Virtualisasi Data Traffic Monitoring Insiden Di Id-SIRTII/CC

Sidang Skripsi

Fiska Mekar Kustiani
10108535

Penguji 1 :
Adam Mukharil Bachtiar

Penguji 2 :
Mira Kania Sabariah, S.T., M.T.

Penguji 3 :
Inne Novitasari, S.Si., M.Si.



Latar Belakang

Masalah

- Pendataan insiden web dilakukan dengan cara memasukkan data yang diambil dari Zone-h (http://www.zone-h.org) dan Indonesian Defacer (http://indonesiandefacer.org) secara satu persatu.

  Akibatnya, terjadi keterlambatan dalam proses pendataan dan tidak semua web yang telah disusupi peretas itu terdata.

Solusi

- Dibutuhkannya alat bantu kerja berupa piranti lunak untuk memonitoring insiden web berbasis protokol internet di Indonesia yang nantinya dapat menyimpan rekaman transaksi (*log file*).



Perumusan Masalah

Bagaimana cara membangun piranti lunak untuk memonitoring insiden web yang terjadi di Id-SIRTII/CC.



Maksud dan Tujuan

Maksud dari penelitian tugas akhir ini adalah untuk membangun virtualisasi data *traffic monitoring* insiden berbasis web di Id-SIRTII/CC.

Sedangkan tujuan yang akan dicapai adalah :

Memudahkan melakukan pemantauan website berdomain Indonesia yang disusupi oleh peretas dan peringatan terhadap ancaman dan gangguan pada website yang berdomain Indonesia.



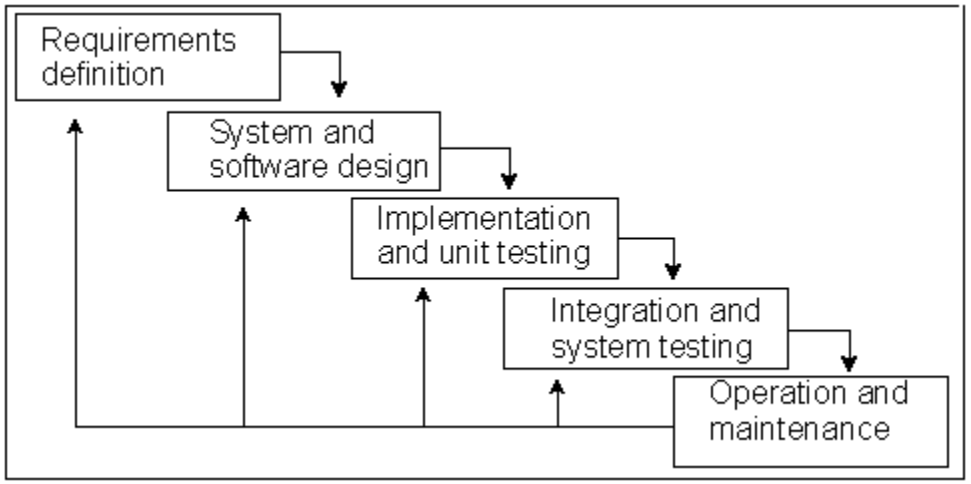
Batasan Masalah

1. Sumber data insiden hanya web yang berdomain Indonesia dan berasal dari *Laboratorium Data Mining Deputy of Research and Development* Id-SIRTII/CC.
2. Untuk pengolahan data menggunakan teknik *Data Mart*.
3. Data yang akan ditampilkan adalah data web domain Indonesia yang telah disusupi oleh peretas berdasarkan jenis domain dan waktu kejadian.
4. Output virtualisasi yang dihasilkan adalah berupa informasi laporan insiden web domain Indonesia dalam bentuk grafik.
5. Metode analisis yang akan digunakan dalam pembangunan piranti lunak ini adalah analisis terstruktur.
6. Perangkat lunak yang akan dibangun berbasis web.



Metodologi Penelitian

- Tahap pengumpulan data
  - Studi Literatur
  - Studi Lapangan
  - Wawancara
- Tahap pembangunan perangkat lunak

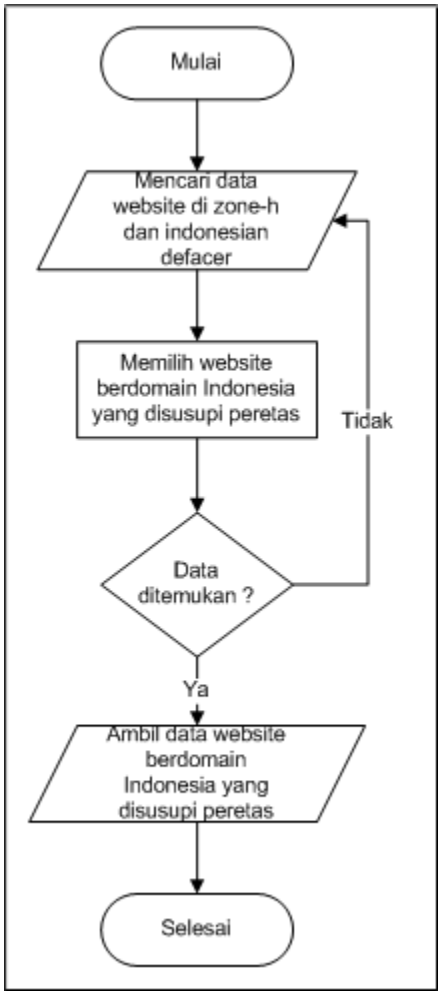


(Sumber: *Software Engineering*, Sommerville)



