

SISTEM INFORMASI KASUS PELAPORAN
CYBER CRIME



Disusun Oleh:

N a m a : Liyandi Caesar Novaldy

NIM : 14523194

PROGRAM STUDI TEKNIK INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA

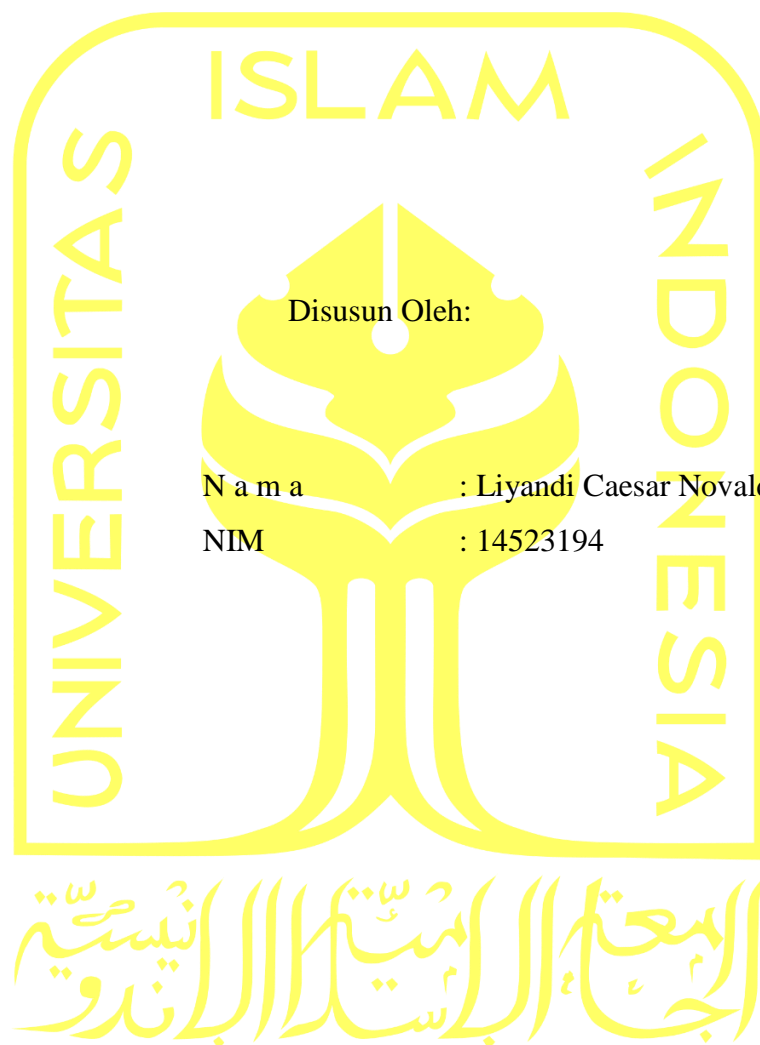
2018

HALAMAN PENGESAHAN DOSEN PEMBIMBING

SISTEM INFORMASI KASUS PELAPORAN

CYBER CRIME

TUGAS AKHIR



Yogyakarta, 24 September 2018

Pembimbing,

(Yudi Prayudi S.Si., M.Kom.,)

HALAMAN PENGESAHAN DOSEN PENGUJI

SISTEM INFORMASI KASUS PELAPORAN
CYBER CRIME

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Teknik Informatika di Fakultas Teknologi Industri Universitas Islam Indonesia
Yogyakarta, 5 November 2018

Tim Penguji

Yudi Prayudi S.Si., M.Kom. _____

Anggota 1

Ari Sujarwo S.Kom., M.I.T. _____

Anggota 2

Andhik Budi Cahyono S.T. M.T. _____



Mengetahui,

Ketua Program Studi Teknik Informatika – Program Sarjana
Fakultas Teknologi Industri
Universitas Islam Indonesia

(Dr. Raden Teduh Dirgahayu, S.T., M.Sc.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Liyandi Caesar Novaldy

NIM : 14523194

Tugas akhir dengan judul:

SISTEM INFORMASI KASUS PELAPORAN *CYBER CRIME*

Saya menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila dikemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung segala resiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 24 September 2018

(Liyandi Caesar Novaldy)

HALAMAN PERSEMBAHAN

Dengan segala usaha dan perjuangan saya serta doa yang tiada henti saya panjatkan kepada Allah S.W.T, tugas akhir ini saya persembahkan kepada orang tua saya yang selalu mendukung saya dengan penuh kasih sayang.

HALAMAN MOTO

“...do what is beautiful. Allah loves those who do what is beautiful. ...”

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur saya ucapkan kepada ALLAH SWT Tuhan semesta alam, yang telah memberikan taufiq beserta hidayahnya sehingga saya dapat menyelesaikan laporan tugas akhir ini.

Tugas akhir ini dibuat sebagai salah satu syarat yang harus dipenuhi untuk memperoleh gelar sarjana di Jurusan Teknik Informatika Universitas Islam Indonesia. Adapun tugas akhir saya mengenai Sistem Informasi Kasus Pelaporan *Cyber crime*.

Pelaksanaan Tugas Akhir ini merupakan salah satu mata kuliah wajib dari jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia dan juga merupakan sarana bagi saya untuk menambah wawasan serta pengalaman dalam menerapkan keilmuan, sesuai dengan yang diambil di bangku perkuliahan.

Oleh karena itu, pada kesempatan ini saya ingin menyampaikan rasa terima kasih kepada:

1. ALLAH SWT , yang telah memberikan kelancaran dalam segala pengerjaan laporan tugas akhir ini.
2. Orang tua dan keluarga atas segala doa dan dukungan selama saya melakukan tugas akhir.
3. Bapak Hendrik, S.T., M.Eng., selaku Ketua Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.
4. Bapak Yudi Prayudi S.Si., M.Kom., selaku Dosen Pembimbing Tugas Akhir di Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.
5. Bapak Lugas Winokusekti, A.Md., selaku Pelaksana Pranata Komputer di Dinas Pendidikan Kabupaten Sleman.
6. Bapak Anggaito Hadi Prabowo, S.H., S.IK, selaku Kepala Kepolisian Resor Sleman Kepala Satuan Reserse Kriminal.

7. Bapak Nuryadi, selaku anggota Reserse Kriminal di Kepolisian Resor Sleman.
8. Teman-teman Teknik Informatika yang telah mendukung dari awal sampai terselesaikannya laporan tugas akhir ini.
9. Semua teman-teman seperjuangan angkatan 2014 yang tidak bisa disebutkan satu persatu.
10. Teman-teman dari Wisma Zaitun yang telah memberikan motivasi dan semangat.
11. Teman-teman dari kota Samarinda yang telah memberikan motivasi dan semangat
12. Semua pihak terkait yang telah banyak membantu saya dalam pelaksanaan Tugas Akhir yang tidak dapat kami sebutkan satu persatu.

Saya menyadari bahwa laporan ini masih belum sempurna, karena keterbatasan kemampuan dan pengalaman. Oleh karena itu, saya mengharapkan masukan yang konstruktif serta kritik dan saran yang membangun demi kesempurnaan Laporan Tugas Akhir ini. akhir kata, saya berharap agar laporan ini dapat bermanfaat bagi semua pihak.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Yogyakarta, 28 Agustus 2018

Liyandi Caesar Novaldy

SARI

Cyber crime adalah suatu tindak kriminal yang dilakukan dengan teknologi komputer sebagai sarana kejahatannya. *Cyber crime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan teknologi internet.

Sejalan perkembangan teknologi informasi kejahatan dunia maya juga berkembang sangat cepat. Berdasarkan Distreskrimsus Polda Metro Jaya kasus kejahatan di dunia maya atau *cyber crime* menjadi kasus paling banyak yang ditangani di sepanjang 2016, setidaknya ada 1207 laporan kasus tersebut dari 1627 kasus yang ditangani oleh polisi.

Sistem informasi memegang peranan penting dalam penyampaian suatu informasi, dalam hal ini lembaga Kepolisian yang khusus dalam mengenai kejahatan dunia maya. Sistem informasi pelaporan *Cyber crime* mendukung proses penginformasian data dan pengiriman informasi mengenai segala bentuk kejahatan dunia maya. Pembangunan sistem informasi pelaporan dan jika diterapkan dengan baik maka lembaga akan memperoleh informasi yang baik, akurat dan tepat waktu sehingga bisa dilakukan tindakan yang tepat.

Sistem informasi ini dibuat sesuai dengan SOP pelaporan yang ada di Kepolisian Resor Sleman dan perancangan sistem nya menggunakan metode *waterfall*. Penelitian dilakukan di Kepolisian Resor Sleman dari mengambil data dan melakukan wawancara kepada anggota reserse kriminal yang ada di lokasi tersebut. Selanjutnya dilakukanlah pengujian untuk system yang dibangun, yaitu pengujian dengan menggunakan metode Black-Box.

Hasil dari penelitian dan pembuatan sistem informasi ini adalah terciptanya sebuah sistem informasi untuk melakukan pelaporan kasus kejahatan dunia maya sesuai dengan SOP dari Kepolisian Resor Sleman yang bernama Sistem Informasi Kasus Pelaporan *Cyber Crime*. Sistem yang dibuat nantinya akan dipakai oleh petugas Kepolisian dan pelapor.

Kata kunci: *Cyber crime*, teknologi komputer, Kepolisian.

GLOSARIUM

Waterfall	metode pengembangan perangkat lunak
Software	perangkat lunak
Hardware	perangkat keras
Entity Relationship Diagram	diagram hubungan entitas
Data Flow Diagram	diagram arus data
Login	masuk
History	riwayat
Form	formulir
Database	basis data
Online	terhubung di dunia maya
Internet fraud	penipuan internet
Cracker	orang yang masuk ke sistem orang lain
economy crime	kejahatan ekonomi
organized crime	kejahatan organisasi
money laundering	pencucian uang
hacker	peretas
e-commerce	transaksi jual beli secara elektronik
computerized	terkomputerisasi
cyberterrorism	teroris dunia maya
web page	halaman web
carding	penyalahgunaan kartu kredit
coding	sistem pengodean
testing	pengujian
maintenance	pemeliharaan
requirements	kebutuhan
source code	kode program
username	nama pengguna
password	kata sandi

primary key

foreign key

home

upload

screenshot

error

kunci utama

kunci tamu dari table lain

beranda

unggah

tangkapan layar

kesalahan

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN DOSEN PEMBIMBING	ii
HALAMAN PENGESAHAN DOSEN PENGUJI.....	iii
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR.....	iv
HALAMAN PERSEMBAHAN	v
HALAMAN MOTO	vi
KATA PENGANTAR	vii
SARI.....	ix
GLOSARIUM	x
DAFTAR ISI	xii
DAFTAR TABEL	xiv
DAFTAR GAMBAR.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Metodologi Penelitian	4
1.7 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI.....	6
2.1 Tinjauan Pustaka	6
2.2 <i>Cyber crime</i>	7
2.3 Modus Kejahatan <i>Cyber crime</i>	8
2.4 Metode Pengembangan Sistem	11
2.5 PHP (PHP: Hypertext Preprocessor).....	12
2.5.1 Kemampuan PHP	12
2.6 MySQL.....	13
2.7 Black-Box <i>Testing</i>	14
BAB III METODOLOGI	15
3.1 Pengumpulan Data	15
3.1.1 Tahapan Pelaporan <i>Cyber crime</i> yang berjalan.....	15
3.2 Analisis Kebutuhan	16
3.2.1 Analisis Kebutuhan Form.....	16
3.2.2 Analisis Kebutuhan Proses	17
3.2.3 Analisis Kebutuhan Output	17
3.2.4 Analisis Kebutuhan Perangkat Lunak	17
3.2.5 Analisis Kebutuhan Perangkat Keras	18
3.3 Perancangan Konseptual	18
3.3.1 Perancangan basis data.	19
3.3.2 Perancangan <i>Data Flow Diagram</i> (DFD)	26
3.4 Perancangan Antarmuka	31
BAB IV HASIL DAN PEMBAHASAN.....	38

4.1	Pengujian Sistem Informasi	38
4.2	Penjelasan dan <i>Screenshot</i> Program.....	44
4.3	Kelebihan dan Kekurangan Program	56
BAB V SIMPULAN DAN SARAN		58
5.1	Simpulan.....	58
5.2	Saran.....	58
DAFTAR PUSTAKA.....		59
LAMPIRAN		61

DAFTAR TABEL

Tabel 3.1 Tabel analisis kebutuhan form	17
Tabel 3.2 Tabel spesifikasi <i>software</i>	17
Tabel 3.3 Tabel spesifikasi <i>hardware</i>	18
Tabel 3.4 Tabel Petugas	21
Tabel 3.5 Tabel Jenis Kasus	21
Tabel 3.6 Tabel Pelapor	22
Tabel 3.7 Tabel Pengaduan	23
Tabel 3.8 Tabel Penanganan	25
Tabel 4.1 Pengujian Black-Box Sistem Informasi Kasus Pelaporan Cyber Crime - Admin.....	38
Tabel 4.2 Pengujian Black-Box Sistem Informasi Kasus Pelaporan Cyber Crime – Pelapor.....	40
Tabel 4.3 Pengujian Black-Box Sistem Informasi Kasus Pelaporan Cyber Crime – Petugas	41

DAFTAR GAMBAR

Gambar 2.1 Model <i>Waterfall Modified</i>	11
Gambar 3.1 Alur pelaporan <i>Cyber crime</i> yang berjalan di Kepolisian	16
Gambar 3.2 <i>Entity Relationship Diagram</i>	19
Gambar 3.3 Relasi Antar Tabel	20
Gambar 3.4 <i>Data Flow Diagram (DFD)</i> Level 0.....	26
Gambar 3.5 <i>Data Flow Diagram (DFD)</i> Level 1.....	27
Gambar 3.6 <i>Data Flow Diagram (DFD)</i> Level 2 Jenis Kasus.....	28
Gambar 3.7 <i>Data Flow Diagram (DFD)</i> Level 2 Petugas	28
Gambar 3.8 <i>Data Flow Diagram (DFD)</i> Level 2 Pelapor	29
Gambar 3.9 <i>Data Flow Diagram (DFD)</i> Level 2 Pengaduan	30
Gambar 3.10 <i>Data Flow Diagram (DFD)</i> Level 2 Penanganan	31
Gambar 3.11 Halaman <i>Login</i>	32
Gambar 3.12 Halaman Petugas	32
Gambar 3.13 Halaman Jenis Kasus	33
Gambar 3.14 Halaman Daftar Laporan	34
Gambar 3.15 Halaman Daftar Pengaduan	34
Gambar 3.16 Halaman <i>History</i> Penanganan.....	35
Gambar 3.17 Halaman Pelapor.....	36
Gambar 3.18 Halaman Daftar Laporan	36
Gambar 3.19 Halaman <i>History</i>	37
Gambar 4.1 Halaman Utama Sistem Informasi Kasus Pelaporan <i>Cyber crime</i> ..	44
Gambar 4.2 Halaman Panduan Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	45
Gambar 4.3 Halaman <i>Login</i> Sistem Informasi Kasus Pelaporan <i>Cyber crime</i> ...	46
Gambar 4.4 Halaman Daftar Sistem Informasi Kasus Pelaporan <i>Cyber crime</i> ...	46
Gambar 4.5 Halaman Pelapor Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	47
Gambar 4.6 Halaman Pengaduan Pelapor Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	48
Gambar 4.7 Halaman Data Pengaduan Pelapor Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	48

Gambar 4.8 Halaman Detail Data Pengaduan Pelapor Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	49
Gambar 4.9 Halaman Beranda Admin Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	50
Gambar 4.10 Halaman Beranda Admin Navigasi Petugas Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	50
Gambar 4.11 Halaman Beranda Admin Navigasi Jenis Kasus Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	51
Gambar 4.12 Halaman Beranda Admin Navigasi Laporan Pengaduan Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	51
Gambar 4.13 Halaman Beranda Petugas Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	52
Gambar 4.14 Halaman Beranda Petugas Navigasi Pengaduan Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	52
Gambar 4.15 Halaman Beranda Petugas Data Pengaduan Pelapor Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	53
Gambar 4.16 Halaman <i>History</i> Penanganan Pelapor Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	54
Gambar 4.17 Halaman Beranda Petugas Navigasi Data Pelapor Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	54
Gambar 4.18 Halaman Beranda Petugas Navigasi Statistik Penyelesaian Kasus Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	55
Gambar 4.19 Halaman Beranda Petugas Navigasi Statistik Jenis Kejahatan Sistem Informasi Kasus Pelaporan <i>Cyber crime</i>	56

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era modern seperti sekarang ini, perkembangan dan pemanfaatan teknologi informasi mengubah peradaban manusia secara global. Perkembangan inilah yang menyebabkan akses ke manapun tanpa batas dan menyebabkan perubahan sosial, ekonomi, maupun budaya secara signifikan.

Perkembangan teknologi membuat hidup kita menjadi lebih mudah dan praktis, Akan tetapi dalam perkembangannya, teknologi informasi bisa juga disalahgunakan untuk tindakan kejahatan dunia maya atau yang biasa kita sebut dengan *cyber crime*. *Cyber crime* adalah suatu tindak kriminal yang dilakukan dengan teknologi komputer sebagai sarana kejahatannya. *Cyber crime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan teknologi internet (Daryono & Sugiantoro, 2017).

Sejalan perkembangan teknologi informasi kejahatan dunia maya juga berkembang sangat cepat. Berdasarkan Distreskrimsus Polda Metro Jaya kasus kejahatan *Cyber crime* menjadi kasus yang paling banyak ditangani di sepanjang 2016, setidaknya ada 1207 laporan kasus tersebut dari 1627 kasus yang ditangani oleh Polisi (Elise Dwi Ratnasari, 2016).

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan *cyber law*. *Cyber law* muncul mengingat kejahatan dunia maya banyak dilakukan melalui internet dan sistem komunikasi baik lingkup lokal maupun global oleh perorangan maupun kelompok. Dari informasi tersebut masih banyak orang yang mengalami kejahatan *Cyber crime* karena ketidaktahuan untuk melaporkan kepihak yang berwajib yang menangani kasus kejahatan *Cyber crime* dan keengganan mereka untuk melaporkan karena model pelaporan yang masih konvensional (Agus & Riskawati, 2016).

