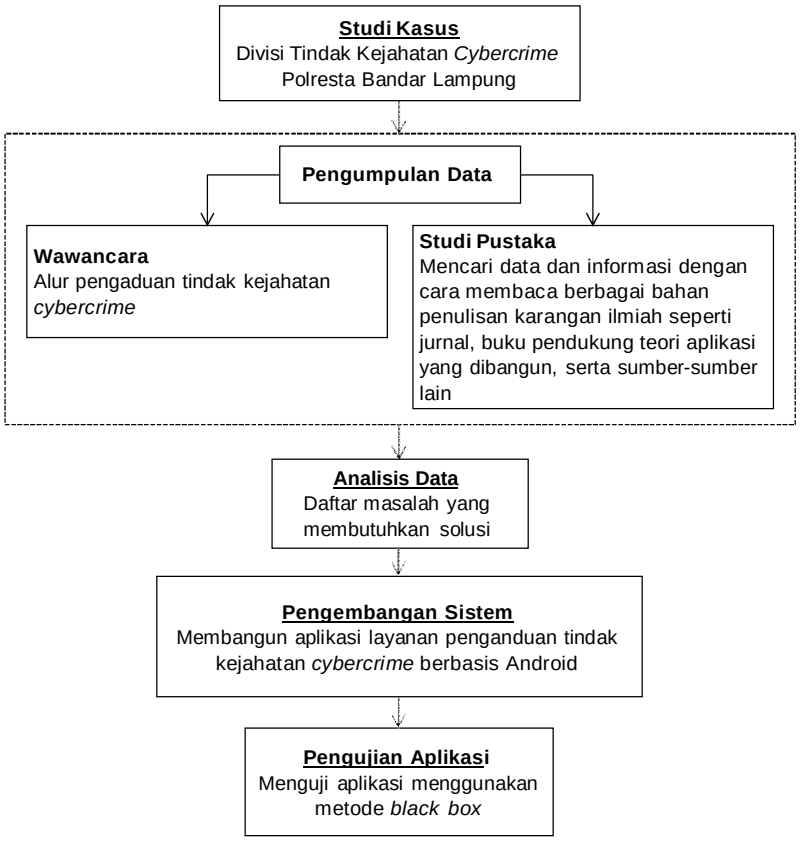
BAB III
METODOLOGI PENELITIAN

Kerangka Penelitian

Penelitian dimulai dengan menentukan tempat penelitian yaitu di Polresta Bandar Lampung bagian divisi tindak kejahatan *cybercrime*. Setelah itu, langkah berikutnya adalah melakukan pengumpulan data berkaitan dengan tindak kejahatan *cybercrime* dengan cara wawancara dan studi pustaka. Setelah data didapat, tahap selanjutnya adalah menganalisa data dengan mencari kekurangan dari sistem yang berjalan kemudian ditetapkanlah suatu solusi. Setelah mendapatkan solusi, langkah selanjutnya adalah mengembangkan sistem dari solusi tersebut. Langkah terakhir adalah menguji coba aplikasi dari pengembangan sistem menggunakan metode pengujian *black box*. Adapun kerangka dari penelitian yang dilakukan adalah seperti pada Gambar 3.1.



Gambar 3.1 Kerangka Kerja Penelitian

Communication

Tahapan awal yang dilakukan adalah berkomunikasi dengan divisi tindak kriminal *cybercrime* Polresta Bandar Lampung. Untuk mendapatkan data terkait dengan tindak kejahatan *cybercrime*, langkah yang diambil peneliti yaitu dengan cara wawancara serta studi pustaka.

a. Wawancara

   Komunikasi dilakukan dengan cara wawancara mengenai layanan pengaduan tindak kejahatan *cybercrime*. Pelapor membuat lapioran tindak kejahatan *cybercrime* ke Polres atau Polsek setempat di daerah kediaman pelapor. Pelapor menyertakan bukti adanya tindak kejahatan *cybercrime* berupa bukti foto serta alamat akun (media sosial) atau alamat *browser* yang terkait. Pelaporan tersebut kemudian akan diselidiki oleh divisi tindak kriminal *cybercrime*. Jika bukti tersebut memenuhi kriteria tindak kejahatan *cybercrime*, maka kasus akan ditindaklanjuti.