Analisis Sistem

Analisis yang sedang berjalan





Analisis Sistem

Analisis yang baru

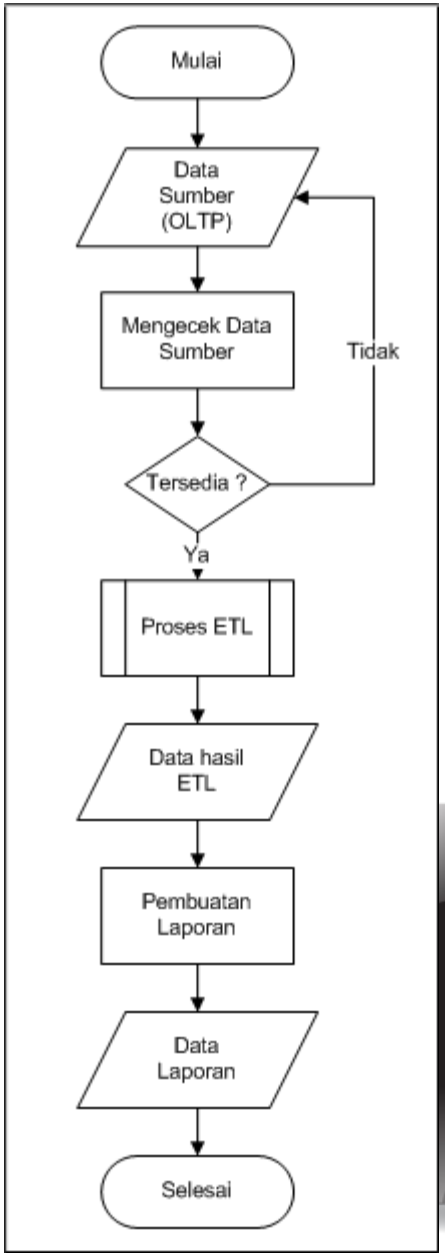




Diagram Relasi OLTP

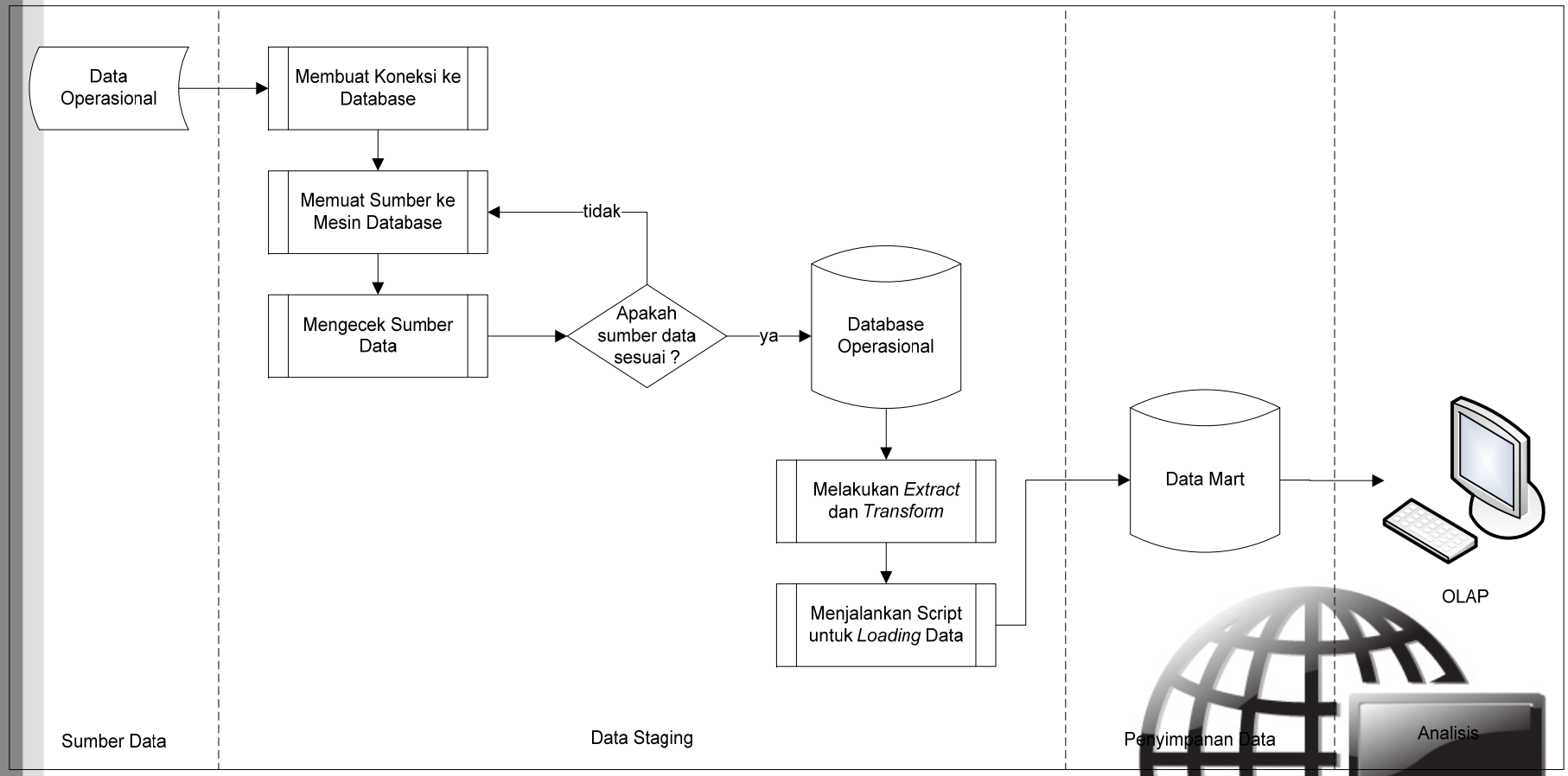
jenis_domain	
PK	**ID_jenis_domain**
	tipe_domain jenis_domain

website	
PK	**ID_website**
	domain_owner alamat_website
FK1	**ID_jenis_domain**

insiden	
PK	**kode_insiden**
	waktu_kejadian status_recovery
FK1	**ID_website**
FK2	**ID_jenis_domain**



