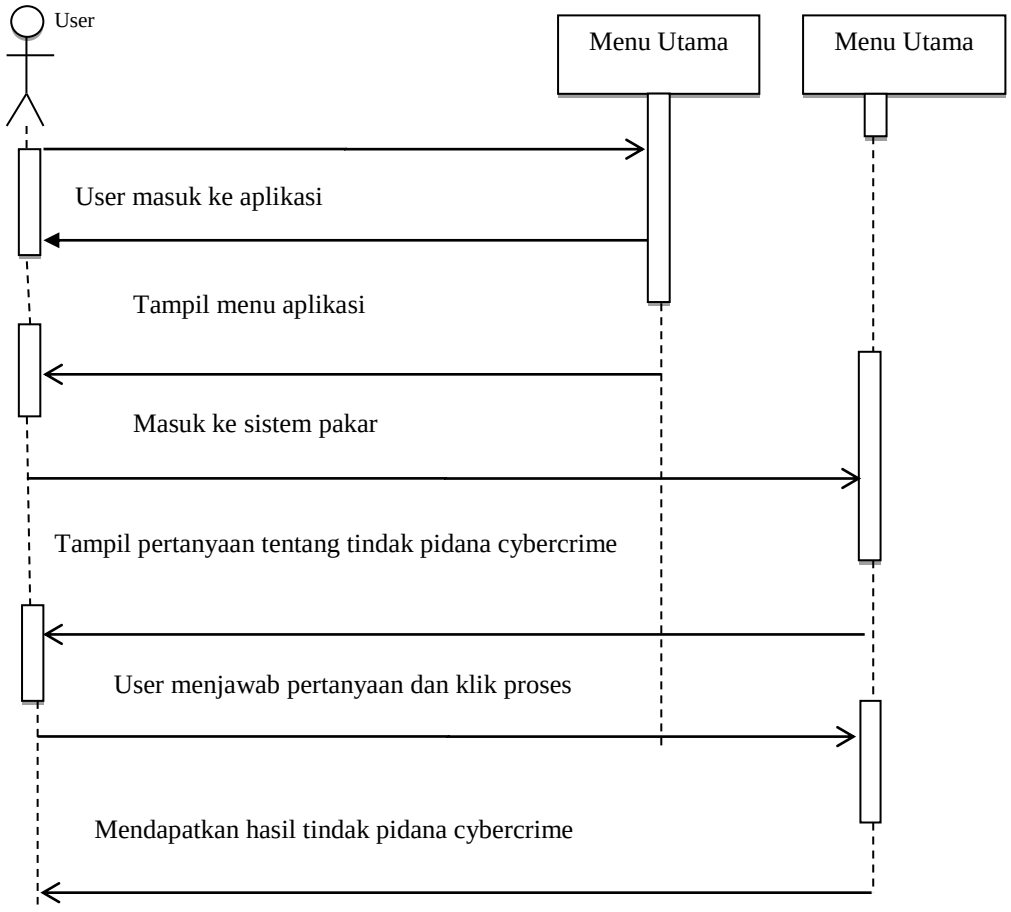
a. *Sequence diagram admin*



Gambar 3.7 *Sequence diagram admin*
(Sumber: Data Penelitian 2016)

*Sequence diagram admin*diatas yang menggambarkan interaksi admin antar obyek dan mengindikasikan diantara obyek tersebut di sistem pakar dalam penelitian ini.

b. *Sequence Diagram User*



Gambar 3.8 *Sequence Diagram User*
(Sumber: Data Penelitian, 2016)

*Sequence diagram user*diatas yang menggambarkan interaksi user antar obyek dan mengindikasikan diantara obyek tersebut di sistem pakar dalam penelitian ini.

3.4.4 Desain *Database*

1. Tabel Admin

Tabel ini berfungsi untuk menyimpan data admin, berisikan *username* dan *password* untuk dapat masuk dan mengakses menu pada halaman admin.

Tabel 3.7 Tabel Admin

No	Field	Type	Size
1	Username	Varchar	30
2	Password	Varchar	30

Sumber: Data Penelitian (2016)

2. Tabel Konsultasi

Tabel ini berfungsi untuk menyimpan data solusi dan pertanyaan yang akan ditampilkan oleh sistem pakar

Tabel 3.8 Tabel Konsultasi

No	Field	Type	Size
1	Id	Int	11
2	solusi_pertanyaan	Varchar	500
3	bila_benar	Int	11
4	bila_salah	Int	11
5	Mulai	char	1
6	Selesai	char	1

Sumber: Data Penelitian (2016)

3. Tabel *Comment*

Tabel ini berfungsi untuk menyimpan data komentar dan saran yang dibuat oleh *user*.