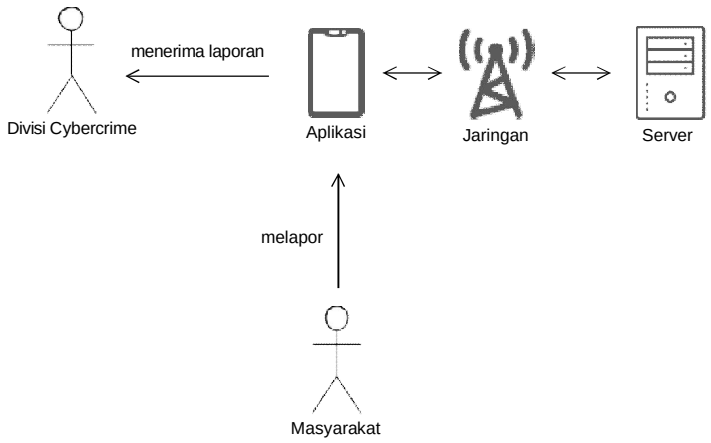
b. Studi Pustaka

   Setelah didapati data dari divisi tindak kejahatan *cybercrime*, maka langkah selanjutnya adalah melakukan studi pustaka. Studi pustaka dilakukan untuk memperoleh data dan informasi berkaitan dengan penelitian. Studi pustaka dilakukan dengan cara mencari informasi terkait dengan aplikasi yang akan dibangun berupa jurnal maupun buku-buku yang berkaitan dengan pengembangan aplikasi.

Arsitektur Sistem

Adapun perancangan arsitektur sistem yang diusulkan adalah seperti yang terlihat pada Gambar 3.2. Aplikasi yang dibangun terdiri dari akses divisi *cybercrime* dan masyarakat. Divisi *cybercrime* dapat dartikan sebagai admin atau orang yang bertanggung jawab atas pelaporan data tindak kejahatan *cybercrime* oleh masyarakat. Dalam hal ini, divisi *cybercrime* adalah orang yang berasal dari kepolisian. Masyarakat disini diartikan sebagai pengguna aplikasi layanan pengaduan *cybercrime*. Masyarakat dapat melaporkan tindak kejahatan *cybercrime* melalui aplikasi ini. Aplikasi layanan pengaduan *cybercrime* ini hanya dapat diakses melalui *smartphone* Android dengan versi minimal 8.0 (Oreo). Data

tindak kejahatan *cybercrime* tersimpan di *server* dengan penyimpanan MySQL yang dapat diakses melalui internet.



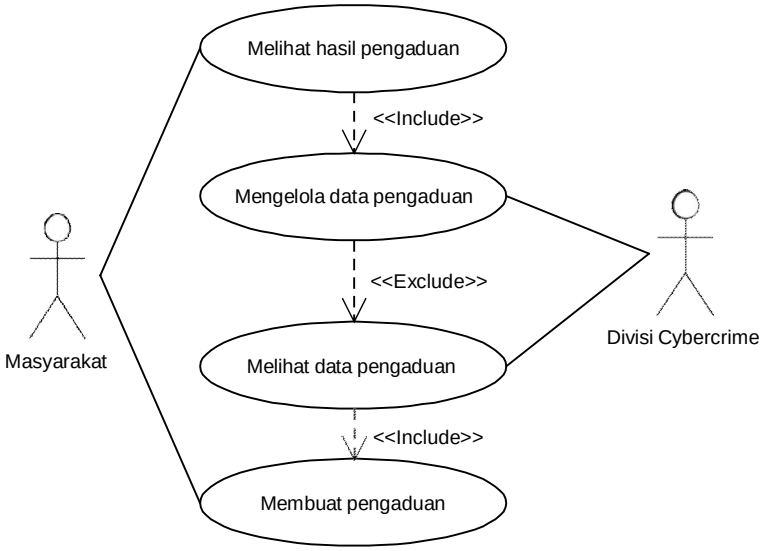
Gambar 3.2 Perancangan Arsitektur Sistem

Modelling Quick Design

Pada tahapn ini, pemodelan perencanaan meliputi perancangan *use case diagram*, *Conceptual Data Model* (CDM) atau *database*, dan perancangan tatap muka (*interface*) aplikasi. Adapun perancangan pemodelan tersebut adalah dijelaskan pada sub pokok bahasan berikut.