Sistem informasi memegang peranan penting dalam penyampaian suatu informasi, dalam hal ini lembaga Kepolisian yang khusus dalam mengenai kejahatan dunia maya. Sistem informasi pelaporan *Cyber crime* mendukung proses penginformasian data dan pengiriman informasi mengenai segala bentuk kejahatan dunia maya. Pembangunan sistem informasi pelaporan, jika diterapkan dengan baik maka lembaga akan memperoleh informasi yang tersampaikan dengan baik, akurat dan tepat waktu sehingga bisa dilakukan tindakan yang tepat. Baik dalam maksud sistem informasi mempunyai manfaat bagi pemakainya, akurat dalam sumber informasi yang diberikan hingga penerimaan informasi supaya terhindar dari kesalahan, dan tepat waktu dalam melakukan proses pengolahan data dan informasi yang datang pada penerima tidak boleh terlambat.

Berdasarkan permasalahan di atas, dibuatlah Sistem Informasi Pelaporan Kasus *Cyber crime* yang dapat diakses dimana saja dan kapan saja oleh petugas maupun pelapor, serta diharapkan dapat mempermudah pelapor untuk melaporkan kasus yang dialaminya dengan cara menghemat sumber daya, waktu dan mendapatkan penanganan yang cepat.

1.2 Rumusan Masalah

Berdasarkan latar belakang pada tugas akhir ini, maka dirumuskan permasalahan pada Sistem Informasi Pelaporan Kasus *Cyber crime*, antara lain:

- a. Bagaimana merancang dan membangun sebuah sistem informasi pelaporan kasus *Cyber crime* sesuai dengan standar untuk pelaporan?
- b. Bagaimana mengelola dan mengimplementasikan Pelaporan Kasus *Cyber crime* menjadi sebuah sistem informasi yang dapat membantu pelapor melakukan pelaporan?

1.3 Batasan Masalah

Berdasarkan rumusan masalah di atas, maka adanya pembatasan masalah sehingga ruang lingkup tidak terlalu melebar. Berikut batasan masalah yang akan dilakukan, antara lain:

- a. Sistem yang dibuat hanya dapat memberikan informasi, tidak sampai ke level pemberian keputusan.
- b. Sistem yang dibuat hanya memberikan formulir berdasarkan form yang sesuai dengan Standar Operasional Prosedur KEPOLISIAN RESOR Sleman dalam hal sistem pelaporan.
- c. Hanya administrator yang dapat mengelola sistem informasi ini secara keseluruhan.
- d. Sistem Informasi Pelaporan Kasus *Cyber crime* ini hanya memiliki beberapa user yang berwenang seperti kasubdit atau kanit, dan penyidik untuk memeriksa laporan yang masuk dari pelapor lalu setelah itu didisposisi oleh mereka dan informasi yang diperlukan untuk autentikasi tersimpan di *database*.
- e. Sistem ini dibangun dengan berbasis web dengan bahasa pemrograman PHP dan basis data MySQL.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah membantu pihak Kepolisian dalam melakukan pelaporan dengan sistem yang mempunyai standar untuk pelaporan kejadian (*incident reporting*) berdasarkan kasus *Cyber crime*, selain itu juga dapat memberikan kemudahan kepada pihak Kepolisian maupun pelapor untuk melakukan pelaporan kejadian dan penanganan secara *online*.

1.5 Manfaat Penelitian

Adapun manfaat penelitian ini adalah:

- a. Sistem informasi dapat membantu bagian penindakan *Cyber crime* dalam memproses kejadian tindak pidana kejahatan dunia maya.

- b. Sistem informasi dapat memberikan informasi terbaru dengan cepat dan efisien atas kasus yang dikerjakan kepada pihak yang berwajib dalam informasi pelaporan yang dilakukan oleh masyarakat atau pelapor.
- c. Sistem informasi mampu memberikan informasi pendukung terkait dengan pengambilan pilihan penanganan.

1.6 Metodologi Penelitian

Metode dalam penelitian untuk membangun sistem informasi pelaporan kasus *Cyber crime* ini menggunakan metode *waterfall*. Metode *waterfall* adalah suatu proses pemodelan sistem informasi secara sistematis dan urut dimulai dari analisa kebutuhan, perancangan, implementasi, dan pengujian sistem. Pemodelan sistem dengan metode ini sangat cocok digunakan untuk sistem yang tetap terjaga karena pengembangannya terstruktur. Melihat keuntungan dari metode *waterfall* maka penulis memutuskan untuk menggunakannya dimana pengaplikasian menggunakan model ini mudah, kelebihan dari model ini juga ketika semua kebutuhan sistem dapat didefinisikan secara utuh dan benar dari awal, maka metode *waterfall* dapat berjalan dengan baik.

a. Analisis Kebutuhan

Semua kebutuhan baik data, *software*, dan *hardware* harus didapatkan dalam fase ini termasuk di dalamnya kegunaan dan batasannya.

b. Perancangan

Tujuan dari tahap ini adalah merancang/memberi gambaran alur program, *database*, dan tampilan yang akan dikerjakan pada tahap berikutnya.

c. Implementasi

Setelah perancangan selesai selanjutnya yaitu implementasinya. Tahap ini merupakan penerjemahan perancangan dalam bahasa yang dikenali komputer.

d. Pengujian

Tahap yang dapat dikatakan sebagai tahapan akhir dalam pembuatan sebuah sistem. Setelah selesai tahapan-tahapan sebelumnya maka yang

terakhir yaitu pengujian untuk mengetahui apakah sistem yang dibuat telah sesuai dengan desainnya dan masih terdapat kesalahan atau tidak.

1.7 Sistematika Penulisan

Sistematika penulisan untuk menggambarkan singkat organisasi penulisan laporan, serta isi dari setiap bagiannya dapat dijelaskan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi uraian tentang latar belakang, rumusan masalah, batasan masalah, manfaat penelitian, tujuan penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi uraian teori dasar yang menjelaskan tentang sistem informasi, *Cyber crime*, dan tinjauan pustaka yang digunakan sebagai acuan mengerjakan tugas akhir.

BAB III METODOLOGI

Bab ini berisi uraian tentang langkah-langkah penyelesaian masalah yaitu dari analisis kebutuhan, perancangan, dan implementasi.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi uraian tentang hasil dari penyelesaian masalah yaitu sistem informasi pelaporan kasus *Cyber crime* dan pembahasannya.

BAB V SIMPULAN DAN SARAN

Bab ini berisi uraian tentang simpulan-simpulan yang merupakan rangkuman dari hasil analisis kinerja pada bagian sebelumnya dan saran-saran yang perlu diperhatikan.

BAB II

LANDASAN TEORI

2.1 Tinjauan Pustaka

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah metode *Waterfall* untuk mendapatkan data yang diperlukan dalam penelitian ini. Sistem informasi ini terdiri dari 10 (sepuluh) form yaitu antara lain: form laporan tindak pidana, form jadwal piket, form pelapor, form terlapor, form saksi, form tindak pidana, form penyelidikan, form penyidik, form surat bukti penyidikan, dan form hasil penyidikan. Simpulan yang diperoleh adalah sistem ini dapat membantu dalam mempercepat pembuatan yaitu laporan berkas tindak pidana, laporan penyidik, dan laporan hasil penyidikan (Irawan, 2015).

Pengelolaan laporan Kepolisian bertujuan untuk memudahkan pembuatan laporan secara rinci dan sesuai standar. Hasil dari sistem pengelolaan laporan Kepolisian jika dibuat maka akan dapat membantu petugas dalam mengelola data laporan Kepolisian, pencatatan laporan, pencarian data, serta dapat menyeragamkan format laporan Kepolisian dan aplikasi pengelolaan laporan Kepolisian ini memudahkan petugas Serse dalam pengambilan data laporan tindak pidana (Irawan, 2015).

Sistem informasi yang dibuat menggunakan bahasa pemrograman PHP yang didukung teknologi AJAX. Dalam penelitian ini dibuatlah program sistem aplikasi pencatatan tindak kejahatan yang terjadi di Sektor Tegal Selatan. Hasil dari sistem informasi tersebut menghasilkan pengolahan data kejahatan yang bisa mengelola data kasus kejahatan, data tahanan, data pencarian orang (DPO), data tingkat kejahatan di lingkungan sektor tegal selatan, lalu ada juga data kasus kejahatan, data tahanan, data pencarian orang (DPO), dan data berita acara pemeriksaan (BAP) yang diselesaikan (Siswanto, Rochim, & Somantri, 2012).

2.2 *Cyber crime*

Perkembangan teknologi komputer juga menghasilkan berbagai bentuk kejahatan komputer di dunia maya yang kemudian melahirkan istilah baru yang dikenal dengan *Cyber crime*, *Internet fraud*, dan lain sebagainya. Sebagian besar dari perbuatan *Cyber crime* dilakukan oleh seseorang yang sering disebut dengan *cracker* (Adrio, 2010).

Kegiatan hacking atau cracking yang merupakan salah satu bentuk *cyber crime* yang dimana hal telah membentuk opini umum para pemakai internet bahwa *cyber crime* adalah perbuatan yang sangat merugikan orang banyak dan perlu dibuatnya undang-undang yang mengatur hal tersebut. Kejahatan tersebut juga pantas ada hukumannya bagi yang melanggar ketentuan dan aturan. Para korban yang terkena dampak dari aksi tersebut memberikan stigma atau pernyataan bahwa bahwa *cracker* dan *hacker* adalah seorang penjahat.

“*Cyber crime*” adalah salah satu bentuk atau dimensi yang baru dari kejahatan masa kini yang mendapat perhatian luas di seluruh dunia. Beberapa julukan/sebutan lainnya yang cukup keren diberikan kepada kejahatan baru ini dalam berbagai tulisan, antara lain sebagai “kejahatan dunia maya”.

“*Cyber crime*” selanjutnya merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luar biasa bagi seluruh bidang kehidupan modern saat ini. Sehubung dengan kekhawatiran akan ancaman dan bahaya *Cyber crime* ini, karena berkaitan erat dengan “*economy crime*” dan “*organized crime*”. Jadi *Cyber crime* dapat dikategorikan sebagai perbuatan yang melanggar dan melawan hukum yang dilakukan lewat internet atau jaringan komputer yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

2.3 Modus Kejahatan *Cyber crime*

- a. *Unauthorized Access to Computer Sistem and Service* (Akses tidak sah ke sistem komputer dan layanan)

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud menyabotase ataupun mencuri informasi penting dan rahasia yang dimiliki oleh korban. Tetapi, ada juga yang melakukannya hanya untuk mencari kesenangan dan mencari tantangan untuk mencoba keahlian yang dimilikinya dengan menembuh suatu sistem yang memiliki tingkat keamanan yang tinggi. Kejahatan ini sering terjadi dan semakin marak dengan berkembangnya teknologi internet.

- b. *Illegal Contents* (isi tidak sah)

Kejahatan dengan memasukkan data atau informasi secara online dengan cara yang tidak benar, tidak etis, dan dapat dianggap sebagai pelanggaran hukum. Contohnya adalah memuat berita bohong, fitnah atau sara yang bisa berdampak menghancurkan martabat atau harga diri dari pihak lain. Selanjutnya ada juga pornografi, informasi rahasia suatu negara, transaksi jual beli barang terlarang, agitasi dan propaganda untuk melawan suatu pemerintahan, dan lain sebagainya.

- c. *Data Forgery* (pemalsuan data)

Kejahatan dengan memalsukan data pada dokumen penting yang tersimpan melalui internet atau jaringan komputer. Biasanya kejahatan ini ditujukan pada dokumen e-commerce dengan membuatnya seolah-olah terjadi "salah ketik" yang pada akhirnya menguntungkan pelaku perorangan atau organisasi.

- d. *Cyber Espionage* (spionase cyber)

Kejahatan yang memanfaatkan internet sebagai media kegiatan mata-mata terhadap pihak lain, dengan memasuki atau membobol secara paksa jaringan komputer target. Kejahatan ini biasa ditujukan terhadap

saingan bisnis atau politik yang dokumen-dokumen atau data pentingnya tersimpan di sistem yang terkomputerisasi (*computerized*).

e. *Cyber Sabotage and Extortion* (sabotase dan pemerasan)

Kejahatan ini dilakukan dengan membuat perusakan, penghacuran atau gangguan pada suatu data, program yang ada dikomputer dan sistem jaringan komputer yang telah terhubung dengan internet. Kejahatan ini dilakukan dengan menyusupkan secara diam-diam suatu virus komputer atau program tertentu, sehingga program atau sistem komputer tidak dapat berjalan secara semestinya atau tidak dapat digunakan atau berjalan sesuai dengan kehendak pelaku. Dalam beberapa kasus yang terjadi, pelaku kejahatan tersebut berpura-pura atau menawarkan dirinya kepada korban untuk memperbaiki data yang disabotase oleh pelaku sebelumnya demi keuntungan pelaku. Biasanya keuntungan yang didapat pelaku adalah bayaran. Kejahatan inipun sering disebut juga dengan *cyberterrorism*.

f. *Offense against Intellectual Property* (kejahatan terhadap properti intelektual)

Kejahatan ini ditujukan terhadap HAKI (Hak atas Kekayaan Intelektual) yang dimiliki oleh pihak lain di dalam jaringan komputer atau internet. Sebagai contoh peniruan suatu web page atau situs yang tampilannya maupun fitur dari luar dalamnya sama. Padahal situs tersebut sudah dimiliki oleh orang lain.

g. *Infringements of Privacy* (pelanggaran privasi)

Kejahatan ini ditujukan terhadap informasi seseorang atau pihak tertentu yang merupakan informasi yang sangat pribadi dan sangat dirahasiakan. Kejahatan ini biasanya ditujukan terhadap data pribadi seseorang yang tersimpan pada formulir-formulir yang pernah dimasukkan korban secara *online* lalu tersimpan di internet atau komputer, yang apabila diketahui oleh pihak yang tidak bertanggung jawab dapat merugikan korban secara immateril maupun materil, seperti nomor ATM, kartu kredit, PIN ATM, KTP, Kartu Keluarga, *password* media sosial dan lain-lain.

h. Cracking

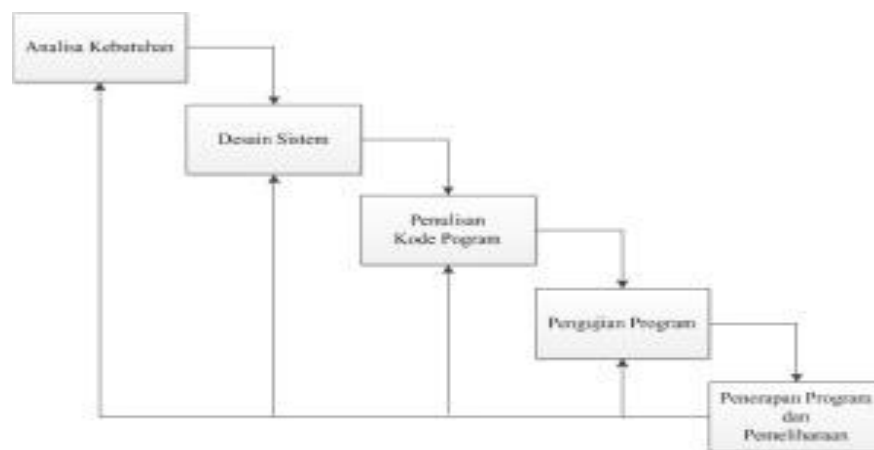
Kejahatan dengan menggunakan teknologi komputer sebagai medianya yang dilakukan untuk merusak sistem keamanan suatu sistem komputer lalu melakukan pencurian, tindakan illegal yang merugikan pihak tertentu. Biasanya korbannya adalah pengembang *software* berbayar, lisensi berbayar, maupun game berbayar. Kita juga sering salah menafsirkan antara *hacker* dan *cracker*, dimana *hacker* sendiri selalu mendapat julukan negatif, padahal *hacker* adalah seseorang yang hobi memprogram dan percaya bahwa suatu informasi adalah sesuatu yang sangat berharga yang tidak boleh dipublikasikan dan bersifat rahasia.

i. Carding

Kejatan dengan menggunakan internet atau teknologi komputer untuk melakukan transaksi dengan menggunakan kartu kredit orang lain secara illegal dengan menembus keamanan pada suatu situs, sehingga dapat merugikan orang tersebut secara materil ataupun non materil. Biasanya kejahatan carding terjadi pada situs *e-commerce* yang menyimpan data kartu kredit.

2.4 Metode Pengembangan Sistem

Metode pengembangan perangkat lunak dengan model *Waterfall modified* merupakan metode pengembangan perangkat lunak yang sistematis. Pendekatan sekuensial dimulai dari level sistem kemudian analisa, desain sistem, *coding*, *testing* dan *maintenance* (Pressman, 2015).



Gambar 2.1 Model *Waterfall Modified*

Sumber: (Pressman, 2015)

a. Perekayasaan Sistem/Informasi

Perekayasaan dan analisa sistem bertujuan menentukan *requirements* yang diperoleh dari level atas pada tahap analisa dan desain. Perekayasaan informasi bertujuan untuk mengidentifikasi *requirements* pada level strategi bisnis.

b. Analisa Kebutuhan Perangkat Lunak

Proses pengidentifikasian *requirements* lebih difokuskan pada perangkat lunak.

c. Desain

Desain perangkat lunak terdiri dari atas beberapa langkah, yaitu: desain struktur data, desain arsitektur perangkat lunak, representasi antarmuka serta desain algoritma detail.

d. *Coding*

Proses menterjemahkan algoritma detail hasil desain yang dibuat ke dalam suatu bentuk yang dapat dimengerti oleh mesin (komputer).

e. *Testing*

Pengujian yang dilakukan pada sistem yaitu pengujian logika internal dari program dan pengujian terhadap sistem yang dibuat.

f. *Maintenance*

Proses pemeliharaan perangkat lunak dan keseluruhan sistem.

2.5 PHP (PHP: Hypertext Preprocessor)

PHP (*Hypertext Preprocessor*) merupakan bahasa berbentuk *skript* yang ditempatkan dalam *server* dan diproses di *server*. Hasilnya akan dikirimkan ke klien, dengan menggunakan browser. Secara khusus PHP dirancang untuk membentuk aplikasi web dinamis, yaitu dapat membentuk suatu tampilan berdasarkan permintaan yang dibuat. Misalnya, dapat menampilkan isi dari *database* ke halaman web. Prinsip PHP mempunyai fungsi yang sama dengan *script-script* seperti ASP (*Active Server Page*), *Cold Fusion*, ataupun *Perl* (Achmad, 2016).