Analisis Data Mart



Analisis ETL *(Extract, Transform, Loading)*

- *Extract*

	A	B	C	D	E
1	kode_insiden	waktu_kejadian	status_recovery	ID_website	ID_jenis_domain
2	1	2012-04-03 00:00	OFF	1	5
3	2	2012-03-26 00:00	OFF	2	5
4	3	2012-03-25 00:00	OFF	3	5
5	4	2012-04-10 13:41	Sudah Diperbaiki	4	5
6	5	2012-04-02 19:24	OFF	5	5
7	6	2012-03-31 00:00	Sudah Diperbaiki	6	5
8	7	2012-04-01 00:00	Belum Diperbaiki	7	5
9	8	2012-04-01 00:00	Belum Diperbaiki	8	5
10	9	2012-04-02 00:00	Sudah Diperbaiki	9	5
11	10	2012-04-02 00:00	Sudah Diperbaiki	10	5
12	11	2012-04-02 00:00	Sudah Diperbaiki	11	5
13	12	2012-03-24 00:00	Sudah Diperbaiki	12	5
14	13	2012-04-03 00:00	Sudah Diperbaiki	13	5
15	14	2012-04-04 00:33	Sudah Diperbaiki	14	5
16	15	2012-04-08 00:00	OFF	15	5
17	16	2012-04-08 00:00	OFF	16	5
18	17	2012-04-08 00:00	OFF	17	5

Gambar Tabel Insiden



- *Transform*

1. Cleaning

Field status_recovery pada tabel insiden dihilangkan ketika proses *transformasi*

Nama Field	Tipe Data	Panjang Data	Kunci	Keterangan
kode_insiden	*int*		PK	*not null*
waktu_kejadian	*datetime*			*not null*
status_recovery	*varchar*	20		*not null*
ID_website	*int*		FK	*not null*
ID_jenis_domain	*int*		FK	*not null*



Nama Field	Tipe Data	Panjang Data	Kunci	Keterangan
kode_insiden	*int*		PK	*not null*
waktu_kejadian	*datetime*			*not null*
ID_website	*int*		FK	*not null*
ID_jenis_domain	*int*		FK	*not null*

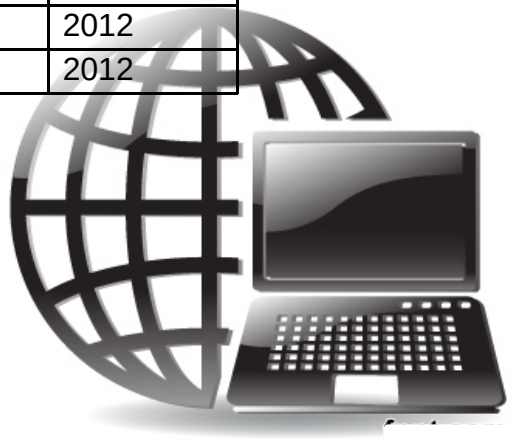


2. Conditioning

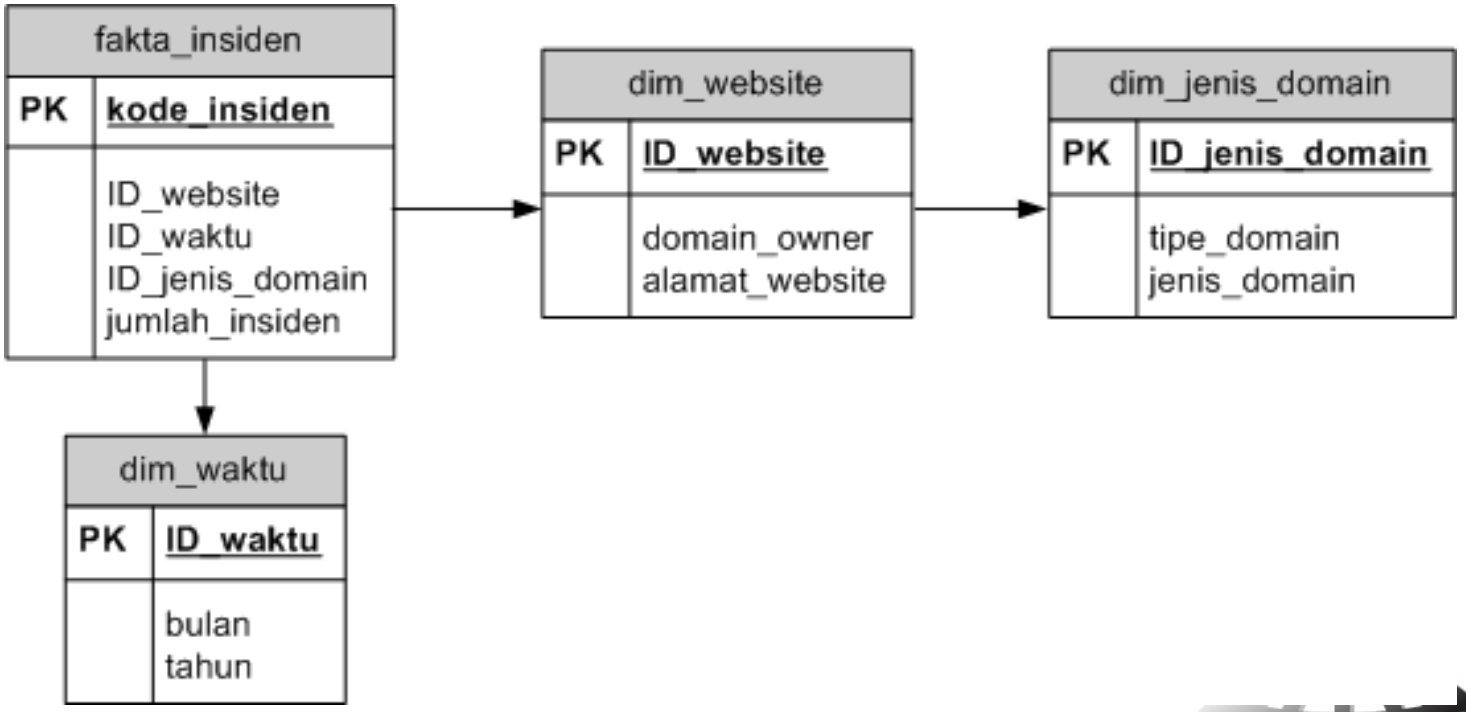
Tabel field waktu_kejadian pada tabel insiden menjadi dim_waktu