Use Case Diagram

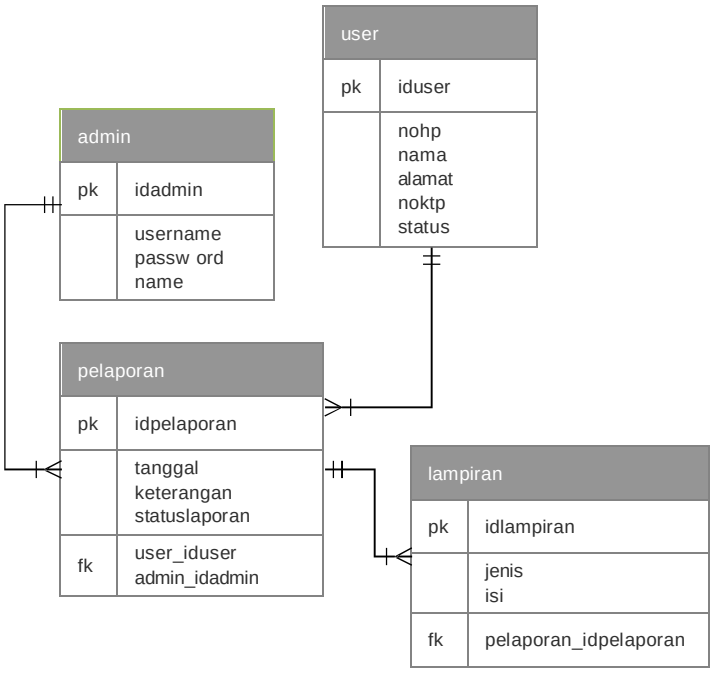
Perancangan *use case diagram* pada aplikasi yang dibangun adalah seperti pada Gambar 3.3. Aplikasi yang dibangun memiliki 2 aktor, yaitu divisi *cybercrime* dan masyarakat. Divisi *cybercrime* dapat melihat data pengaduan dari masyarakat dan mengtelola data pengaduan tersebut seperti tindak lanjut dari pengaduan yang diterima. Sedangkan masyarakat hanya dapat membuat data pengaduan dan melihat data hasil tindak lanjut dari pengaduan tersebut.



Gambar 3.3 Perancangan *Use Case Diagram*

***Conceptual Data Model* (CDM)**

Perancangan CDM atau biasa disebut dengan *database* pada aplikasi yang dibangun terdiri dari 4 tabel, yaitu tabel admin, tabel *user*, tabel pelaporan, dan tabel lampiran. Tabel admin dan tabel *user* berelasi dengan tabel pelaporan. Tabel pelaporan kemudian direlasikan dengan tabel lampiran. Adapun perancangan *database* adalah seperti pada Gambar 3.4.



Gambar 3.4 Perancangan CDM atau *Database*

Adapun kamus data dari tiap-tiap tabel pada perancangan CDM di atas adalah sebagai berikut :

a. Tabel Admin

Nama tabel : Admin
Primary key : Idadmin
Foreign key : -
Fungsi : menyimpan data admin/divisi *cybercrime*

Tabel 3.1 Kamus Data Tabel Admin

field_name	***Type***	***length***	**keterangan**
idadmin	*Int*	*default*	id admin
username	*Varchar*	6	*username*
password	*Varchar*	6	*password*
nama	*Varchar*	50	nama admin

b. Tabel *User*

Nama tabel : *User*
Primary key : Iduser
Foreign key : -
Fungsi : menyimpan data *user*/masyarakat