2.5.1 Kemampuan PHP

PHP secara mendasar dapat mengerjakan semua yang dapat dikerjakan oleh program CGI, seperti mendapatkan hasil dari form, menghasilkan isi halaman web yang dinamik, dan menerima cookies. Kemampuan PHP yang paling diandalkan dan signifikan adalah dukungan kepada banyak *database*. Membuat halaman web yang menggunakan data dari *database* dengan sangat mudah dapat dilakukan. *Database* yang didukung oleh PHP diantaranya: AdabasD, dBase, Empress, FilePro, FrontBase, Hyperwave, IBM DB2, informix, Ingres, Interbase, MSQL, Direct MS SQL, MySQL, ODBC, Oracle (OC17 dan OC18), Ovrimos, PostgreSQL, Solid, Sqlite, Sybase, Velocis dan Unix DBM.

PHP juga mendukung untuk berkomunikasi dengan layanan lain menggunakan protocol IMAP, SNMP, NNTP, POP3, HTTP dan masih banyak

lagi. PHP dalam pemrogramannya juga dapat membuka soket jaringan secara mentah dan berinteraksi dengan menggunakan protocol lainnya (Achmad, 2016).

2.6 MySQL

My Structured Query Language (MySQL) merupakan sebuah perangkat lunak yang tergolong sebagai DBMS (*Database Management Sistem*) yang bersifat Open Source. Open Source menyatakan bahwa *software* ini dilengkapi dengan *source code* (kode yang dipakai untuk membuat MySQL), selain itu tentu saja bentuk executable-nya atau kode yang dapat dijalankan secara langsung dalam sistem operasi, dan bisa diperoleh dengan cara mendownload (mengunduh) di internet secara gratis. Sebagai *software* DBMS, MySQL memiliki sejumlah fitur seperti: *multiplatform*, andal, cepat, dan mudah digunakan, jaminan keamanan akses, mendukung perintah SQL (Solichin, 2010).

MySQL memiliki banyak sekali keistimewaan. Berikut ini beberapa keistimewaan/keunggulan yang dimiliki oleh MySQL:

- a. *Portability*, dapat berjalan stabil pada berbagai sistem operasi.
- b. *Open Source*, dapat digunakan secara gratis.
- c. *Multi User*, dapat digunakan oleh banyak user dalam waktu yang bersamaan tanpa mengalami masalah.
- d. *Performance Tuning*, memiliki kecepatan dalam menangani query sederhana, dengan kata lain dapat memproses lebih banyak SQL per satuan waktu.
- e. *Column Type*, memiliki tipe kolom yang sangat kompleks.
- f. *Command dan Functions*, memiliki operator dan fungsi secara penuh yang mendukung SELECT dan WHERE dalam query.
- g. *Security*, memiliki beberapa lapisan keamanan seperti level subnetmask, nama host, dan izin akses user dengan sistem perizinan yang mendetail secara *password*.
- h. *Scalability dan Limits*, mampu menangani *database* dalam skala besar, dengan jumlah record lebih dari 50 juta dan 60 juta table serta 5 miliar baris.
- i. *Connectivity*, dapat melakukan koneksi dengan client menggunakan protocol TCP/IP, Unix soket (Unix), atau Named Pipes (NT).

- j. *Localisation*, dapat mendekeksi pesan kesalahan (error code) pada client dengan menggunakan lebih dari 20 bahasa.
- k. *Interface*, memiliki antarmuka terhadap berbagai aplikasi dan bahasa pemrograman dengan menggunakan fungsi API (application Programming Interface).
- l. *Client dan Tools*, dilengkapi dengan berbagai tool yang dapat digunakan untuk administrasi *database*, dan pada setiap tool yang ada disertakan petunjuk *online*.
- m. *Structure Table*, memiliki struktur tabel yang lebih fleksibel dalam menangani *ALTER TABLE*, dibandingkan *database* lainnya.

2.7 Black-Box Testing

Metode Black-Box *Testing* berfokus pada spesifikasi fungsional dari perangkat lunak. Tester dapat mendefinisikan kumpulan kondisi input dan melakukan pengujian pada spesifikasi fungsional program. Tester dapat mendefinisikan kumpulan kondisi form dan melakukan pengujian pada spesifikasi fungsional program 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.

Ujicoba blackbox bukan merupakan alternatif dari ujicoba whitebox, tetapi merupakan pendekatan yang melengkapi untuk menemukan kesalahan lainnya, selain menggunakan metode whitebox.

Metode Black Box Testing cenderung untuk menemukan hal-hal berikut yaitu fungsi yang tidak benar atau tidak ada, kesalahan antarmuka (interface errors), kesalahan pada struktur data dan akses basis data, kesalahan performansi (performance errors), kesalahan inisialisasi dan terminasi. (Mustaqbal, Fajri, & Hendra, 2015).

BAB III

METODOLOGI

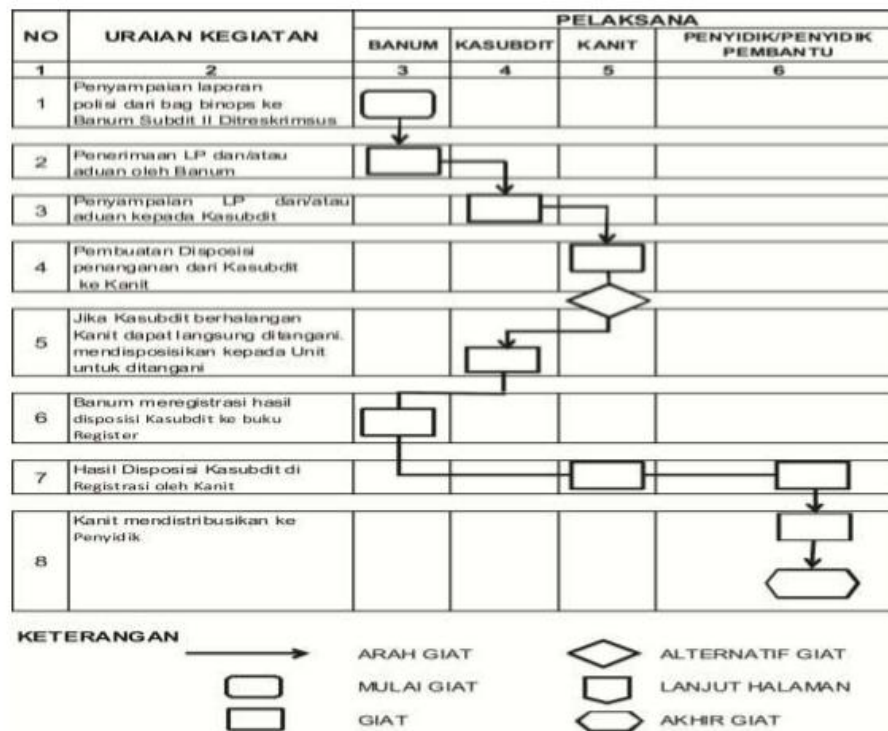
3.1 Pengumpulan Data

Metode pengumpulan data pada penelitian ini dengan menggunakan dokumen yaitu pengambilan data melalui dokumen tertulis maupun elektronik dari lembaga/institusi. Dokumen diperlukan untuk mendukung kelengkapan data yang lain. Selain pengumpulan data menggunakan dokumen, metode wawancara juga digunakan dalam penelitian ini untuk mendapatkan hasil data yang lebih terperinci dengan dilakukan sesi tanya jawab pada narasumber. Metode wawancara dengan narasumber dilakukan di Kepolisian Resor Sleman dengan Bapak Nuryadi sebagai anggota reserse kriminal.

3.1.1 Tahapan Pelaporan *Cyber crime* yang berjalan

Saat ini sistem Pelaporan yang berjalan di Kepolisian, mulai dari tingkat Kepolisian Sektor, Kepolisian Resor, Kepolisian Daerah sampai tingkat pusat khususnya yang berhubungan dengan pelaporan kejahatan. *Cyber crime* masih menjadi satu dengan tindak kejahatan kriminal yang umum dan cara pelaporan yang masih konvensional, sebagai contoh masyarakat yang mengalami korban kejahatan datang ke kantor Kepolisian membawa bukti atau dokumen yang berkaitan kasus yang dilaporkan atau diadukan pelapor membuat surat pernyataan yang menyatakan bahwa laporan tersebut belum pernah dilaporkan atau ditangani oleh polisi. Laporan atau pengaduan diserahkan dari siaga Ops kepada reserse criminal untuk diberikan ke Bagian Bin Opsonal. Laporan di proses kemudian diteruskan ke penyidik lalu didisposisikan untuk dilakukan proses hukum sesuai undang-undang. Jika proses selesai maka pelapor datang ke Kepolisian untuk mengambil jawaban atas surat permohonan yang diajukan. (Daryono & Sugiantoro, 2017).

Berikut adalah contoh alur pelaporan *Cyber crime* yang berjalan di Kepolisian dapat dilihat pada Gambar 3.1.



Gambar 3.1 Alur pelaporan *Cyber crime* yang berjalan di Kepolisian

Sumber: (Daryono & Sugiantoro, 2017)

3.2 Analisis Kebutuhan

Analisis kebutuhan pada pembuatan sistem ini saya membaginya menjadi beberapa bagian yang terdiri dari analisis kebutuhan form, analisis kebutuhan proses, analisis kebutuhan output, analisis kebutuhan peralatan pendukung.

3.2.1 Analisis Kebutuhan Form

Analisis kebutuhan form merupakan data yang dibutuhkan untuk Sistem Informasi Pelaporan Kejahatan *Cyber crime*. Dari data yang dimasukkan ke dalam sistem, sistem akan mengolah data tersebut menjadi informasi. Masukkan data yang dibutuhkan yaitu:

Tabel 3.1 Tabel analisis kebutuhan form

No	Keterangan
1	Data Petugas
2	Data Jenis Kasus
3	Data Pelapor
4	Data Pengaduan
5	Data Penanganan

3.2.2 Analisis Kebutuhan Proses

Analisis kebutuhan proses merupakan proses apa saja yang berjalan pada sistem. Admin diharuskan untuk melakukan proses *login* terlebih dahulu selanjutnya admin dapat mengatur (tambah, ubah, hapus, tampil) data pada proses mengelola petugas dan jenis kasus. Pelapor dapat mendaftarkan dirinya sebelum melaporkan dan mengisi form laporan yang ada. Kasubdit bisa menangani laporan yang masuk dengan memabalasnya dan melakukan tindakan dalam proses penanganan.

3.2.3 Analisis Kebutuhan Output

Analisis kebutuhan output dari sistem informasi pelaporan kejahatan *Cyber crime* berupa data laporan yang ditampilkan untuk kebutuhan Kepolisian, selain itu juga memuat informasi mengenai tindak kejahatan yang bisa dilanjutkan ketahapan penyidikan lebih lanjut atau hanya cukup sampai tahap pelaporan.

3.2.4 Analisis Kebutuhan Perangkat Lunak

Analisis kebutuhan perangkat lunak adalah menentukan *software* apa yang digunakan untuk membuat sistem, beberapa *software* diantaranya:

Tabel 3.2 Tabel spesifikasi *software*

No	<i>Software</i>	Keterangan
1	Windows 10 Education	Sistem Operasi yang saya gunakan dalam melakukan penelitian.
2	XAMPP	<i>Software</i> untuk menyambungkan web server ke <i>database</i> , dengan memanfaatkan apache sebagai web server dan

		MySQL sebagai basis data untuk menampung data.
3	PHP	Bahasa Pemrograman yang digunakan.
4	Sublime Text	Text editor program.
5	Clickchart Diagram File	Software untuk membuat ERD, DFD Level 0, DFD level 1, DFD level 2.
6	Balsamiq Project	Software untuk membuat perancangan antar muka.
7	Google Chrome	Browser untuk menampilkan output program.
8	Piktochart	Aplikasi infografis berbasis web untuk membuat alur mekanisme pelaporan <i>cyber crime</i> .

3.2.5 Analisis Kebutuhan Perangkat Keras

Analisis kebutuhan perangkat keras adalah kebutuhan *hardware* minimal yang digunakan untuk menjalankan sistem. Spesifikasi *hardware* yang digunakan agar sistem dapat berjalan yaitu:

Tabel 3.3 Tabel spesifikasi *hardware*

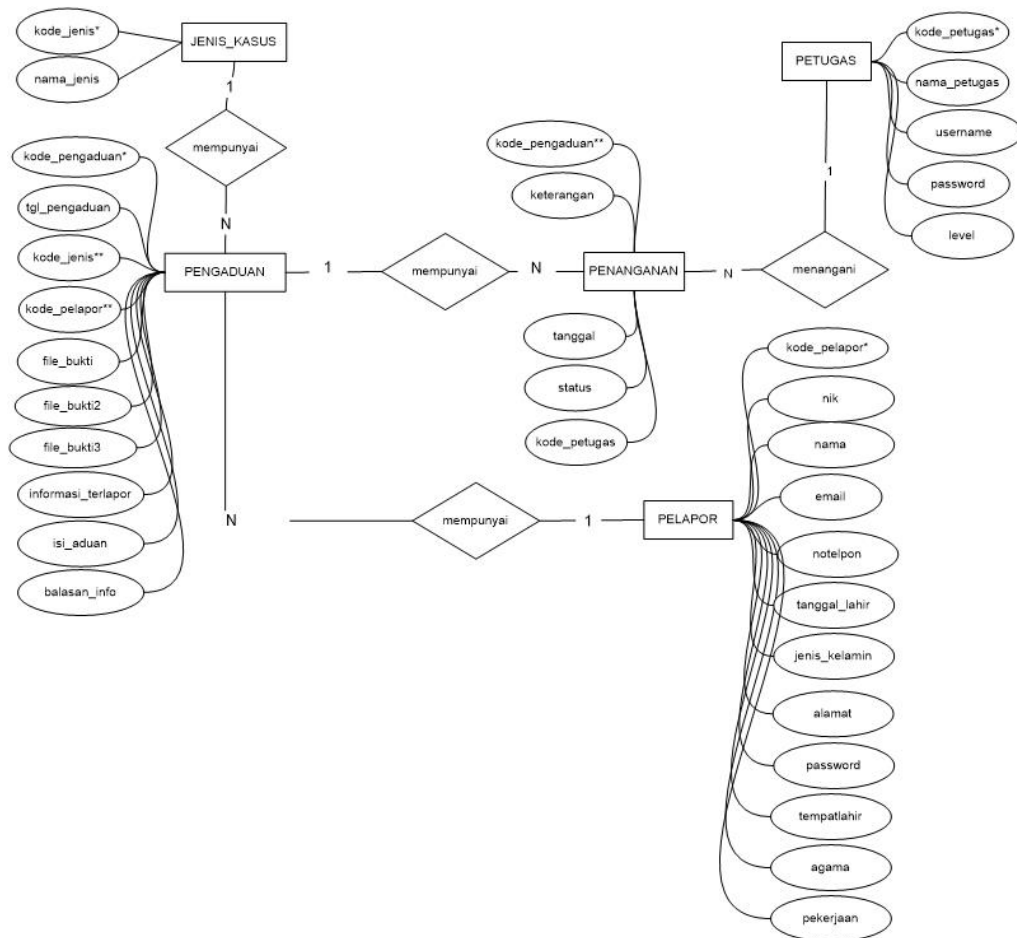
No	Perangkat	Jumlah	Spesifikasi Unit
1	Notebook Asus A555L	1	Sistem Operasi: Windows 10 Education 64-bit Processor: Intel® Core™ i5-5200U CPU @ 2.20GHz RAM: 4.00 GB DDR3L VGA: NVIDIA GEFORCE 840M
2	Mouse & Keyboard	1	Logitech MK240 Nano Combo

3.3 Perancangan Konseptual

Perancangan konseptual terdiri dari perancangan basis data, perancangan *Data Flow Diagram* (DFD), dan perancangan antarmuka.

3.3.1 Perancangan basis data.

Pada perancangan basis data terdapat 5 entitas yaitu: petugas, jenis kasus, pengaduan, penanganan, dan pelapor. Berikut ini adalah *Entity Relationship Diagram* Sistem Informasi Kasus Pelaporan *Cyber crime*, seperti Gambar 3.2.



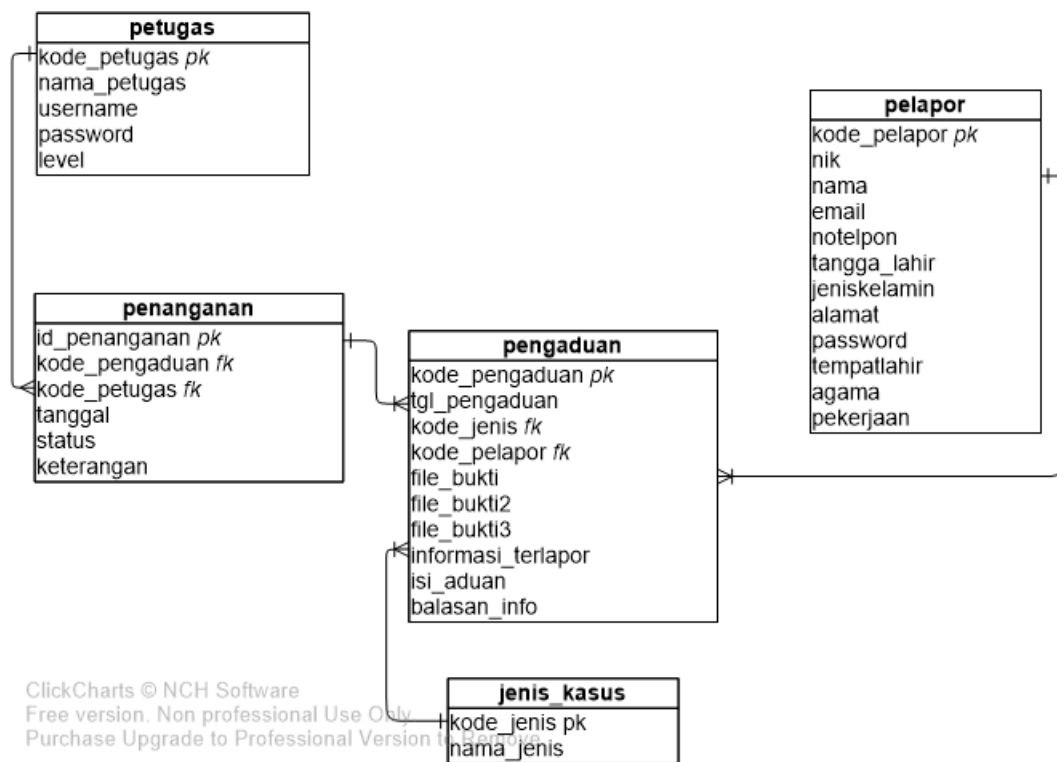
Gambar 3.2 *Entity Relationship Diagram*

Pada gambar 3.2 di atas pada setiap entitas memiliki atribut. Entitas PETUGAS memiliki kode_petugas, nama_petugas, *username*, *password* dan level. Entitas JENIS_KASUS memiliki kode_jenis dan nama jenis. Entitas PELAPOR memiliki kode_pelapor, nik, nama, email, notelpon, tanggal_lahir, jenis_kelamin, alamat, *password*, tempatlahir, agama, dan pekerjaan . Entitas PENGADUAN memiliki kode_pengaduan, tgl_pengaduan, kode_jenis, kode_pelapor, file_bukti, filebukti1, filebukti2, informasi_pelapor, isi_aduan, dan balasan info. Entitas

PENANGANAN memiliki kode_pengaduan, tanggal, status, kode_petugas, keterangan.