kode_insiden	ID_website	waktu_kejadian	jumlah_insiden
1	1	3/4/2012 0:00	50
2	2	31/3/2012 0:00	40
3	3	1/4/2012 0:00	30
4	4	2/4/2012 0:00	20
5	5	26/3/2012 0:00	60
6	6	2/4/2012 0:00	10

ID_Waktu	Bulan	Tahun
01	4	2012
02	3	2012
03	4	2012



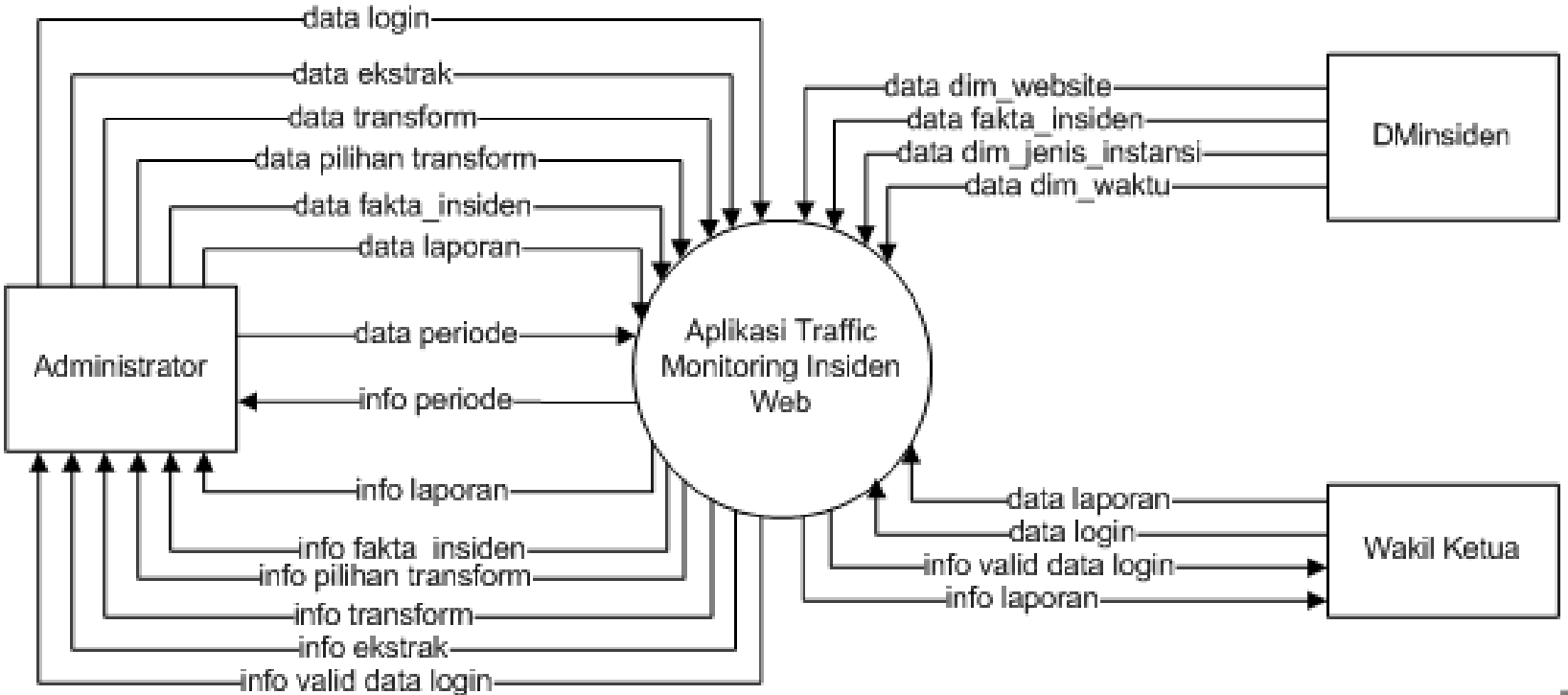
Skema Data Mart



Snowflake Schema

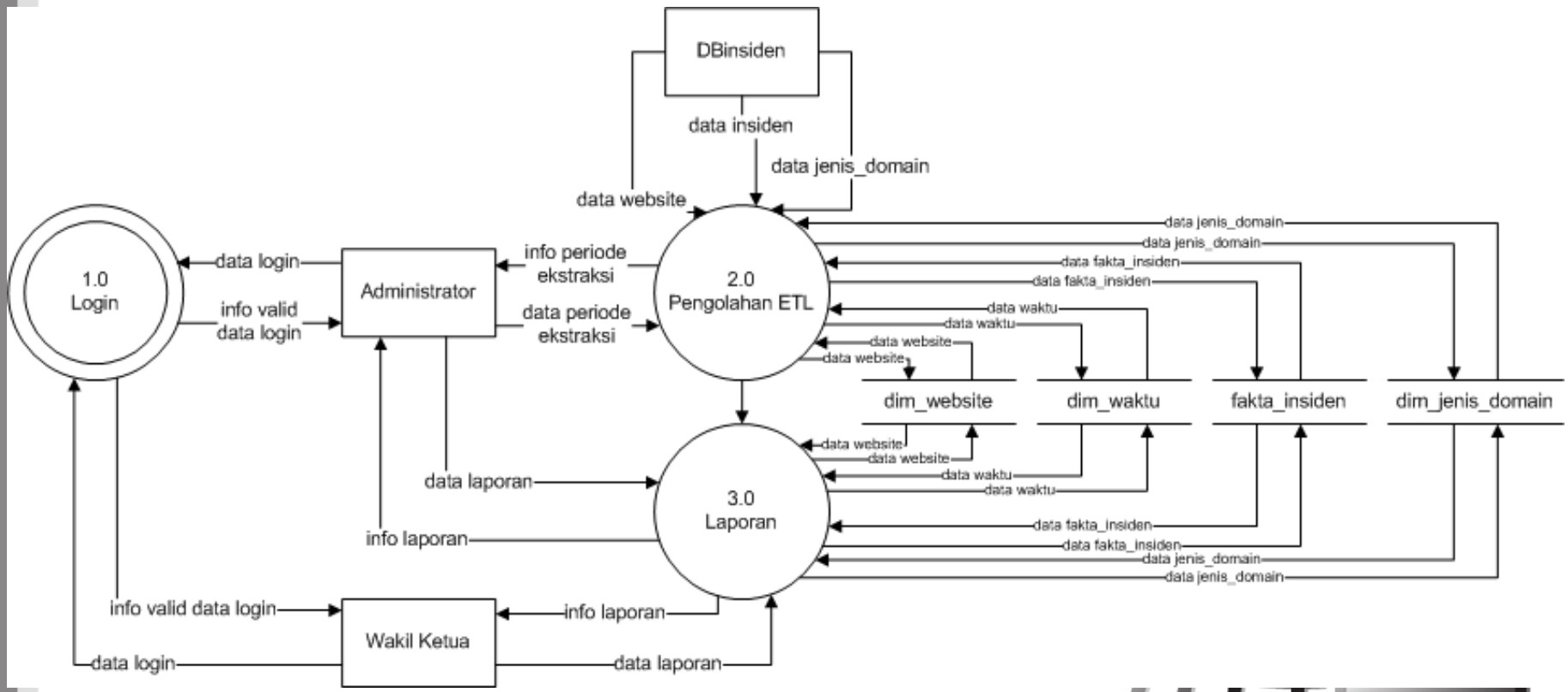