Tabel 3.2 Kamus Data Tabel *User*

field_name	***type***	***Length***	**keterangan**
iduser	*int*	*Default*	id user
nohp	*varchar*	16	nomor hp
nama	*varchar*	50	nama pengguna
alamat	*tinytext*	*Default*	alamat pengguna
noktp	*varchar*	18	nomor ktp
status	*enum*	(‘0’, ‘1’, ‘2’, ‘3’)	status (menunggu verifikasi, terverifikasi, gagal verifikasi, tidak aktif)

c. Tabel Pelaporan

Nama tabel : Pelaporan
Primary key : Idpelaporan
Foreign key : admin_idadmin
user_iduser
Fungsi : menyimpan data pengelolaan pengaduan

Tabel 3.3 Kamus Data Tabel Pelaporan

field_name	***type***	***length***	**keterangan**
idpelaporan	*int*	*Default*	id pengaduan
tanggal	*datetime*	*Default*	tanggal pengaduan
keterangan	*text*	*Default*	isi pengaduan
statuslaporan	*enum*	(‘0’,’1’)	status laporan (menunggu, sudah diterima)
user_iduser	*int*	*Default*	id *user*
admin_idadmin	*int*	*Default*	id admin

d. Tabel Lampiran

Nama tabel : Lampiran
Primary key : Idlampiran
Foreign key : pelaporan_idpelaporan
Fungsi : menyimpan data isi pengaduan termasuk *link* dan foto bukti

Tabel 3.4 Kamus Data Tabel Lampiran

field_name	***type***	***length***	**keterangan**
idlampiran	*int*	*default*	id lampiran
jenis	*enum*	*'File', 'Link'*	jenis lampiran bukti
isi	*text*	*default*	isi pengaduan
pelaporan_idpelaporan	*int*	*default*	id pelaporan

***Interface* Aplikasi**

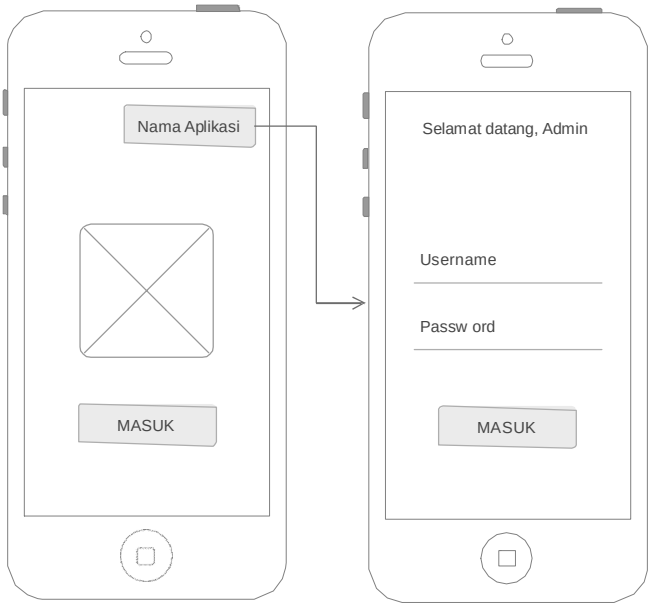
Perancangan *interface* aplikasi layanan pengaduan *cybercrime* berbasis Android terdiri dari 2 hak akses, yaitu akses divisi *cybercrime* (admin) dan akses masyarakat. Adapun perancangan *interface* dari masing-masing hak akses adalah sebagai berikut :

a. *Interface* Akses Admin

Interface aplikasi dengan hak akses admin terdiri dari beberapa menu, yaitu *login*, menu utama, dan pengelolaan pengaduan. Adapun perancangan *interface* dari masing-masing menu dengan hak akses admin adalah sebagai berikut :

1. *Interface Login*

Login dirancang untuk dapat memverifikasi hak akses admin. Jika *username* dan *password* yang dimasukkan *valid* dengan yang disimpan ke dalam *database*, maka sistem akan menampilkan menu utama aplikasi sesuai dengan hak akses yang digunakan. Perancangan *interface login* akses admin adalah seperti pada Gambar 3.5.