Terdapat beberapa relasi antar entitas yaitu JENIS_KASUS dengan PENGADUAN berelasi 1:N yang artinya satu JENIS_KASUS mempunyai banyak PENGADUAN. PELAPOR dengan PENGADUAN berelasi 1:N yang artinya satu pelapor bisa melakukan banyak pengaduan ke sistem informasi yang dibuat. PETUGAS dengan PENANGANAN berelasi 1:N artinya satu Petugas melakukan banyak penanganan laporan. PENGADUAN dengan PENANGANAN berelasi 1:N artinya satu pengaduan mempunyai banyak penanganan.

Selanjutnya yaitu, relasi antar tabel yang ditunjukkan pada gambar 3.3 di bawah ini.



Gambar 3.3 Relasi Antar Tabel

Dari pembuatan ERD yang dilanjutkan dengan relasi antar tabel maka dijabarkan tipe data dan daya tampung data yang akan dijabarkan dalam setiap tabel.

Tabel 3.4 Tabel Petugas

Kolom	Tipe Data	Key
kode_petugas	Char (2)	<i>Primary key</i>
nama_petugas	Varchar (50)	-
<i>username</i>	Varchar (50)	-
<i>password</i>	Varchar (50)	-
level	Varchar (50)	-

Tabel 3.4 Petugas yang dibuat akan digunakan untuk menyimpan data petugas, terdapat 5 kolom dengan tipe data masing-masing. Berikut penjelasan struktur tabel petugas:

- a. Kolom kode_petugas untuk menyimpan data Kode petugas sebagai *Primary key* dengan tipe data *Char* dengan batasan 2 pengisian karakter.
- b. Kolom nama_petugas untuk menyimpan data nama petugas dengan tipe data *varchar* dengan batasan 50 pengisian karakter.
- c. Kolom *username* untuk menyimpan data *username* dengan tipe data *varchar* dengan batasan 50 pengisian karakter.
- d. Kolom *password* untuk menyimpan data *password* dengan tipe data *varchar* dengan batasan 50 pengisian karakter.
- e. Kolom Level untuk menyimpan data level petugas dengan tipe data *varchar* dengan batasan 50 pengisian karakter.

Tabel 3.5 Tabel Jenis Kasus

Kolom	Tipe Data	Key
kode_jenis	Char (3)	<i>Primary key</i>

nama_jenis	Varchar (50)	-
------------	--------------	---

Tabel 3.5 Jenis Kasus yang dibuat akan digunakan untuk menyimpan data jenis kasus, terdapat 2 kolom dengan tipe data masing-masing. Berikut penjelasan struktur tabel jenis kasus:

- a. Kolom kode_jenis untuk menyimpan data kode jenis sebagai *Primary key* dengan tipe data *char* dengan batasan 3 pengisian karakter.
- b. Kolom nama_jenis untuk menyimpan data nama jenis dengan tipe data *varchar* dengan batasan 50 pengisian karakter.

Tabel 3.6 Tabel Pelapor

Kolom	Tipe Data	Key
kode_pelapor	Int (11)	<i>Primary key, AI</i>
nik	Varchar (20)	-
nama	Varchar (50)	-
email	Varchar (100)	-
notelpon	Varchar (15)	-
tanggal_lahir	Date	-
jenis_kelamin	Char (1)	-
alamat	<i>Text</i>	-
<i>password</i>	Varchar (50)	-
tempatlahir	Varchar (100)	-
agama	Varchar (100)	-
pekerjaan	Varchar (100)	-

Tabel 3.6 Pelapor yang dibuat akan digunakan untuk menyimpan data pelapor, terdapat 12 kolom dengan tipe data masing-masing. Berikut penjelasan struktur tabel pelapor:

- a. Kolom *kode_pelapor* untuk menyimpan kode pelapor sebagai *Primary key* dengan tipe data *int* dengan batasan 11 pengisian karakter, kolom ini *auto increment* sehingga akan terisi sendiri.
- b. Kolom *nik* untuk menyimpan nik pelapor dengan tipe data *varchar* dengan batasan 20 pengisian karakter.
- c. Kolom *nama* untuk menyimpan data nama pelapor dengan tipe data *varchar* dengan batasan 50 pengisian karakter.
- d. Kolom *email* untuk menyimpan data email pelapor dengan tipe data *varchar* dengan batasan 100 pengisian karakter.
- e. Kolom *notelpon* untuk menyimpan data No Telpon pelapor dengan tipe data *varchar* dengan batasan 15 pengisian karakter.
- f. Kolom *tanggal_lahir* untuk menyimpan data tanggal lahir pelapor dengan tipe data *date*.
- g. Kolom *jenis_kelamin* untuk menyimpan data jenis kelamin pelapor dengan tipe data *varchar* dengan batasan 1 pengisian karakter.
- h. Kolom *alamat* untuk menyimpan data alamat pelapor dengan tipe data *text*.
- i. Kolom *password* untuk menyimpan data *password* pelapor dengan tipe data *varchar* dengan batasan 50 pengisian karakter.
- j. Kolom *tempatlahir* untuk menyimpan data tempat lahir pelapor dengan tipe data *varchar* dengan batasan 100 pengisian karakter.
- k. Kolom *agama* untuk menyimpan data agama pelapor dengan tipe data *varchar* dengan batasan 100 pengisian karakter.
- l. Kolom *pekerjaan* untuk menyimpan data pekerjaan pelapor dengan tipe data *varchar* dengan batasan 100 pengisian karakter.

Tabel 3.7 Tabel Pengaduan

Kolom	Tipe Data	Key
Kode_pengaduan	Char (10)	<i>Primary key</i>
Tgl_pengaduan	Date	-
Kode_jenis	Char (3)	<i>Foreign key</i>

Kode_pelapor	Int (11)	<i>Foreign key</i>
File_bukti	Varchar (100)	-
File_bukti2	Varchar (100)	-
File_bukti3	Varchar (100)	-
Informasi_terlapor	<i>Text</i>	-
Isi_aduan	<i>Text</i>	-
Balasan_info	<i>text</i>	-

Tabel 3.7 Pengaduan yang dibuat akan digunakan untuk menyimpan data pengaduan, terdapat 10 kolom dengan tipe data masing-masing. Berikut penjelasan struktur tabel pengaduan:

- a. Kolom kode_pengaduan untuk menyimpan data kode pengaduan sebagai *Primary key* dengan tipe *char* dengan batasan 10 pengisian karakter.
- b. Kolom tgl_pengaduan untuk menyimpan data tanggal pengaduan dengan tipe data *date*.
- c. Kolom kode_jeis untuk menyimpan data kode jenis sebagai *Foreign key* dengan tipe data *char* dengan batasan 3 pengisian karakter.
- d. Kolom kode_pelapor untuk menyimpan data kode pelapor sebagai *Foreign key* dengan tipe data *int*.
- e. Kolom file_bukti untuk menyimpan data berkas yang digunakan sebagai bukti laporan dengan tipe data *varchar* dengan batasan 100 pengisian karakter.
- f. Kolom file_bukti1 untuk menyimpan data berkas yang digunakan sebagai bukti laporan dengan tipe data *varchar* dengan batasan 100 pengisian karakter.
- g. Kolom file_bukti2 untuk menyimpan data berkas yang digunakan sebagai bukti laporan dengan tipe data *varchar* dengan batasan 100 pengisian karakter.

- h. Kolom *informasi_terlapor* untuk menyimpan data yang berkaitan dengan informasi terlapor dengan tipe data *text*.
- i. Kolom *isi_aduan* untuk menyimpan data isi aduan dengan tipe data *text*.
- j. Kolom *balasan_info* untuk menyimpan data info balasan yang ditujukan kasubdit ke user dengan tipe data *text*.

Tabel 3.8 Tabel Penanganan

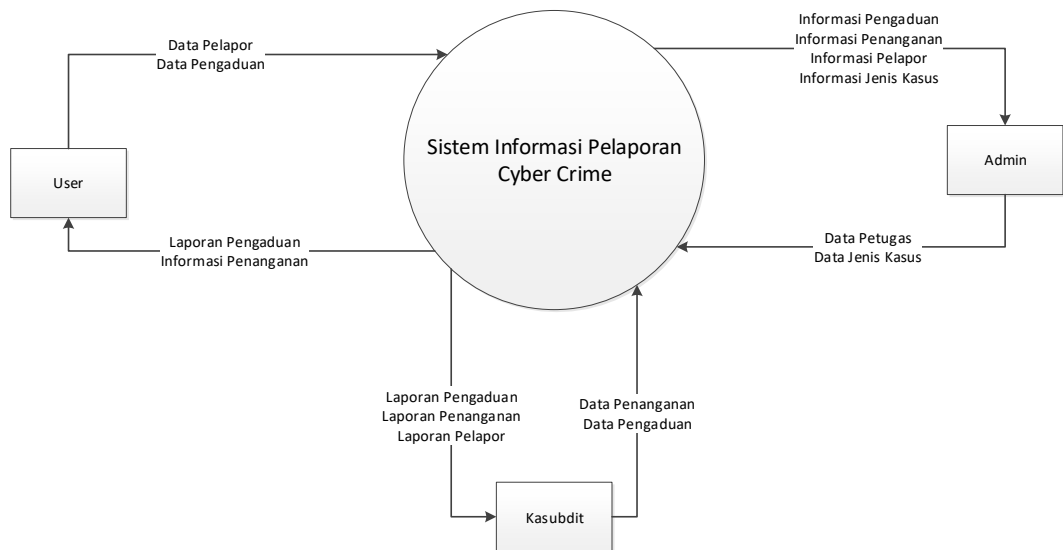
Kolom	Tipe Data	Key
<i>id_penanganan</i>	Int (11)	<i>Primary key</i>
<i>kode_pengaduan</i>	Char (10)	<i>Foreign key</i>
<i>kode_petugas</i>	Varchar (2)	<i>Foreign key</i>
<i>tanggal</i>	Date	-
<i>status</i>	Varchar (100)	-
<i>keterangan</i>	<i>Text</i>	-

Tabel 3.8 Penanganan yang dibuat akan digunakan untuk menyimpan data penanganan, terdapat 6 kolom dengan tipe data masing-masing. Berikut penjelasan struktur tabel penanganan:

- a. Kolom *id_penanganan* untuk menyimpan data id penanganan sebagai *Primary key* dengan tipe data *int* dengan batasan 11 pengisian karakter.
- b. Kolom *kode_pengaduan* untuk menyimpan data kode pengaduan sebagai *Foreign key* dengan tipe data *char* dengan batasan 10 pengisian karakter.
- c. Kolom *kode_petugas* untuk menyimpan data kode petugas sebagai *Foreign key* dengan tipe data *char* dengan batasan 2 pengisian karakter.
- d. Kolom *tanggal* untuk menyimpan data tanggal dengan tipe data *date*.
- e. Kolom *status* untuk menyimpan data status pengaduan dengan tipe data *varchar* dengan batasan 100 pengisian karakter.

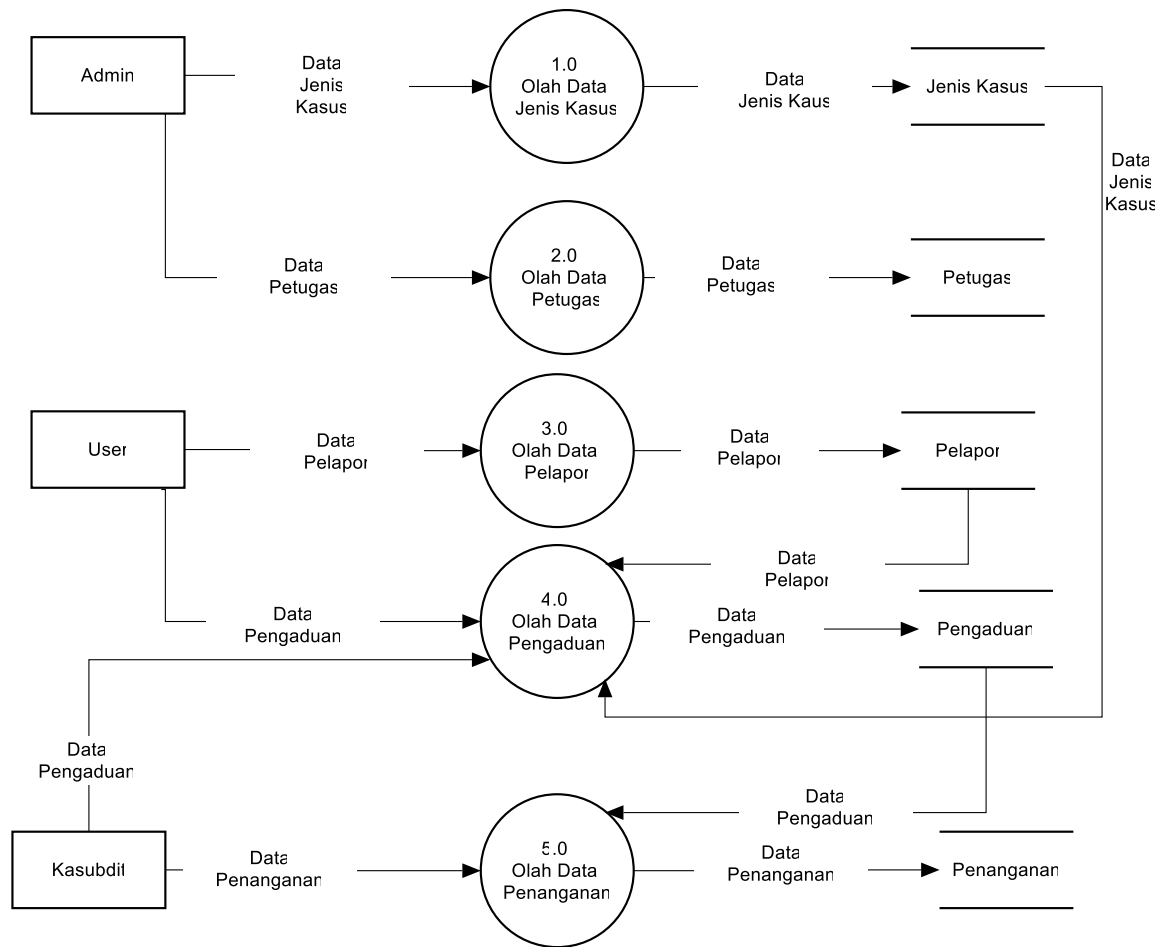
- f. Kolom keterangan untuk menyimpan data keterangan dengan tipe data *text*.

3.3.2 Perancangan *Data Flow Diagram* (DFD)



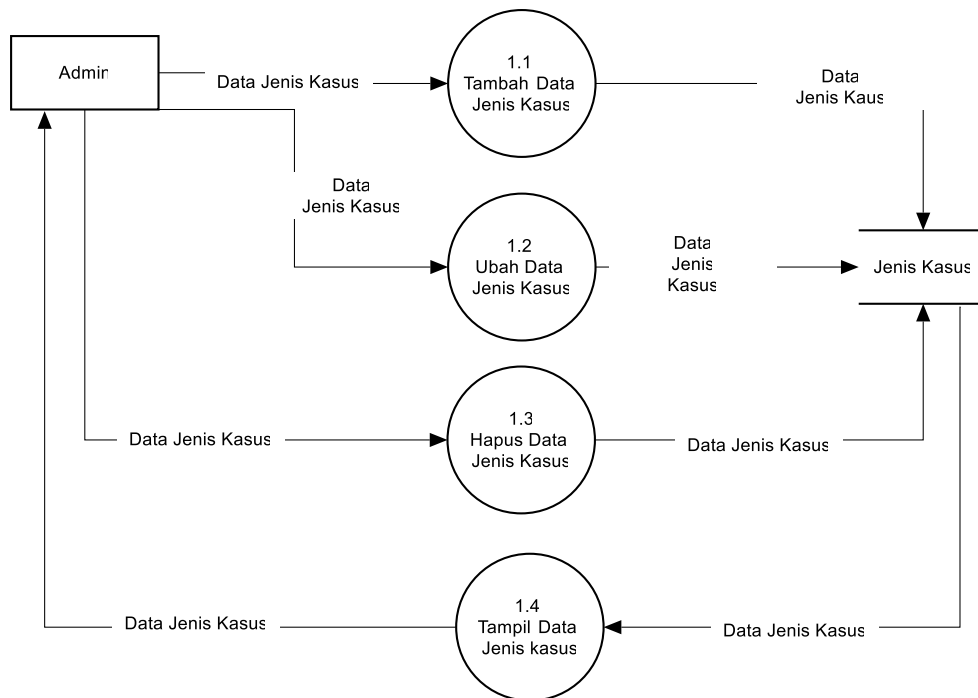
Gambar 3.4 *Data Flow Diagram* (DFD) Level 0

Diagram Level 0 pada gambar 3.4 di atas terdiri dari tiga entitas luar yaitu admin, user dan kasubdit dengan proses Sistem Informasi Kasus Pelaporan *Cyber crime*. Arus data dari admin ke sistem yaitu data petugas dan jenis kasus sedangkan arus data dari sistem ke admin yaitu informasi jenis kasus, informasi pelapor dan informasi petugas. Arus data dari user ke sistem yaitu data pelapor dan data pengaduan sedangkan arus data dari sistem ke user yaitu laporan pengaduan dan informasi penanganan. Arus data dari kasubdit ke sistem yaitu data penanganan dan data pengaduan sedangkan arus data dari sistem ke kasubdit yaitu laporan pengaduan, laporan penanganan, dan laporan pelapor.