Diagram Konteks



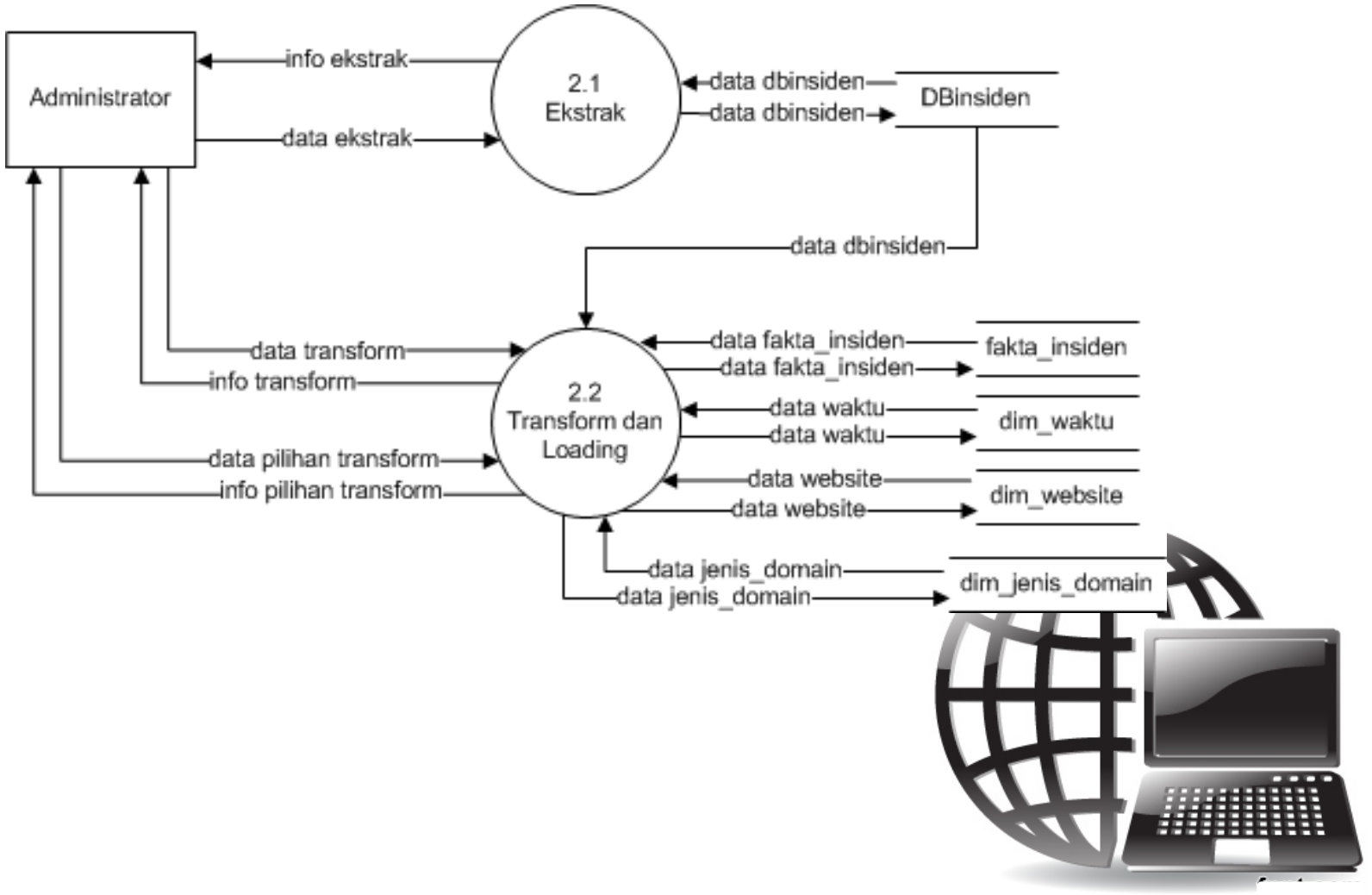


DFD Level 1

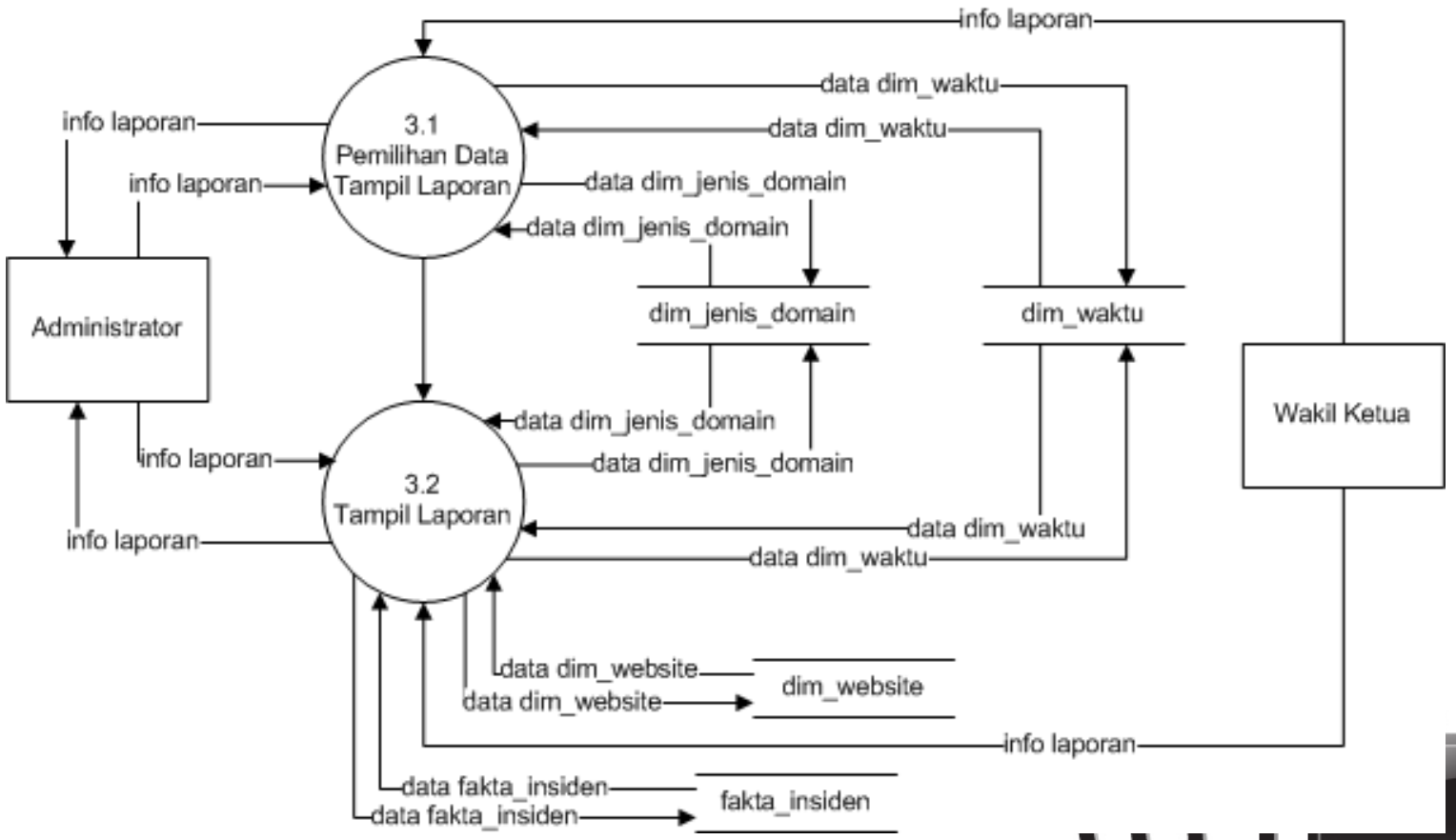

DBinsiden
data insiden
data jenis_domain
data website
1.0
Login
data login
info valid
data login
Administrator
info periode
ekstraksi
data periode
ekstraksi
2.0
Pengolahan ETL
data jenis_domain
data jenis_domain
data fakta_insiden
data fakta_insiden
data waktu
data waktu
data website
data website
dim_website
dim_waktu
fakta_insiden
dim_jenis_domain
data website
data website
data waktu
data waktu
data laporan
3.0
Laporan
info laporan
data fakta_insiden
data fakta_insiden
data jenis_domain
data jenis_domain
info valid data login
Wakil Ketua
info laporan
data login
data laporan