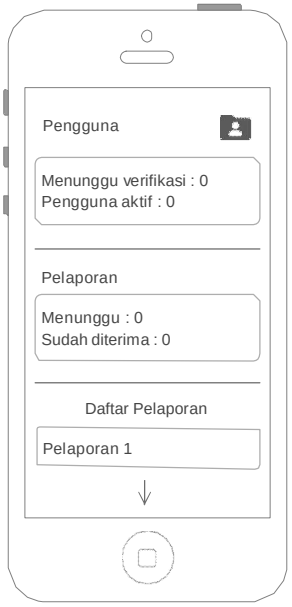


Gambar 3.5 Perancangan Interface *Login* Akses Admin

2. *Interface* Menu Utama

Menu utama dirancang untuk ditampilkan ketika sistem dapat memverifikasi hak akses admin. Menu ini berisikan informasi pengguna,

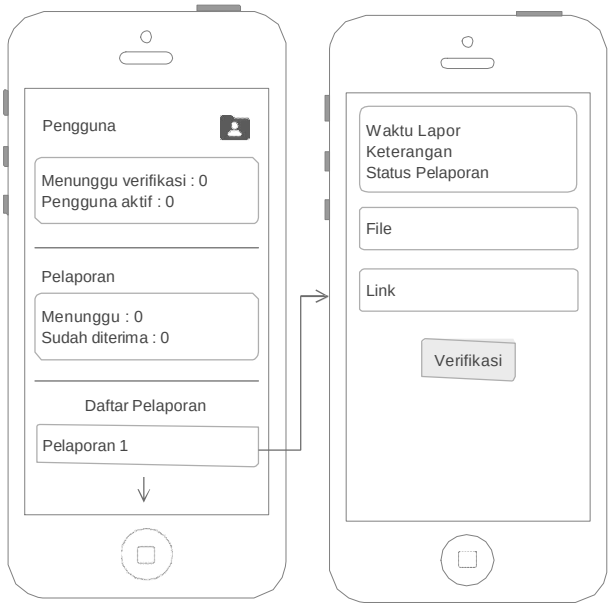
pelaporan/pengaduan, serta daftar pelaporan/pengaduan. Perancangan *interface* menu utama akses admin adalah seperti pada Gambar 3.6.



Gambar 3.6 Perancangan *Interface* Menu Utama Akses Admin

3. *Interface* Pengelolaan Pengaduan

   Interface ini dirancang untuk dapat dipergunakan oleh admin dalam mengelola data pengaduan seperti memverifikasi pengaduan cybercrime. Perancangan *interface* pengelolaan pengaduan akses admin adalah seperti pada Gambar 3.7.



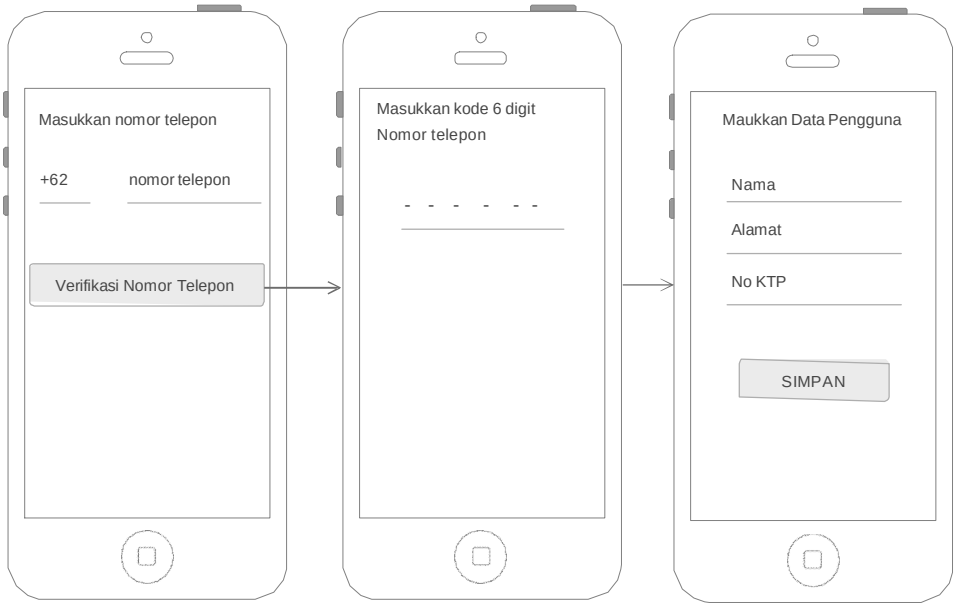
Gambar 3.7 Perancangan *Interface* Pengelolaan Pengaduan Akses Admin

b. *Interface* Akses Masyarakat (Publik)