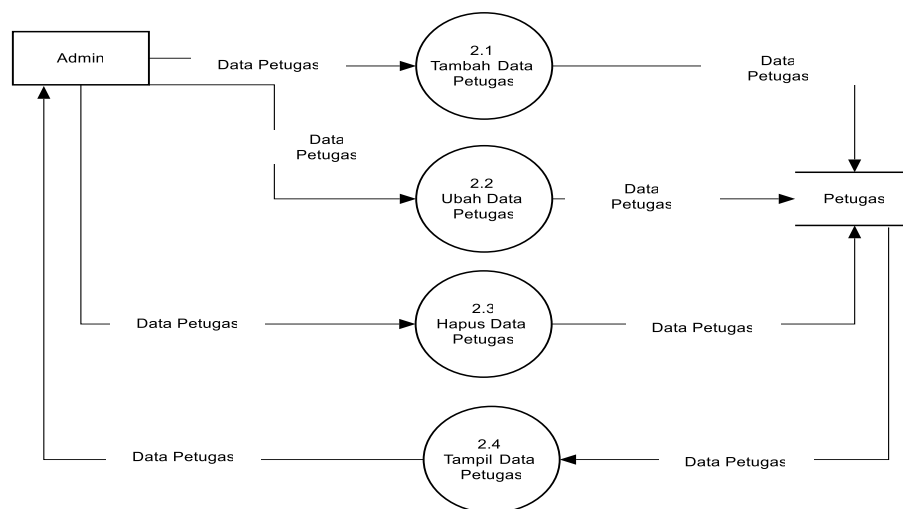
Gambar 3.5 Data Flow Diagram (DFD) Level 1

DFD level 1 pada gambar 3.5 di atas terdiri dari tiga entitas luar yaitu admin dan kasubdit. Terdapat 5 proses di dalamnya yaitu olah data jenis kasus, olah data petugas, olah data pelapor, olah data pengaduan, dan olah data penanganan. Pada penyimpanan data terdapat penyimpanan data jenis kasus, petugas, pelapor, pengaduan dan penanganan.



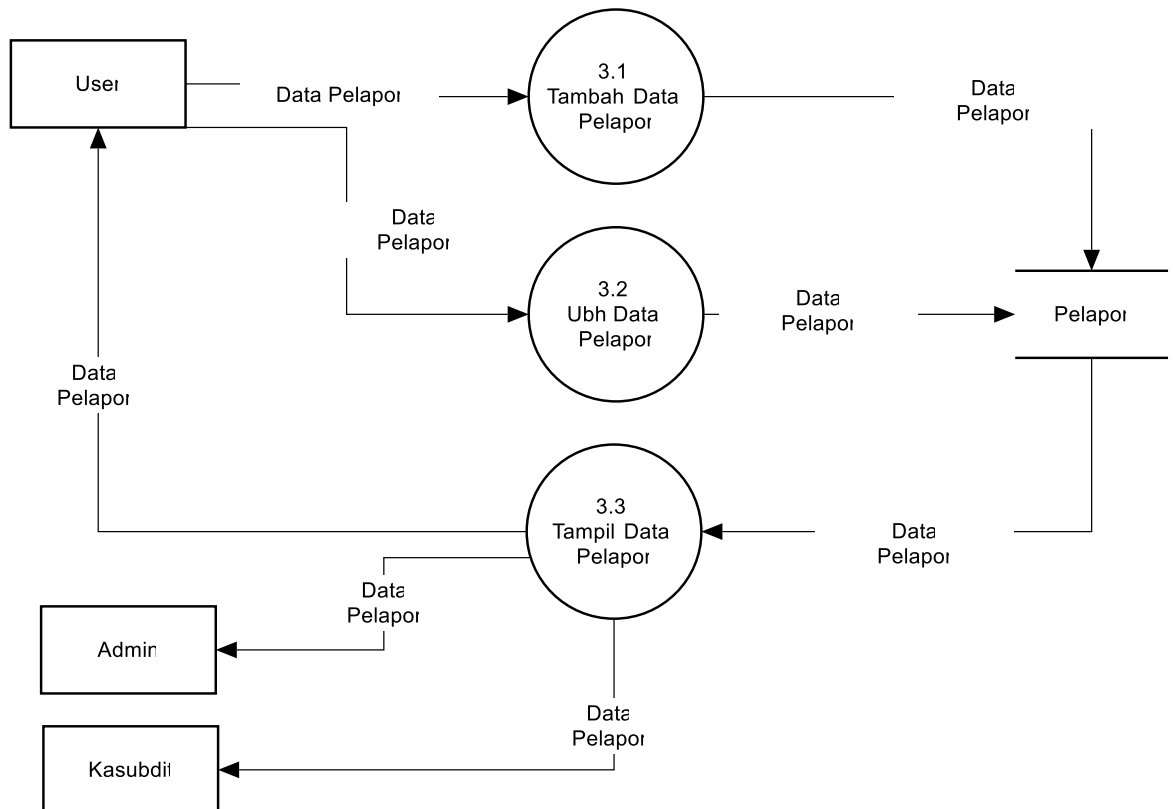
Gambar 3.6 Data Flow Diagram (DFD) Level 2 Jenis Kasus

DFD level 2 untuk proses jenis kasus pada gambar 3.6 di atas terdiri dari satu entitas luar yaitu admin. Pada penyimpanan data terdapat satu penyimpanan yaitu penyimpanan jenis kasus. Terdapat empat proses yaitu tambah data, ubah data, hapus data, dan tampil data.



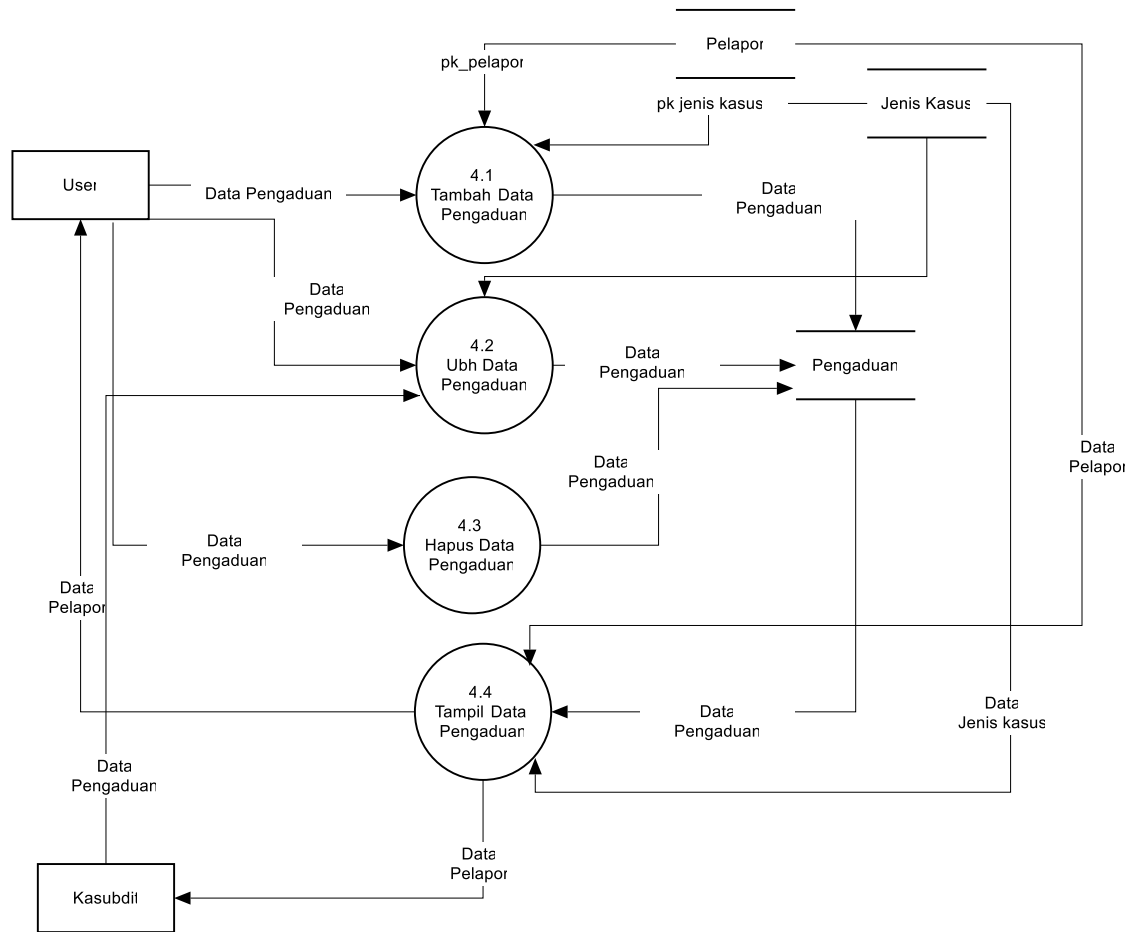
Gambar 3.7 Data Flow Diagram (DFD) Level 2 Petugas

DFD level 2 untuk proses petugas pada gambar 3.7 terdiri dari satu entitas luar yaitu admin. Pada penyimpanan data terdapat satu penyimpanan yaitu penyimpanan petugas. Terdapat 4 proses yaitu tambah data petugas, ubah data petugas, hapus data petugas dan tampil data petugas.



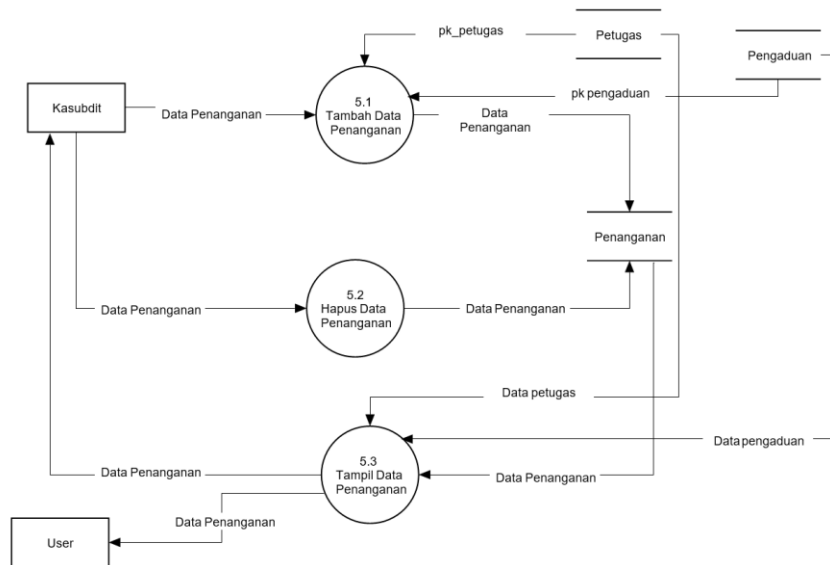
Gambar 3.8 Data Flow Diagram (DFD) Level 2 Pelapor

DFD level 2 untuk proses mengelola pelapor pada gambar 3.8 terdiri dari tiga entitas luar yaitu admin, kasubdit, dan user. Pada penyimpanan data terdapat satu penyimpanan yaitu penyimpanan pelapor. Terdapat tiga proses yaitu tambah pelapor, ubah pelapor, dan tampil pelapor.



Gambar 3.9 Data Flow Diagram (DFD) Level 2 Pengaduan

DFD level 2 untuk proses pengaduan pada gambar 3.9 di atas terdiri dari 2 entitas luar yaitu kasubdit dan user. Pada penyimpanan data terdapat 3 penyimpanan yaitu penyimpanan pelapor, jenis kasus dan pengaduan. Terdapat empat proses yaitu tambah pengaduan, ubah pengaduan, hapus pengaduan, dan tampil pengaduan.



Gambar 3.10 Data Flow Diagram (DFD) Level 2 Penanganan

DFD level 2 untuk proses penanganan pada gambar 3.10 di atas terdiri dari dua entitas luar yaitu kasubdit dan user. Pada penyimpanan data terdapat tiga penyimpanan yaitu penyimpanan petugas, penanganan dan pengaduan. Terdapat tiga proses yaitu tambah penanganan, hapus penanganan, dan tampil penanganan.

3.4 Perancangan Antarmuka

Perancangan antarmuka terdiri dari dua yaitu *front end* dan *back end*. *Front end* yaitu antarmuka yang akan tampil pada layar untuk digunakan oleh para pengunjung umum. *Back end* yaitu antarmuka yang akan tampil di belakang layar maksudnya hanya untuk digunakan oleh admin. Berikut ini adalah beberapa perancangan tampilan antarmuka yang akan digunakan:

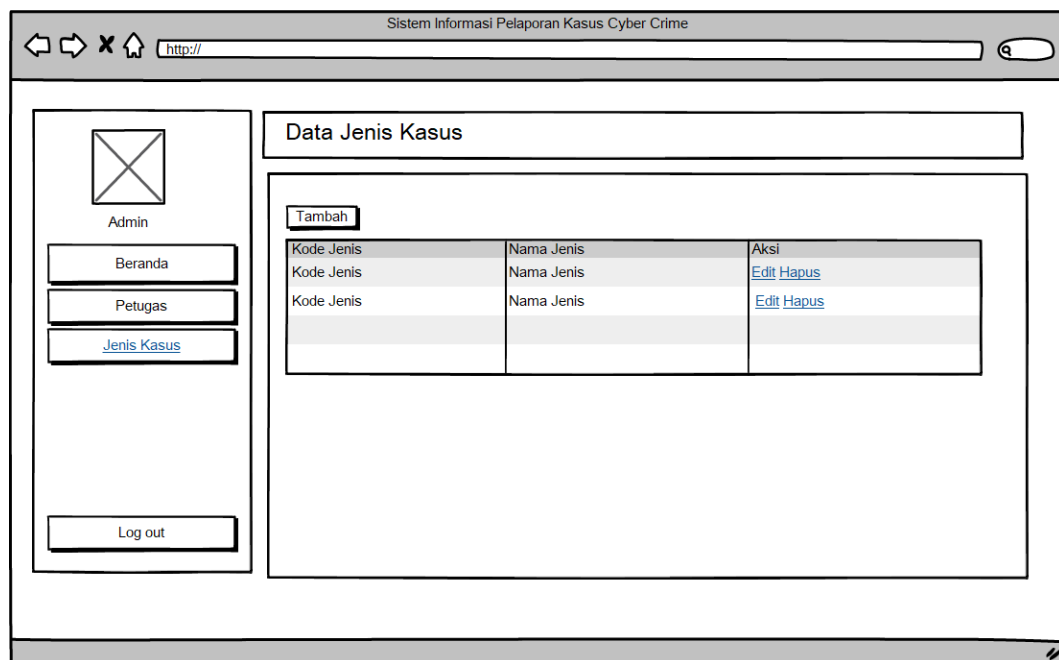
Gambar 3.11 Halaman *Login*

Perancangan halaman *login* seperti pada gambar 3.11 merupakan tampilan untuk user, kasubdit, dan admin sebelum dapat mengakses menu yang disediakan. Dalam halaman admin aktor harus mengisikan *username* dan *password* yang terdaftar dalam sistem, jika *username* dan *password* ada dalam sistem maka akan masuk ke menu-menu yang disediakan jika tidak ada maka akan memunculkan peringatan bahwa *username* dan *password* tidak terdaftar sehingga tidak dapat masuk ke dalam menu.

Kode Petugas	Nama Petugas	Username	Password	Level	Aksi
Kode Petugas	Nama Petugas	Username	Password	Level	Edit Hapus
Kode Petugas	Nama Petugas	Username	Password	Level	Edit Hapus

Gambar 3.12 Halaman Petugas

Perancangan antarmuka halaman petugas seperti gambar 3.12 merupakan halaman yang disediakan untuk admin dalam mengelola data petugas. Dalam halaman petugas admin bisa melihat data petugas yang terdaftar dimulai dari kode petugas, nama petugas hingga level. Dalam halaman petugas admin dapat menambah data petugas, mengubah data dan menghapus data.



Gambar 3.13 Halaman Jenis Kasus

Perancangan halaman jenis kasus yang terdapat dalam hak akses admin ditunjukkan dalam gambar 3.13. Dalam halaman jenis kasus admin dapat melihat data jenis kasus yang ada di dalam sistem. Admin dapat mengelola data jenis kasus yang meliputi menambah data jenis kasus, mengubah data, menghapus data dan juga melakukan pencarian data.

Sistem Informasi Pelaporan Kasus Cyber Crime

Daftar Pelapor

Nik

Nama

Email

No Telpn

Tanggal Lahir

Jenis Kelamin Laki - Laki Perempuan

Alamat

Daftar

Gambar 3.14 Halaman Daftar Laporan

Perancangan halaman daftar pelapor seperti yang terlihat dalam gambar 3.14 merupakan halaman yang disediakan bagi calon user atau pelapor yang akan berpartisipasi dalam menggunakan sistem ini. Dalam halaman daftar pelapor, user diharuskan mengisi biodata yang sudah disediakan yang meliputi nik, nama, email, no telpon, tanggal lahir, jenis kelamin, alamat. Proses pendaftaran bisa dilakukan ketika semua biodata sudah terisi lengkap sehingga bisa dilakukan proses pendaftaran.