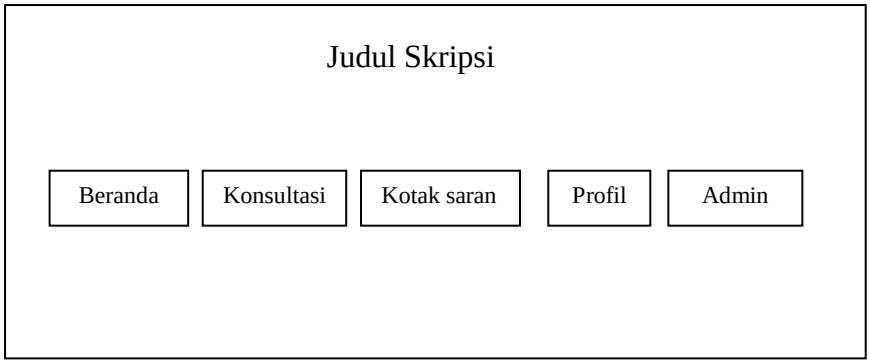
Tabel 3.9 Tabel *Comment*

No	Field	Type	Size
1	Nama	Varchar	30
2	Komentar	Varchar	500
3	Date	Datetime	

Sumber: Data Penelitian (2016)

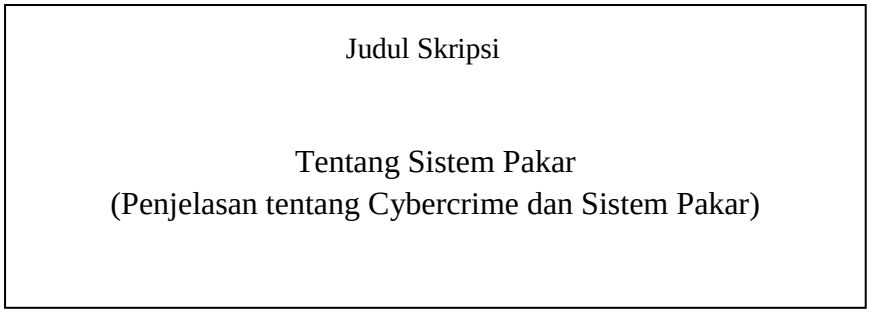
3.4.5 Desain Antarmuka (*Prototype*)

1. Menu Depan Sistem



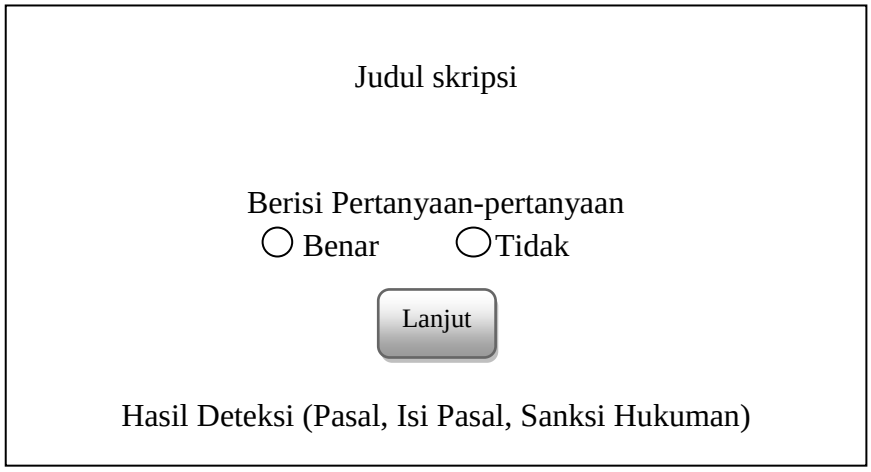
Gambar 3.9 Menu Utama User
(Sumber: Data Penelitian, 2016)