Interface aplikasi dengan hak akses masyarakat terdiri dari beberapa menu, yaitu pendaftaran, menu utama, pengaduan, dan riwayat pelaporan. Adapun perancangan *interface* dari masing-masing menu dengan hak akses masyarakat atau publik adalah sebagai berikut :

1. *Interface* Pendaftaran

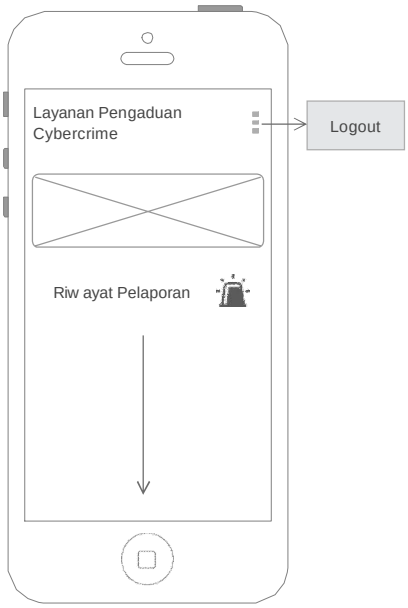
   Perancangan *interface* pendaftaran akun akses masyarakat/publik adalah seperti pada Gambar 3.8. Masyarakat mendaftar akun menggunakan nomor telepon (*handphone*).



Gambar 3.8 Perancangan *Interface* Pendaftaran Akses Masyarakat

2. *Interface* Menu Utama

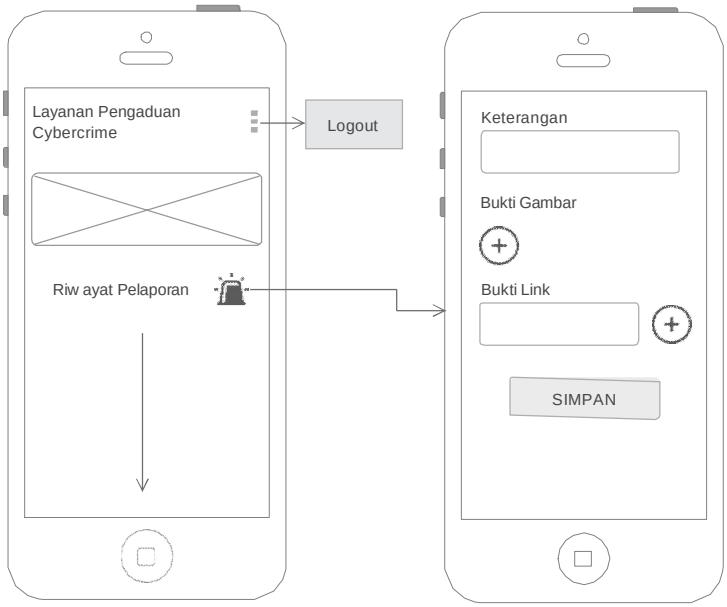
   Menu utama akses masyarakat dirancang untuk ditampilkan jika telah berhasil mendaftar. Adapun perancangan *interface* menu utama akses masyarakat adalah seperti pada Gambar 3.9.