Sistem Informasi Pelaporan Kasus Cyber Crime

Pengaduan

Tanggal Pengaduan

Jenis

File Bukti

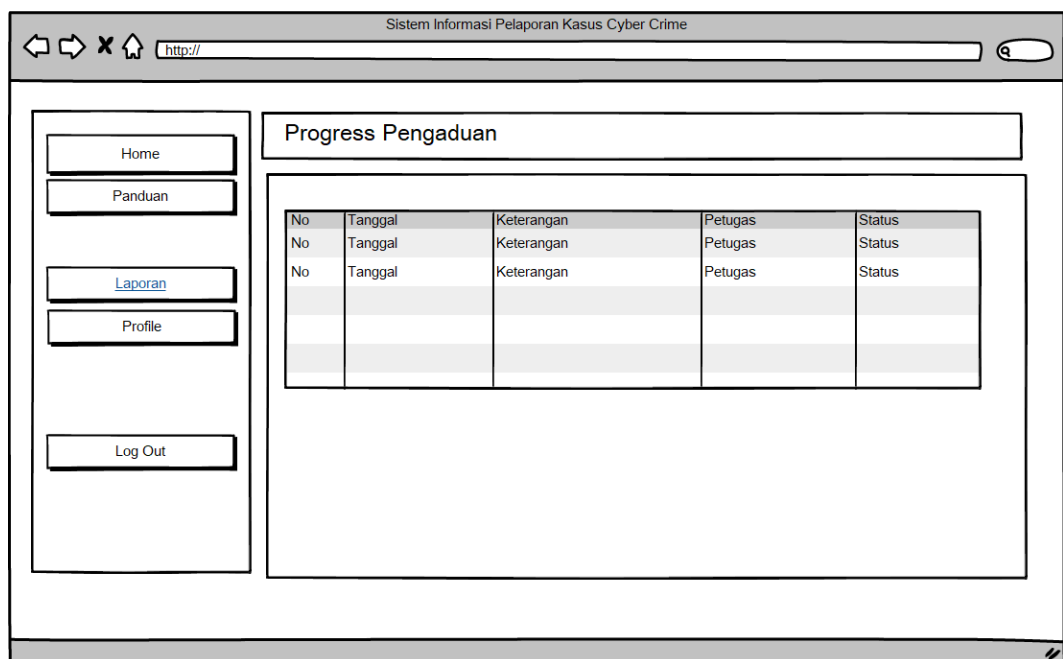
Informasi Terlapor

Isi Aduan

Daftar

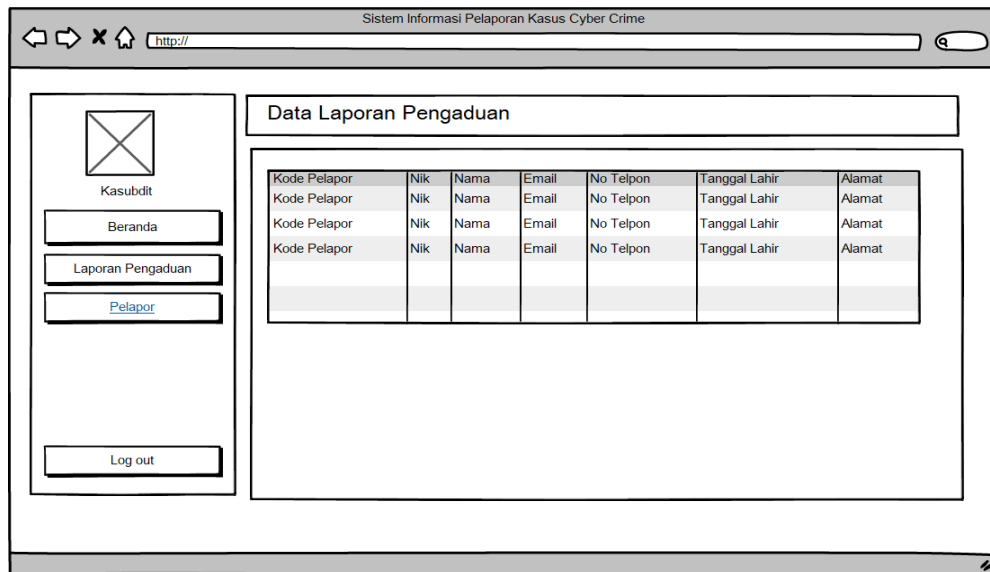
Gambar 3.15 Halaman Daftar Pengaduan

Perancangan antarmuka halaman pengaduan seperti pada gambar 3.15 merupakan halaman yang dapat diakses oleh user yang sudah melakukan proses *login* dengan benar. Dalam halaman pengaduan user dapat mengisi form pengaduan dengan mengisi tanggal pengaduan, jenis pengaduan yang akan dipilih, bukti dari laporan yang akan disampaikan, informasi mengenai terlapor jika mengetahui data/informasi yang bersangkutan serta isi aduan yang berisa tentang informasi yang akan dilaporkan.



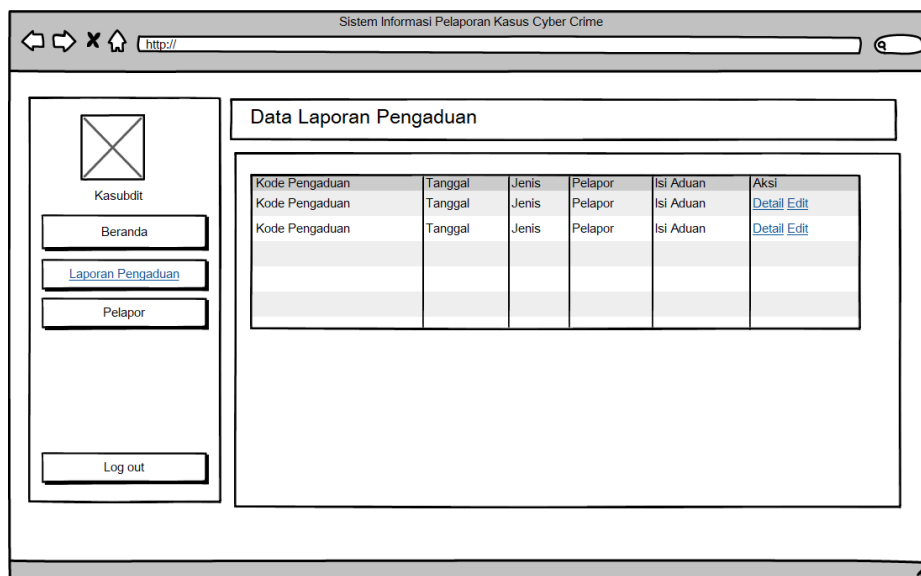
Gambar 3.16 Halaman *History* Penanganan

Perancangan halaman *history* seperti dalam gambar 3.16 merupakan halaman yang dapat diakses oleh user ketika sudah melakukan proses pengaduan. Dalam halaman ini user bisa melihat proses pengaduan yang sudah diajukan apakah sudah ditindak lanjuti atau sedang dalam proses sehingga bisa memantau jalannya laporan yang sudah diajukan.



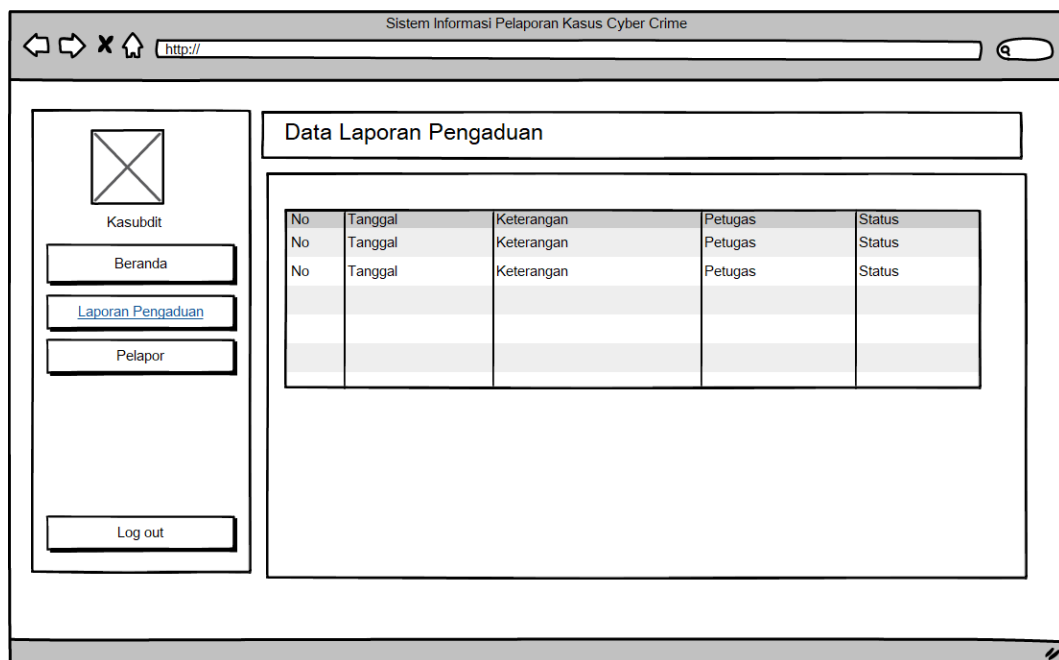
Gambar 3.17 Halaman Pelapor

Perancangan halaman pelapor seperti pada gambar 3.17 merupakan halaman yang dapat diakses oleh kasubdit dalam mengelola data laporan. Dalam halaman ini kasubdit dapat dengan mudah bisa memantau pelapor yang sudah terdaftar dalam sistem, Kasubdit juga dapat melakukan proses pencarian mengenai informasi biodata yang disimpan oleh user.



Gambar 3.18 Halaman Daftar Laporan

Perancangan antarmuka halaman daftar laporan atau pengaduan seperti pada gambar 3.18 merupakan halaman yang dapat diakses oleh kasubdit dalam menjalankan sistem ini. Dalam halaman ini kasubdit mampu melihat data laporan yang sudah dilaporkan kedalam sistem. Kasubdit bisa melihat informasi detail mengenai laporan yang ada.



Gambar 3.19 Halaman *History*

Perancangan detail laporan pengaduan dalam gambar 3.19 menampilkan progres sejauh mana laporan yang sudah dilakukan oleh user ditangani. Halaman ini diakses oleh kasubdit dalam menjalankan sistem ini. Sebelum laporan ini tampil kasubdit harus mengisikan data penanganan yang telah dilakukan dengan mengisi tanggal, petugas, dan status yang sudah dicapai dalam pengerjaan laporan.

BAB IV HASIL DAN PEMBAHASAN

4.1 Pengujian Sistem Informasi

Pengujian dilakukan setelah diselesaikan seluruh rangkaian implementasi dari Sistem Informasi Kasus Pelaporan *Cyber Crime*. Pengujian ini akan menggunakan metode *black-box testing*. Pengujian ini akan dilakukan untuk memastikan bahwa seluruh fungsionalitas yang dibangun pada Sistem Informasi Kasus Pelaporan *Cyber Crime* berjalan dengan sempurna tanpa ada kesalahan (*error*). Penulis membuat sejumlah *black-box test case* yang akan diujikan kepada sub menu atau modul dari aplikasi Sistem Informasi Kasus Pelaporan *Cyber Crime*.

Proses pengujian dilakukan di Kepolisian Resor Sleman melibatkan Bapak Nuryadi sebagai anggota reserse kriminal Kepolisian Resor Sleman dan saya sebagai pengembang dengan pengujian Sistem Informasi Kasus Pelaporan *Cyber crime* yang telah saya selesaikan. Saya sebagai pengembang melakukan pengujian untuk memastikan sistem berjalan dengan baik sesuai proses yang ditentukan, lalu Bapak Nuryadi melakukan proses pengujian dengan cara mencoba menggunakan sistem yang dibuat dan memberikan evaluasi kepada pengembang.

Tabel 4.1 Pengujian Black-Box Sistem Informasi Kasus Pelaporan Cyber Crime -
Admin

Test Case	Skenario	Aktivitas	Hasil	Kesimpulan
Kelola admin	Lihat dokumen petugas	Mengklik tombol bertuliskan view pada tabel data	Menampilkan informasi data petugas	Berhasil
	Tambah data petugas	Mengklik tombol tambah di atas table data	Meneruskan ke halaman form	Berhasil

		Mengisikan data yang dibutuhkan	Seluruh langkah dapat dilewati	Berhasil
		Mengklik tombol simpan	Menampilkan modal dan klik konfirmasi 'YA'	Berhasil
	Hapus data petugas	Mengklik tombol berlogo sampah pada tabel data	Menampilkan modal dan klik 'YA'	Berhasil
	Ubah dokumen petugas	Mengklik tombol berlogo pensil pada tabel aksi	Meneruskan ke halaman form	Berhasil
		Mengisikan data yang dibutuhkan	Seluruh langkah dapat dilewati	Berhasil
		Mengklik tombol simpan	Menampilkan modal dan klik konfirmasi 'YA'	Berhasil
	Lihat dokumen data jenis kasus	Mengubah status yang terletak di posisi paling atas menjadi lengkap	Filter berubah menjadi lengkap	Berhasil
	Tambah data jenis kasus	Mengklik tombol tambah di atas table data	Meneruskan ke halaman form	Berhasil
		Mengisikan data yang dibutuhkan	Seluruh langkah dapat dilewati	Berhasil

		Mengklik tombol simpan	Menampilkan modal dan klik konfirmasi 'YA'	Berhasil
	Hapus data petugas	Mengklik tombol berlogo sampah pada tabel data	Menampilkan modal dan klik 'YA'	Berhasil
	Ubah dokumen petugas	Mengklik tombol berlogo pensil pada tabel aksi	Meneruskan ke halaman form	Berhasil
		Mengisikan data yang dibutuhkan	Seluruh langkah dapat dilewati	Berhasil
		Mengklik tombol simpan	Menampilkan modal dan klik konfirmasi 'YA'	Berhasil
	Mencari Laporan Pengaduan	Mengubah tanggal awal dan tanggal akhir di form yang telah disediakan	Input dan filter berubah sesuai pilihan	Berhasil
		Mengklik tombol pilih yang berada di posisi bawah	Halaman menampilkan dokumen	Berhasil

Tabel 4.2 Pengujian Black-Box Sistem Informasi Kasus Pelaporan Cyber Crime –
Pelapor

Test Case	Skenario	Aktivitas	Hasil	Kesimpulan
Kelola pelapor	Lihat dokumen data pengaduan	Mengklik navigasi pengaduan	Menampilkan informasi data pengaduan	Berhasil

	Tambah data petugas	Mengklik tombol tambah di atas table data	Meneruskan ke halaman form	Berhasil
		Mengisikan data yang dibutuhkan	Seluruh langkah dapat dilewati	Berhasil
		Mengklik tombol simpan	Menampilkan modal dan klik konfirmasi 'YA'	Berhasil
	Lihat profil pelapor	Mengklik navigasi profil	Menampilkan informasi data profil pelapor	Berhasil
	Ubah profil pelapor	Mengklik navigasi profil	Meneruskan ke halaman form	Berhasil
		Mengisikan data yang dibutuhkan	Seluruh langkah dapat dilewati	Berhasil
		Mengklik tombol simpan	Menampilkan modal dan klik konfirmasi 'YA'	Berhasil
	Lihat Panduan	Mengklik navigasi panduan	Menampilkan informasi panduan	Berhasil

Tabel 4.3 Pengujian Black-Box Sistem Informasi Kasus Pelaporan Cyber Crime –
Petugas

Test Case	Skenario	Aktivitas	Hasil	Kesimpulan
Kelola petugas	Lihat dokumen dapat laporan baru	Mengklik tombol bertuliskan view pada tabel data	Menampilkan informasi data pengaduan	Berhasil

		Mengklik tombol aksi berlogo orang	Meneruskan ke halaman informasi pelapor	Berhasil
	Dokumen data pengaduan baru	Mengklik tombol aksi belogo garis	Menampilkan data pengaduan, data penanganan dan history penanganan	Berhasil
		Mengklik tombol simpan untuk status penanganan	Menampilkan modal dan klik konfirmasi 'YA'	Berhasil
	Hapus data history penanganan	Mengklik tombol berlogo sampah pada tabel data	Menampilkan modal dan klik 'YA'	Berhasil
	Lihat dokumen dapat laporan proses	Mengklik tombol bertuliskan view pada tabel data	Menampilkan informasi data pengaduan yang diproses	Berhasil
		Mengklik tombol aksi berlogo orang	Meneruskan ke halaman informasi pelapor	Berhasil
	Dokumen data pengaduan proses	Mengklik tombol aksi belogo garis	Menampilkan data pengaduan, data penanganan dan history penanganan	Berhasil
		Mengklik tombol simpan untuk status penanganan	Menampilkan modal dan klik konfirmasi 'YA'	Berhasil
	Hapus data history penanganan	Mengklik tombol berlogo	Menampilkan modal dan klik 'YA'	Berhasil

		sampah pada tabel data		
	Lihat dokumen dapat laporan selesai	Mengklik tombol bertuliskan view pada tabel data	Menampilkan informasi data pengaduan yang diproses	Berhasil
	Dokumen data pengaduan selesai	Mengklik tombol aksi berlogo orang	Meneruskan ke halaman informasi pelapor	Berhasil
		Mengklik tombol aksi belogo garis	Menampilkan data pengaduan, data penangaman dan history penanganan	Berhasil
		Mengklik tombol simpan untuk status penanganan	Menampilkan modal dan klik konfirmasi 'YA'	Berhasil
	Hapus data history penanganan	Mengklik tombol berlogo sampah pada tabel data	Menampilkan modal dan klik 'YA'	Berhasil
	Lihat Stastitik penyelesaian kasus dan jenis Kasus	Mengklik navigasi penyelesaian kasus dan jenis kasus	Menampilkan halaman data penyelesaian kasus dan jenis kasus	Berhasil
	Lihat data pelapor	Mengklik navigasi pelapor	Menampilkan halaman data pelapor	Berhasil
	Mencari dokumen data pelapor berdasarkan biodata	Mengklik tombol cari yang berada di posisi kanan paling atas	Halaman menampilkan dokumen	Berhasil
	Mencari Laporan Pengaduan	Mengubah tanggal awal dan tanggal akhir di form	Input dan filter berubah sesuai pilihan	Berhasil

		Mengklik tombol pilih yang berada di posisi bawah	Halaman menampilkan dokumen	Berhasil
--	--	---	-----------------------------	----------

Tabel 4.1 hingga Tabel 4.3 menunjukkan hasil akhir daripada pengujian *black-box testing*. Setelah melewati beberapa pengujian, penulis mendapatkan hasil akhir yang memuaskan, Pengujian telah berhasil melewati TC (*Test Case*) yang dibuat di tiap-tiap menunya. Kesimpulan yang diambil dari pengujian *black-box* ini tidak bersifat kuantitatif melainkan menggunakan kata ‘berhasil’ jika tiap-tiap menu berhasil melewati *test case* yang telah dibuat.