2. Menu Beranda



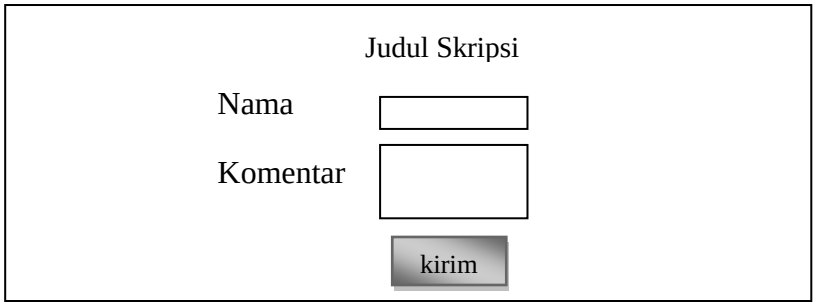
Gambar 3.10 Menu Tentang Sistem & Hukum
(Sumber: Data Penelitian, 2016)

3. Menu Konsultasi Sistem Pakar



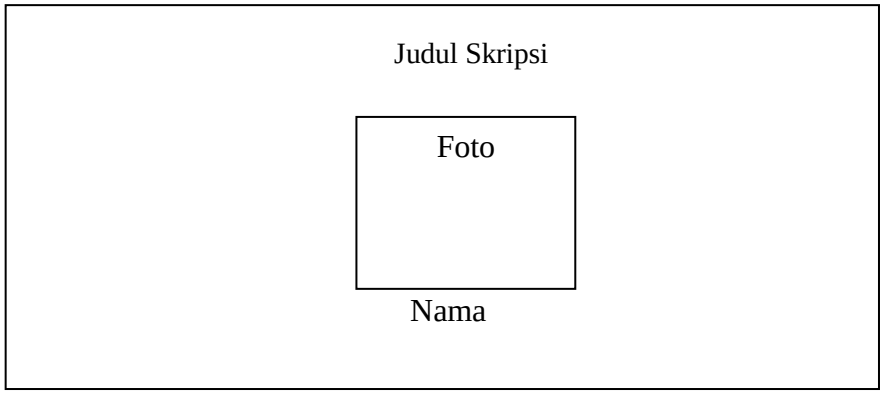
Gambar 3.11 Menu Konsultasi Sistem Pakar
(Sumber: Data Penelitian, 2016)

4. Menu Komentar dan Saran



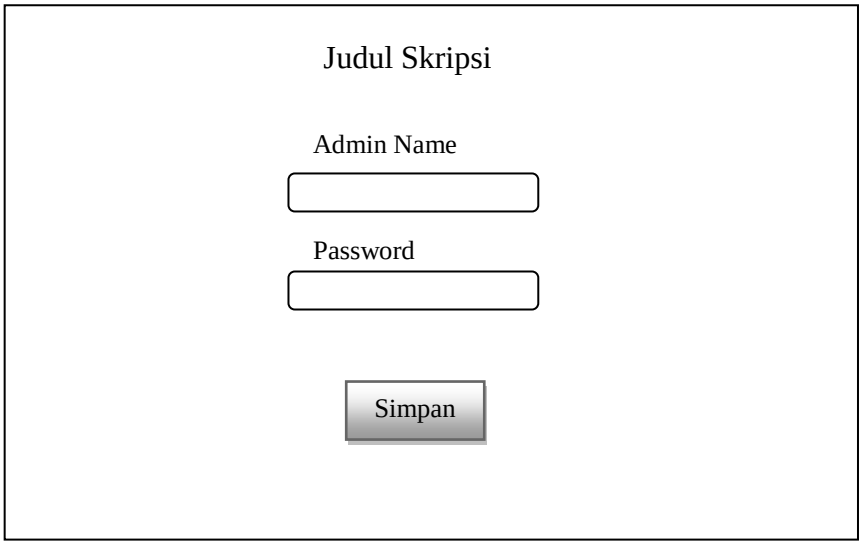
Gambar 3.12 Menu Komentar & Saran
(Sumber: Data Penelitian, 2016)