Gambar 3.9 Perancangan *Interface* Menu Utama Akses Masyarakat

3. *Interface* Pengaduan

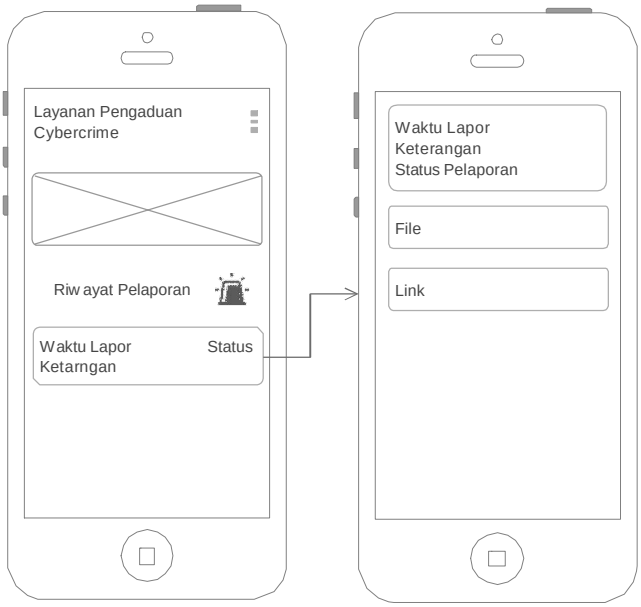
   Menu ini dirancang untuk dapat dipergunakan oleh masyarakat dalam melaporkan tindak kejahatan *cybercrime* dengan mengisi *form* yang telah disediakan seperti gambar dan *link* bukti beserta isi keterangannya. Adapun perancnagan *interface* pengaduan akses masyarakat adalah seperti pada Gambar 3.10.



Gambar 3.10 Perancangan *Interface* Pengaduan Akses Masyarakat

4. *Interface* Riwayat Pelaporan

   Menu ini dirancang untuk dapat digunakan oleh masyarakat dalam melihat data riwayat pengaduan. Adapun perancnagan *interface* riwayat pelaporan akses masyarakat adalah seperti pada Gambar 3.11.



Gambar 3.11 Perancangan *Interface* Riwayat Pelaporan Akses Masyarakat

Kebutuhan Perangkat Keras dan Lunak

Proses pembuatan aplikasi yang dibangun tidak terlepas dari *tools* pendukung dalam pembuatannya. Adapun *tools* pendukung yang dimaksud adalah perangkat lunak dan perangkat keras. Perangkat lunak dan perangkat keras yang digunakan adalah sebagai berikut:

a. Perangkat Lunak

Perangkat lunak yang digunakan dalam pembuatan aplikasi layanan penganduan tindak kejahatan *cybercrime* berbasis Android ini adalah sebagai berikut :

1. Sistem operasi Windows 10 64 bit.
2. Aplikasi perancangan/pemodelan sistem : Edraw Max
3. Aplikasi *database* : MySQL *Workbech*
4. Aplikasi pembuatan program : Android Studio
5. Server : Node.js
6. JDK terbaru
7. *Smartphone* Android minimal versi 8.0

b. Perangkat Keras

Perangkat keras yang digunakan dalam pembuatan aplikasi layanan penganduan tindak kejahatan *cybercrime* berbasis Android ini adalah laptop atau *Personal Computer* dengan spesifikasi sebagai berikut :

1. RAM 4 GB jika tidak menggunakan emulator Android (percobaan langsung menggunakan *smartphone* Android)
2. RAM 8 GB atau lebih jika menggunakan emulator Android untuk menjalankan atau testing pemograman
3. Hardisk minimal 160 GB jika hanya terpasang sistem operasi, DB *Browser* MySQL, dan Android Studio saja. Disarankan di atas 160 GB, semakin besar kapasitas hardisk semakin baik
4. 1280 x 800 minimum resolusi layar
5. Prosesor *intel core* atau amd atau prosessor setaranya
6. *Smartphone* Android

Perencanaan Uji Coba *Blackbox*

Aplikasi akan diuji coba menggunakan metode black box testing. Adapun jenis ujicoba yang akan digunakan adalah sebagai berikut :

a. Functional Testing

1. Unit Testing

Menguji fungsi tiap menu aplikasi.

2. Integration Testing

Menguji menu pengaduan akses masyarakat yang berinteraksi dengan menuutama akses admin serta menu pengelolaan pelaporan akses admin.

b. Non Functional Testing

1. Message Testing

Pengujian dilakukan pada pemberitahuan login berhasil/gagal, notifikasi pengaduan dan pesan-pesan lainnya yang terdapat pada fungsi menu aplikasi.

2. *Instalation Testing*

   Mneguji pemasangan aplikasi pada versi Android yang berbeda.