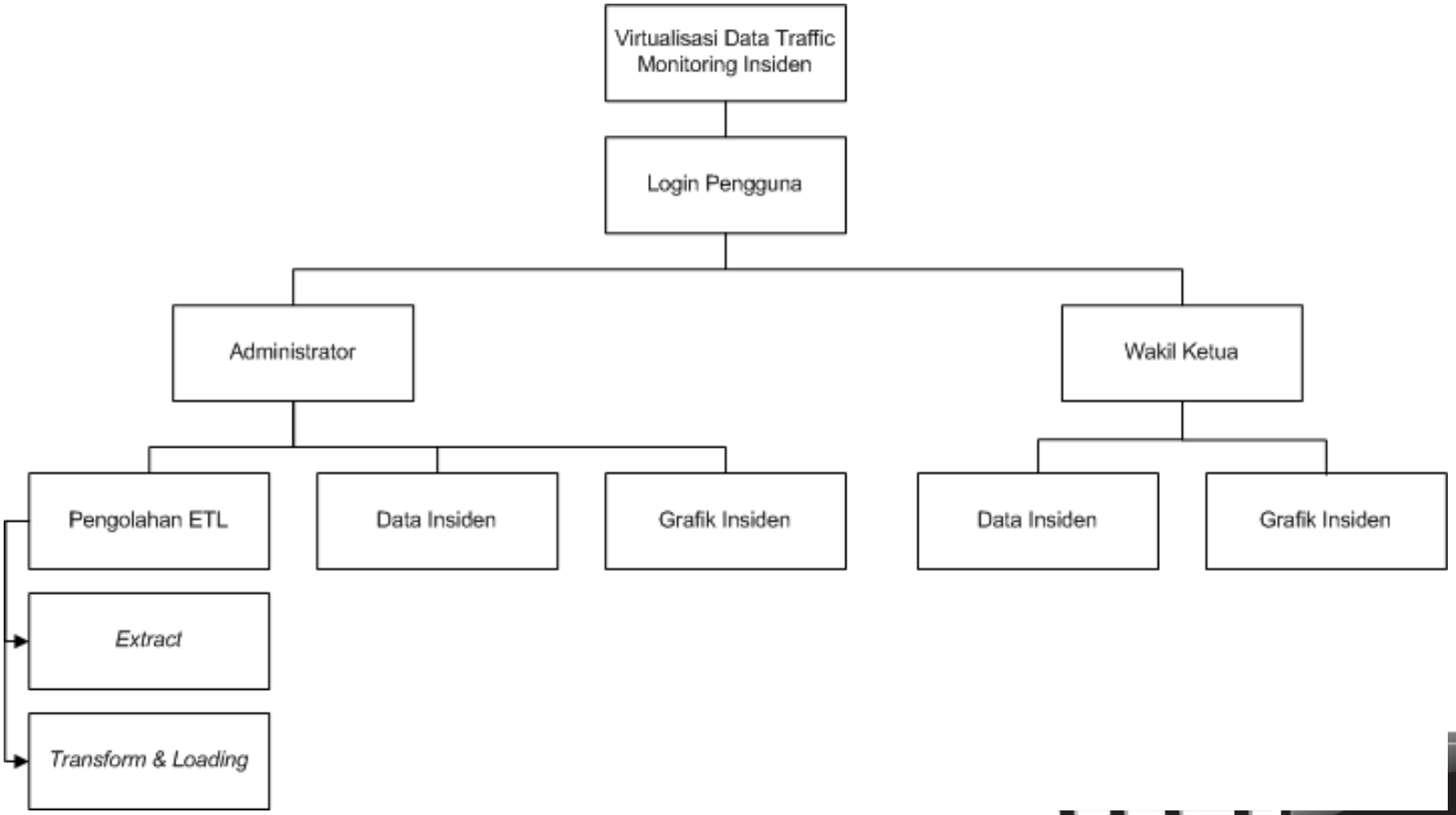
DFD Level 2 Proses Pengolahan ETL



DFD Level 3 Proses Laporan