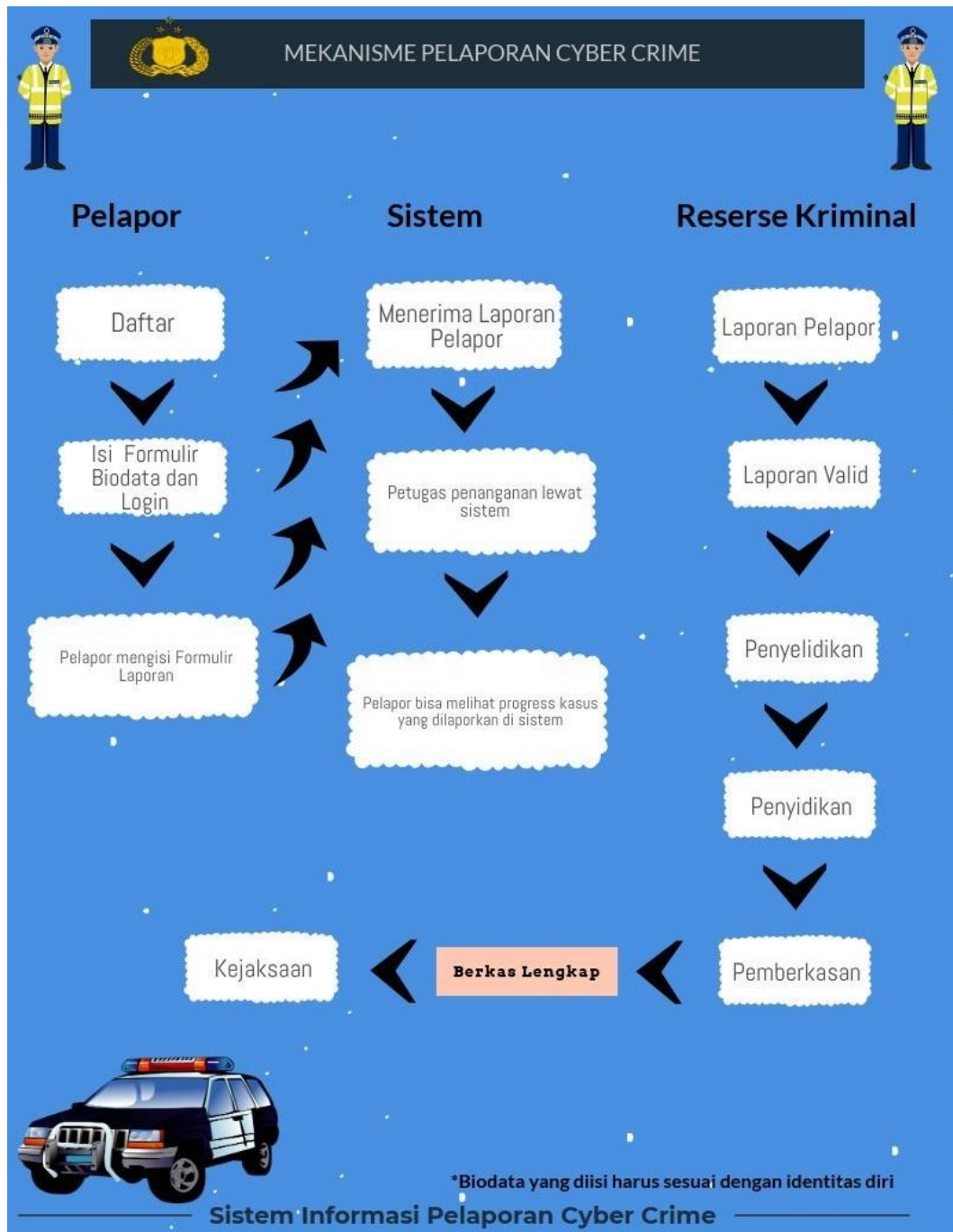
Pengujian ini menutup seluruh rangkaian metodologi penelitian yang dilakukan oleh penulis bersama pihak dari Kepolisian Resor Sleman yang dimulai dari tahap analisis, perancangan, implementasi dan pengujian. Setelah melakukan tahapan metodologi penelitian ini, penulis akan memaparkan kesimpulan dan hasil daripada penelitian ini.

4.2 Penjelasan dan *Screenshot* Program



Gambar 4.1 Halaman Utama Sistem Informasi Kasus Pelaporan *Cyber crime*

Penjelasan Gambar 4.1 adalah Halaman utama dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman tersebut berisi beberapa navigasi yaitu *Home*, *Panduan*, dan *Login*.



Gambar 4.2 Halaman Panduan Sistem Informasi Kasus Pelaporan *Cyber crime*

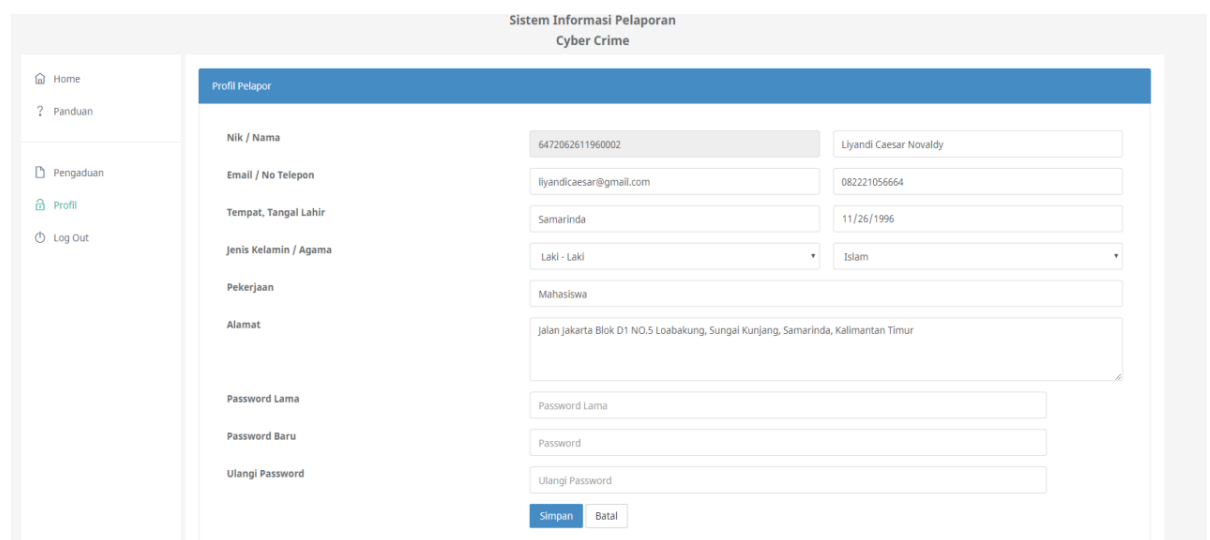
Penjelasan Gambar 4.2 adalah Halaman Panduan dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman tersebut berisi beberapa tentang panduan penggunaan sistem atau mekanisme pelaporan *cyber crime*.

Gambar 4.3 Halaman *Login* Sistem Informasi Kasus Pelaporan *Cyber crime*

Penjelasan Gambar 4.3 adalah Halaman *Login* dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman *login* terdiri dari *username* dan *password* yang harus diisi oleh admin, petugas dan pelapor. Jika pelapor ingin *login* harus daftar terlebih dahulu dimenu daftar. Khusus untuk admin bisa mendaftarkan *login* petugas untuk memproses laporan pelapor dan untuk *username* dan *password* admin sudah diatur oleh *database* dan hanya admin saja berhak mengakses halaman tersebut.

Gambar 4.4 Halaman Daftar Sistem Informasi Kasus Pelaporan *Cyber crime*

Penjelasan Gambar 4.4 adalah Halaman Daftar dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman daftar diisi oleh calon pelapor. Calon Pelapor mengisikan NIK, Nama, Email, No Telepon, Jenis Kelamin, Agama, Pekerjaan, Alamat, dan *password*. Setelah selesai mendaftar pelapor akan *login* menggunakan nomor telepon sebagai *username* dan *password* yang sudah ditentukan sendiri oleh pelapor.



The screenshot displays the 'Profil Pelapor' (Reporter Profile) page within the 'Sistem Informasi Pelaporan Cyber Crime' application. The page features a sidebar with navigation options: Home, Panduan, Pengaduan, Profil, and Log Out. The main content area contains a form for entering personal information. The form fields and their values are as follows:

Field	Value
Nik / Nama	6472062611960002 Liyandi Caesar Novaldy
Email / No Telepon	liyandicaesar@gmail.com 082221056664
Tempat, Tanggal Lahir	Samarinda 11/26/1996
Jenis Kelamin / Agama	Laki - Laki Islam
Pekerjaan	Mahasiswa
Alamat	Jalan Jakarta Blok D1 NO.5 Loabakung, Sungai Kurjang, Samarinda, Kalimantan Timur
Password Lama	Placeholder
Password Baru	Placeholder
Ulangi Password	Placeholder

At the bottom of the form, there are two buttons: 'Simpan' (Save) and 'Batal' (Cancel).

Gambar 4.5 Halaman Pelapor Sistem Informasi Kasus Pelaporan *Cyber crime*

Penjelasan Gambar 4.5 adalah Halaman Pelapor dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman Pelapor berisi tentang Profil Pelapor dan Halaman Pengaduan, sisanya sama seperti halaman utama yaitu ada *Home*, *Panduan*, *Logout* (sudah *login* pelapor). Jika kita mengklik Profil maka akan muncul data yang telah kita masukkan sebelumnya dan ada tambahan fitur ubah *password* pelapor.

Tambah Pengaduan

Jenis: Illegal Contents

File Bukti 1 (*Wajib): Choose File kib.png

File Bukti 2 (*Opsional): Choose File panduan.png

File Bukti 3 (*Opsional): Choose File panduan.png

Informasi Terlapor: Berita Bohong yang di share oleh akun X di [facebook](#)

Isi Aduan: Berita yang di share oleh X mengandung kebohongan dan buktinya tidak ada atas berita yang di sharing, yang menimbulkan [kehebohan](#) di [facebook](#).

Simpan Batal

Gambar 4.6 Halaman Pengaduan Pelapor Sistem Informasi Kasus Pelaporan *Cyber crime*

Penjelasan Gambar 4.6 adalah Halaman Pengaduan Pelapor dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman Pengaduan Pelapor diisi oleh pelapor yang ingin melaporkan kasus *cyber crimenya*. Halaman Pengaduan Pelapor terdiri dari Jenis Laporan (Misalnya: *Illegal Contents*, *Hacking*, dan lain-lain) yang dimana jenis laporan tersebut disesuaikan oleh admin dan bisa ditambah tergantung kebutuhan oleh admin, selanjutnya ada File Bukti yang bisa diupload oleh pelapor hingga sampai 3 file bukti, lalu ada Informasi Terlapor dan Isi Aduan yang akan diisi oleh pelapor sendiri.

Data Pengaduan Tambah Data

Show 10 entries Search:

Tanggal	Jenis	Isi Aduan	Info Balasan	Status	Aksi
2018-09-23	Illegal Contents	Berita yang di share oleh X mengandung kebohongan dan buktinya tidak ada atas berita yang di sharing, yang menimbulkan kehebohan di facebook.		Baru	

Showing 1 to 1 of 1 entries Previous 1 Next

Gambar 4.7 Halaman Data Pengaduan Pelapor Sistem Informasi Kasus Pelaporan *Cyber crime*.

Penjelasan Gambar 4.7 adalah Halaman Data Pengaduan Pelapor dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman Data Pengaduan Pelapor berisi tentang laporan yang telah ditambah pelapor sebelumnya di sistem. Halaman tersebut memuat Tanggal terjadinya laporan, Jenis Laporan, Isi Aduan, Info Balasan, Status dan Aksi. Info Balasan masih kosong yang nantinya akan diisi oleh petugas dan untuk Status jika sudah ditangani oleh petugas nantinya akan berubah menjadi proses atau selesai. Aksi sendiri jika diklik akan muncul halaman detail pengaduan yang dibuat.

Data Pengaduan

No Pengaduan	P000000015
Tanggal Pengaduan	23-09-2018
Pelapor	Liyandi Caesar Novaldy
Jenis Kasus	Illegal Contents
Informasi Terlapor	Berita Bohong yang di share oleh akun X di facebook
Isi Aduan	Berita yang di share oleh X mengandung kebohongan dan buktinya tidak ada atas berita yang di sharing, yang menimbulkan kebohohan di facebook.
File Bukti	

History Penanganan

No	Tanggal	Petugas	Status	Keterangan

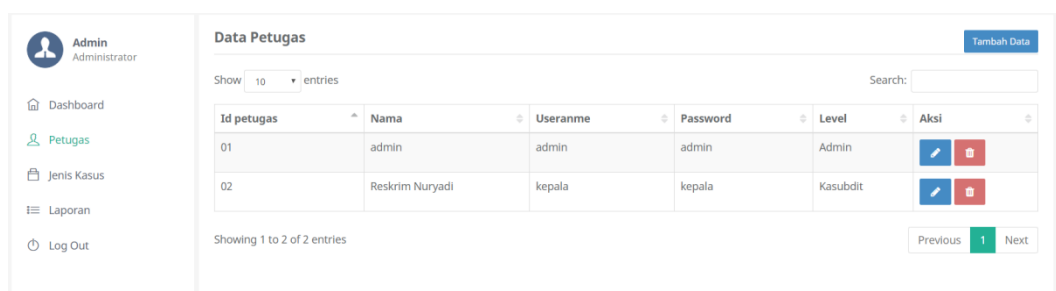
Gambar 4.8 Halaman Detail Data Pengaduan Pelapor Sistem Informasi Kasus Pelaporan *Cyber crime*.

Penjelasan Gambar 4.8 adalah Halaman Detail Data Pengaduan Pelapor dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman Data Detail Pengaduan Pelapor muncul jika kita mengklik Aksi seperti Gambar 4.7. Halaman Data Detail Pengaduan Pelapor memuat tentang data yang dimasukkan sebelumnya beserta file-file bukti yang sudah diupload. Halaman Data Detail Pengaduan Pelapor ini juga memuat *History* Penanganan dari petugas. Jadi jika pelapor ingin melihat proses laporannya bisa mengecek lewat halaman ini.



Gambar 4.9 Halaman Beranda Admin Sistem Informasi Kasus Pelaporan *Cyber crime*.

Penjelasan Gambar 4.9 adalah Halaman Beranda Admin dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman Beranda Admin berisi dashboard yang merupakan data Petugas yang bertugas di sistem dan Data Jenis Kasus, lalu ada Laporan yang memuat tentang laporan pengaduan dari pelapor.



Gambar 4.10 Halaman Beranda Admin Navigasi Petugas Sistem Informasi Kasus Pelaporan *Cyber crime*.

Penjelasan Gambar 4.10 adalah Halaman Beranda Admin di Navigasi Petugas dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman ini memuat tentang data petugas yang ada di sistem. Jika ingin menambahkan, mengubah, dan menghapus petugas bisa dilakukan oleh admin. Tabel yang bisa diubah yaitu nama, *username*, *password* dan level.

Id jenis	jenis	Aksi
J01	Hacking	[Edit] [Delete]
J02	Cracking	[Edit] [Delete]
J03	Unauthorized Access to Computer System and Service	[Edit] [Delete]
J04	Illegal Contents	[Edit] [Delete]
J05	Data Forgery	[Edit] [Delete]
J06	Infringements of Privacy	[Edit] [Delete]

Gambar 4.11 Halaman Beranda Admin Navigasi Jenis Kasus Sistem Informasi Kasus Pelaporan *Cyber crime*.

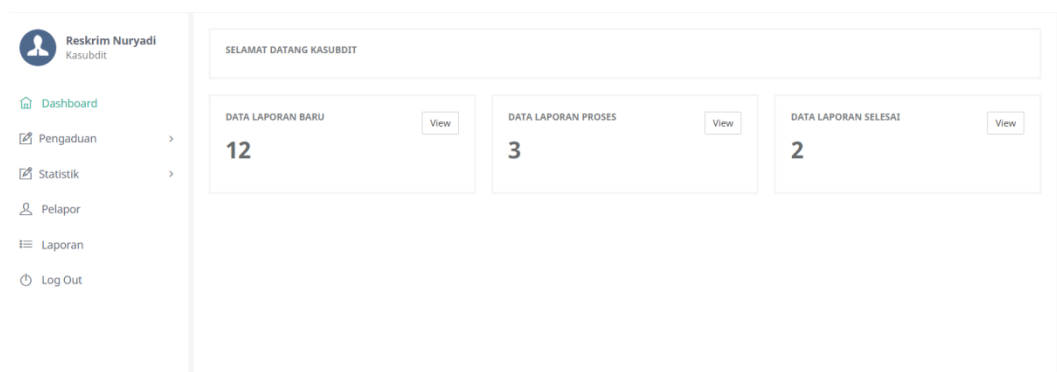
Penjelasan Gambar 4.11 adalah Halaman Beranda Admin di Navigasi Jenis Kasus dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman ini memuat tentang jenis kasus *cyber crime* yang bisa tambah, ubah, dan hapus sesuai kebutuhan oleh admin.

No	No Aduan	Tanggal Aduan	Jenis	Pelapor	Isi Aduan	Status
1	P000000015	23-09-2018	Illegal Contents	Liyandi Caesar Novaldy	Berita yang di share oleh X mengandung kebohongan dan buktinya tidak ada atas berita yang di sharing, yang menimbulkan kebohohan di facebook.	Baru
2	P000000016	23-09-2018	Hacking	Setyo Legianto	Akun saya di hack oleh X dengan menggunakan web phisingnya yang di share di facebook. Facebooknya bernama xxx, setelah saya searching korbannya juga bukan hanya saya seperti yang saya lampirkan pada File Bukti 2	Baru
3	P000000017	23-09-2018	Data Forgery	Setyo Legianto	Akun palsu yang tertera di twitter X adalah palsu. Foto dan Nama profil dia bukan dia melainkan teman saya. Dia melakukan penipuan dengan mengirim pesan kepada saya untuk mentransfer sejumlah uang dengan lagi sakit.	Baru
4	P000000018	23-09-2018	Data Forgery	Setyo Legianto	Akun palsu yang tertera di facebook X adalah palsu. Foto dan Nama profil dia bukan dia melainkan teman saya. Dia melakukan penipuan dengan mengirim pesan kepada saya untuk mentransfer sejumlah uang dengan lagi sakit.	Baru

Gambar 4.12 Halaman Beranda Admin Navigasi Laporan Pengaduan Sistem Informasi Kasus Pelaporan *Cyber crime*.