5. Menu Profil



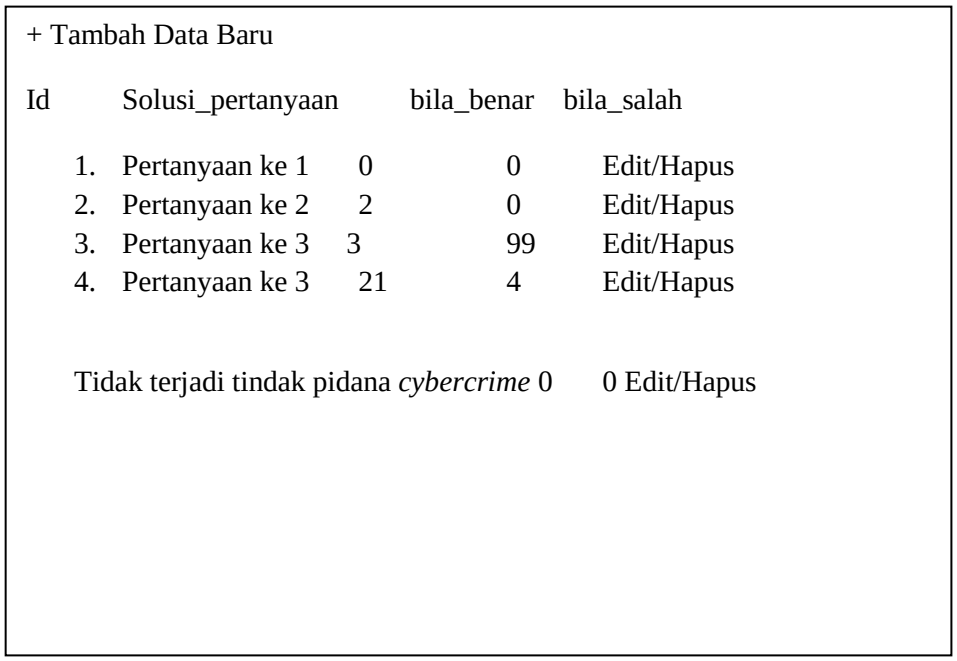
Gambar 3.13 Menu Profil
(Sumber: Data Penelitian, 2016)

6. Login Admin



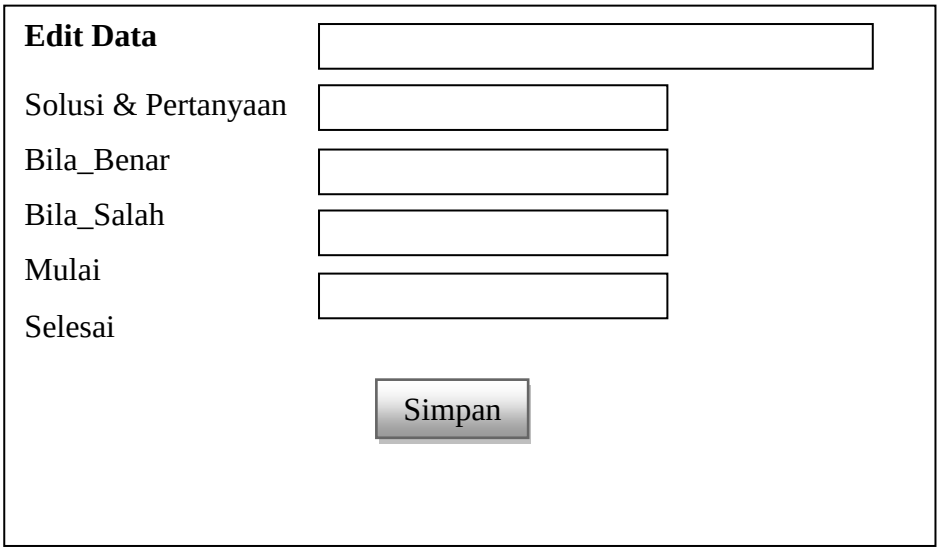
Gambar 3.14 Halaman Login Admin
(Sumber: Data Penelitian, 2016)

7. Halaman Admin



Gambar 3.15 Halaman Admin
(Sumber: Data Penelitian, 2016)

8. Halaman Edit Data



Gambar 3.16 Halaman Edit Data
(Sumber: Data Penelitian, 2016)

3.5 Lokasi dan Jadwal Penelitian

Penelitian ini dilakukan di Kantor Dinas Komunikasi dan Informatika (Kominfo) lantai 7 (tujuh) Gedung Wali Kota Batam yang beralamat Jalan Engku Puteri No. 1 Batam Center.

3.5.1 Jadwal Penelitian

Setiap rancangan penelitian perlu dilengkapi dengan jadwal kegiatan yang akan dilaksanakan. Dalam jadwal yang berisi kegiatan apa saja yang akan dilakukan, dan berapa lama dilakukan (Sugiyono, 2012:286). Berikut ini adalah tabel jadwal kegiatan yang dilakukan selama penelitian berlangsung.

No	Kegiatan	Tahun 2016/2017																			
		September				Oktober				November				Desember				Januari			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Pengajuan judul																				
2	BAB I																				
3	BAB II																				
4	BAB III																				
5	BAB IV																				
6	BAB V, Daftar Pustaka dan Lampiran																				

Gambar 3.17 Jadwal Penelitian
(Sumber: Data Penelitian, 2016)