Penjelasan Gambar 4.12 adalah Halaman Beranda Admin di Navigasi Laporan Pengaduan dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat.

Halaman ini memuat tentang semua laporan pengaduan yang dimasukkan oleh pelapor lengkap dengan nomor aduan sampai status aduan untuk rekap admin.



Gambar 4.13 Halaman Beranda Petugas Sistem Informasi Kasus Pelaporan *Cyber crime*.


Penjelasan Gambar 4.13 adalah Halaman Beranda Petugas dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman ini memuat tentang laporan pengaduan yang diisi oleh pelapor, statistik penyelesaian dan jenis kasus, data pelapor dan halaman laporan pengaduan yang sama seperti admin.



Gambar 4.14 Halaman Beranda Petugas Navigasi Pengaduan Sistem Informasi Kasus Pelaporan *Cyber crime*.

Penjelasan Gambar 4.14 adalah Halaman Beranda Petugas Navigasi Pengaduan dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman ini memuat tentang laporan pengaduan yang diisi oleh pelapor. Data Pengaduan dibagi menjadi 3 yaitu Baru, Proses, dan Selesai. Pengaduan Baru muncul jika pelapor mengisi laporan kasus *cyber crime* diakunnya dan langsung masuk ke data

pengaduan milik petugas, sedangkan Pengaduan akan masuk ke Proses ketika petugas telah melakukan penanganan laporan yang dibuat oleh pelapor, jika sudah dilakukan penanganan dari petugas maka status laporan diubah otomatis menjadi Proses dan *history* dari penanganan kasus bisa dilihat oleh pelapor.


No Pengaduan	P00000015
Tanggal Pengaduan	23-09-2018
Pelapor	Liyandi Caesar Novaldy
Jenis Kasus	Illegal Contents
Informasi Terlapor	Berita Bohong yang di share oleh akun X di facebook
Isi Aduan	Berita yang di share oleh X mengandung kebohongan dan buktinya tidak ada atas berita yang di sharing, yang menimbulkan kehebohan di facebook.
File Bukti	
Apakah Laporan Selesai ?	<input checked="" type="checkbox"/>

Data Penanganan

Status:

Keterangan:

History Penanganan

No	Tanggal	Petugas	Status	Keterangan	Aksi
1	23-09-2018	Reskrim Nuryadi	Penyelidikan	Silahkan datang ke kantor untuk dimintai keterangan dalam bentuk berita acara	

Gambar 4.15 Halaman Beranda Petugas Data Pengaduan Pelapor Sistem Informasi Kasus Pelaporan *Cyber crime*.

Penjelasan Gambar 4.15 adalah Halaman Beranda Petugas Data Pengaduan Pelapor dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman ini berisi tentang laporan pelapor yang akan ditangani oleh petugas, lengkap dari nomor pengaduan sampai file bukti. Disini petugas bisa melakukan penanganan kepada pelapor dengan memilih status dan keterangannya. Status yang bisa dipilih yaitu Penyelidikan, Penyidikan, Pemberkasan, dan Selesai. Jika kasus selesai maka petugas bisa klik centang di form laporan selesai seperti Gambar 4.15. *History* Penanganan akan ditampilkan di akun petugas maupun akun pelapor.

History Penanganan

No	Tanggal	Petugas	Status	Keterangan
1	23-09-2018	Reskrim Nuryadi	Penyelidikan	Silahkan datang ke kantor untuk dimintai keterangan dalam bentuk berita acara
2	23-09-2018	Reskrim Nuryadi	Penyidikan	Ke kantor untuk dimintai keterangan dalam bentuk berita acara
3	23-09-2018	Reskrim Nuryadi	Penyidikan	Penyitaan Barang Bukti
4	23-09-2018	Reskrim Nuryadi	Penyidikan	Permintaan Keterangan dari Ahli
5	23-09-2018	Reskrim Nuryadi	Penyidikan	Permintaan Keterangan Tersangka
6	23-09-2018	Reskrim Nuryadi	Pemberkasan	Proses Pemberkasan
7	23-09-2018	Reskrim Nuryadi	Pemberkasan	Pemberkasan di kirim ke Kejaksaan
8	23-09-2018	Reskrim Nuryadi	Pemberkasan	Berkas Lengkap
9	23-09-2018	Reskrim Nuryadi	Pemberkasan	Berkas tersangka berikut barang bukti di kirim ke Kejaksaan

Gambar 4.16 Halaman *History* Penanganan Pelapor Sistem Informasi Kasus Pelaporan *Cyber crime*.

Penjelasan Gambar 4.16 adalah Halaman *History* Penanganan Pelapor dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman ini berisi tentang hasil dari penanganan yang dilakukan petugas lengkap dengan tanggal penanganan, petugas yang menangani, status dan keterangan laporan.

Data Pelapor

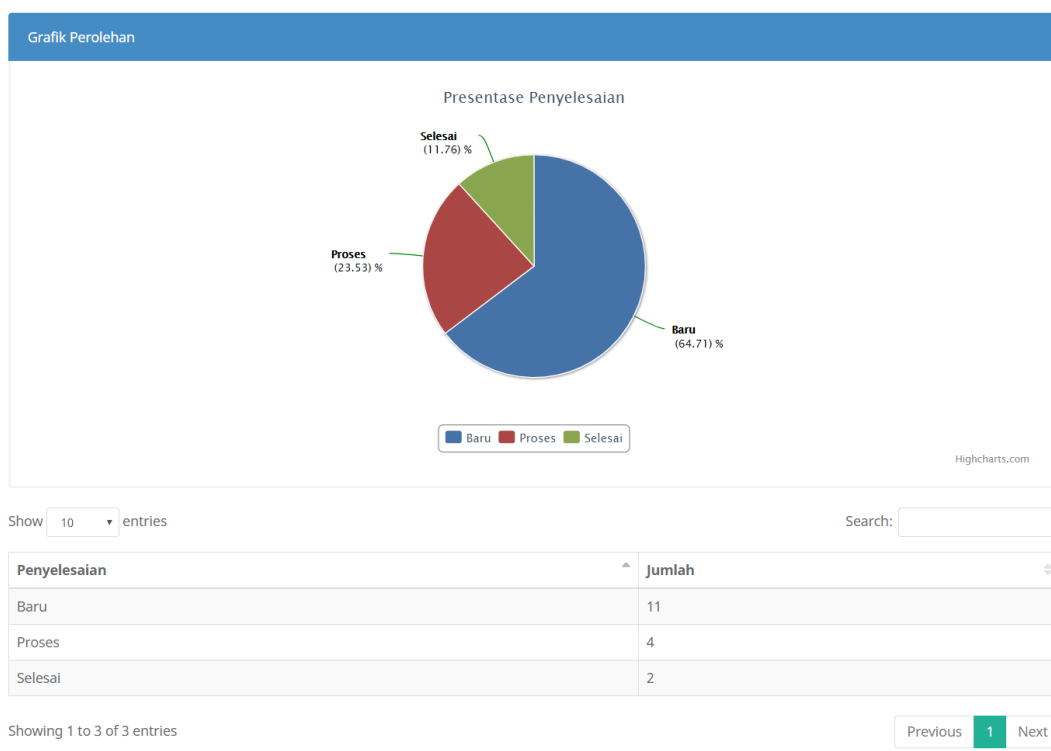
Show entries Search:

Nik	Nama	Email	No Telpn	Tempat,Tgl Lahir	JK	Agama	Pekerjaan	Alamat
6172012801960002	Rachman Winoto Nugroho	rachmanwinoto@gmail.com	085210457323	Singkawang, 28-01-1996	L	Islam	Mahasiswa	Jalan Beringin No 1, Condong, Singkawang Tengah, Singkawang, Kalimantan Barat
6472052602960001	Setyo Legianto	setyolegianto@gmail.com	087819925553	Samarinda, 26-02-1996	L	Islam	Mahasiswa	Jalan Kemakmuran GG.PLN, Sungai Pinang Dalam, Sungai Pinang Dalam, Samarinda Kalimantan Timur
6472062611960002	Liyandi Caesar Novaldy	liyandicaesar@gmail.com	082221056664	Samarinda, 26-11-1996	L	Islam	Mahasiswa	Jalan Jakarta Blok D1 NO.5 Loabakung, Sungai Kunjang, Samarinda, Kalimantan Timur

Showing 1 to 3 of 3 entries Previous **1** Next

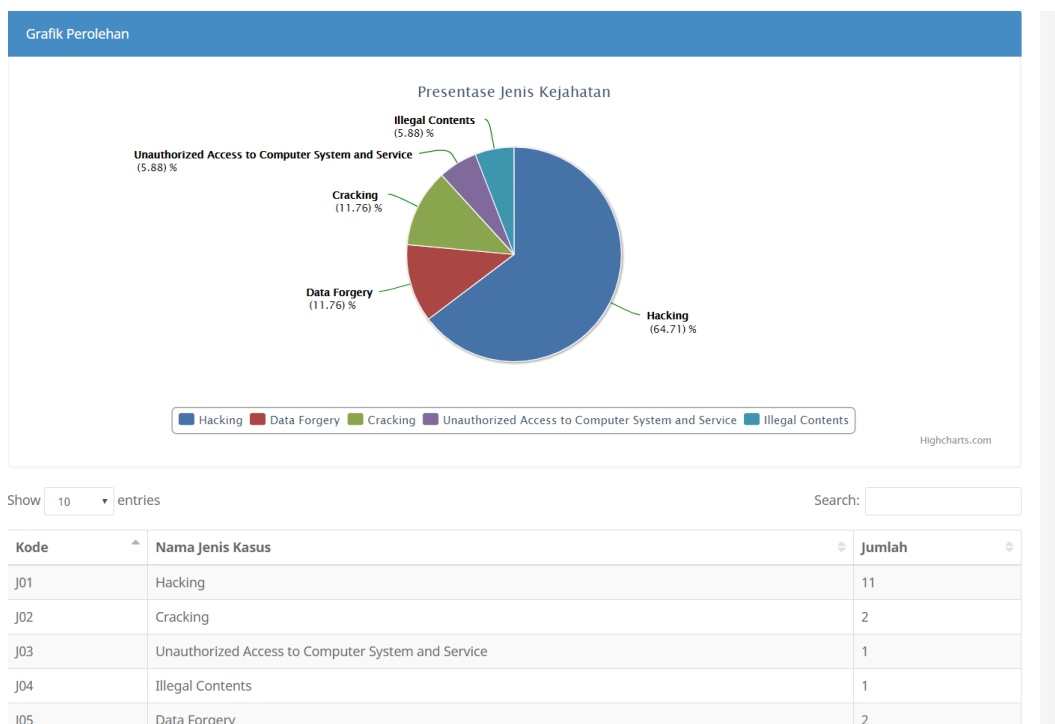
Gambar 4.17 Halaman Beranda Petugas Navigasi Data Pelapor Sistem Informasi Kasus Pelaporan *Cyber crime*.

Penjelasan Gambar 4.17 adalah Halaman Beranda Petugas Navigasi Data Pelapor dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman ini memuat tentang biodata lengkap pelapor.



Gambar 4.18 Halaman Beranda Petugas Navigasi Statistik Penyelesaian Kasus Sistem Informasi Kasus Pelaporan *Cyber crime*.

Penjelasan Gambar 4.18 adalah Halaman Beranda Petugas Navigasi Statistik Penyelesaian Kasus dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman ini berisi tentang persentase atas kasus yang telah ditangani oleh petugas dari kasus baru, kasus proses dan kasus selesai.



Gambar 4.19 Halaman Beranda Petugas Navigasi Statistik Jenis Kejahatan Sistem Informasi Kasus Pelaporan *Cyber crime*.

Penjelasan Gambar 4.19 adalah Halaman Beranda Petugas Navigasi Statistik Jenis Kejahatan yang dilaporkan oleh pelapor dari Sistem Informasi Kasus Pelaporan *Cyber crime* yang saya buat. Halaman ini berisi tentang persentase atas jenis kasus apa saja yang telah dilaporkan pelapor.

4.3 Kelebihan dan Kekurangan Program

Kelebihan dari program yang dibuat yaitu:

- Sistem Informasi Kasus Pelaporan *Cyber crime* ini dapat memudahkan pelaporan *cyber crime* bagi pelapor.
- Sistem Informasi Kasus Pelaporan *Cyber crime* ini dapat merekap penyelesaian kasus *cyber crime* dan merekap jenis kejahatan yang dilaporkan.
- Sistem Informasi Kasus Pelaporan *Cyber crime* ini dapat mengurangi beban kerja petugas reserse kriminal, piket reserse kriminal dan piket Sentra Pelayanan Kepolisian Terpadu.

Kekurangan dari program yang dibuat yaitu:

- a. Sistem Informasi Kasus Pelaporan *Cyber crime* ini hanya memberikan jawaban data penanganan secara umum, tidak memberikan jawaban data penanganan yang detail bagi pelapor.
- b. Sistem Informasi Kasus Pelaporan *Cyber crime* ini tidak mengakomodasi data petugas dan jabatan petugas.

BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Kesimpulan yang dapat diambil dari judul tugas akhir “Sistem Informasi Kasus Pelaporan *Cyber Crime*“ antara lain sebagai berikut:

1. Memudahkan pelapor untuk melaporkan kasus *cyber crime* mereka secara *online*
2. Memudahkan bagian reserse kriminal yang bertugas menangani *cyber crime* maupun bagian piket di Kepolisian dalam menangani kasus yang dilaporkan pelapor.

5.2 Saran

Berdasarkan sistem informasi yang telah dibangun, perlu adanya pengembangan sistem informasi ini guna meningkatkan layanan kepada publik. Oleh karena itu agar sistem menjadi lebih baik lagi maka saya menyarankan:

1. Memperluas penggunaan sistem informasi ini di Kepolisian yang menangani *cyber crime* dengan data dan perangkat yang mendukung.
2. Meningkatkan kualitas dari sistem informasi yang dibuat untuk memajemen sistem dengan baik dari sisi *client* maupun *server* yang digunakan.

DAFTAR PUSTAKA

- Achmad, S. (2016). Pemrograman Web dengan PHP dan MySQL. *Kom Universitas Budi Luhur*. <https://doi.org/10.1002/hed.24064>
- Adrio. (2010). Kejahatan Dengan Komputer | Computer Community. Retrieved December 11, 2018, from <https://kingrio.wordpress.com/2010/04/07/kejahatan-dengan-komputer/>
- Agus, A. A., & Riskawati. (2016). PENANGANAN KASUS CYBER CRIME DI KOTA MAKASSAR (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). *Jurnal Supremasi*.
- Daryono, & Sugiantoro, B. (2017). Pengembangan Framework Pelaporan Cyber Crime. *JISKa*.
- Elise Dwi Ratnasari. (2016). Cyber Crime, Kasus Kejahatan Terbanyak di 2016. Retrieved December 11, 2018, from <https://www.cnnindonesia.com/nasional/20161230232449-12-183255/cyber-crime-kasus-kejahatan-terbanyak-di-2016>
- Irawan, S. A. (2015). Perancangan Aplikasi Pengelolaan Laporan Kepolisian Studi Kasus Polsek Gatak. Retrieved from <http://eprints.ums.ac.id/36198/>
- Mustaqbal, M. S., Fajri, F. R., & Hendra, R. (2015). Pengujian Aplikasi Menggunakan Black Box Testing Boundary Value Analysis (Studi Kasus : Aplikasi Prediksi Kelulusan Snmptn). *Jurnal Ilmiah Teknologi Informasi Terapan*. <https://doi.org/ISSN : 2407 - 3911>
- Pressman, R. (2015). Software Engineering Seventh Edition. *Metode Waterfall*. <https://doi.org/10.1016/B978-1-4160-6911-9.00148-1>
- Siswanto, B., Rochim, A. F., & Somantri, M. (2012). SISTEM APLIKASI PENCATATAN TINDAK KEJAHATAN PADA POLSEK TEGAL SELATAN BERBASIS WEB. *TRANSIENT*, 1(3), 52–57. Retrieved from <https://ejournal3.undip.ac.id/index.php/transient/article/view/16>

Solichin, A. (2010). *MySQL Dari Pemula Hingga Mahir*. Universitas Budi Luhur.

LAMPIRAN

1. Lampiran Surat Keterangan Riset dan Wawancara di Kepolisian Resor Sleman

KEPOLISIAN NEGARA REPUBLIK INDONESIA
DAERAH ISTIMEWA YOGYAKARTA
RESOR SLEMAN



SURAT KETERANGAN Nomor : Sket/ 42 /VIII/2018/Reskrim

1. a. Surat Fakultas Teknologi Industri Universitas Islam Indonesia Nomor : 981/Kaprodi.TF/20/Penelitian/VII/2018 tanggal 17 Juli 2018 perihal Permohonan Penelitian/ Tugas Akhir;
b. Disposisi Wakapolres Sleman Nomor: B/1829/VII/2018 tanggal 24 Juli 2018 isi, silakan diarahkan.

2. Kepala Kepolisian Resor Sleman menerangkan bahwa :

N a m a : LIYANDI CAESAR NOVALDY
No. Mahasiswa : 14523194
Univ / Akademi : UNIVERSITAS ISLAM INDONESIA
Program studi : S-1 TEKNIK INDUSTRI

Telah melaksanakan Riset dan wawancara di Polres Sleman guna penyusunan Tugas Akhir dengan judul :

"SISTEM INFORMASI PELAPORAN KASUS CYBER CRIME"

3. Demikian untuk menjadi maklum.

Dikeluarkan di : Sleman
Pada tanggal : 02 Agustus 2018
di : KEPALA KEPOLISIAN RESOR SLEMAN
KASAT RESKRIM