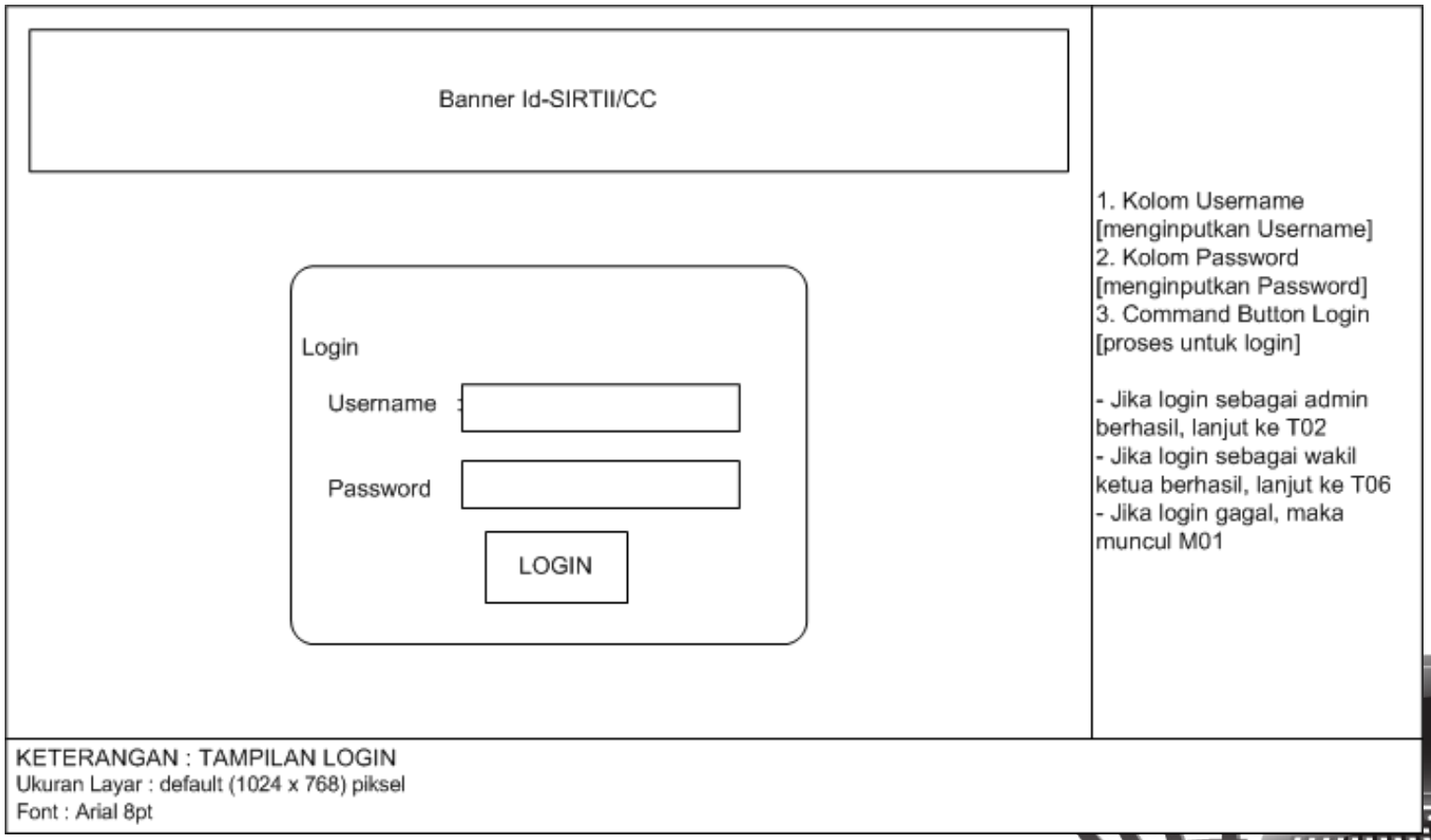
Struktur Menu





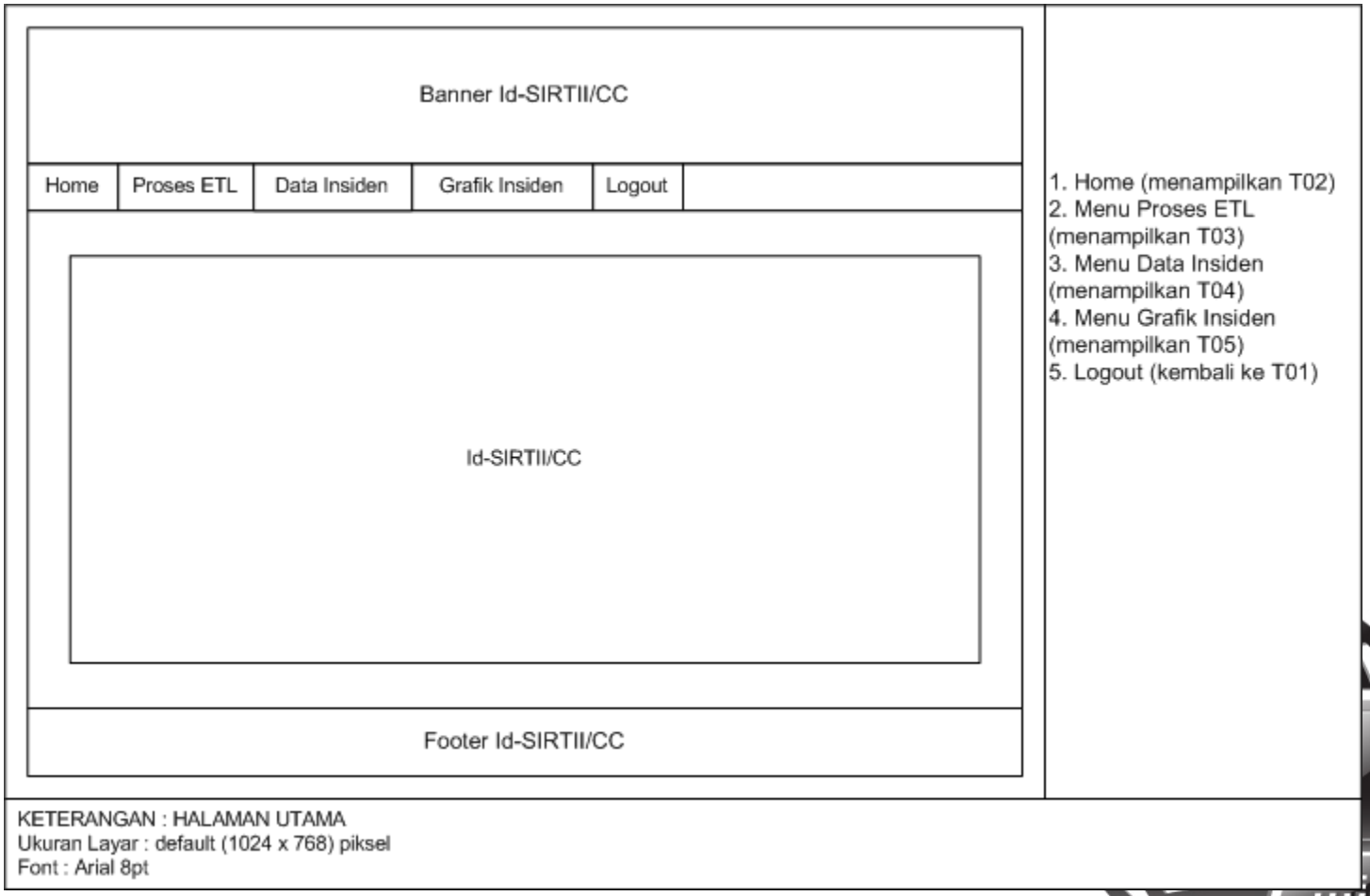
Perancangan Antarmuka

HALAMAN LOGIN



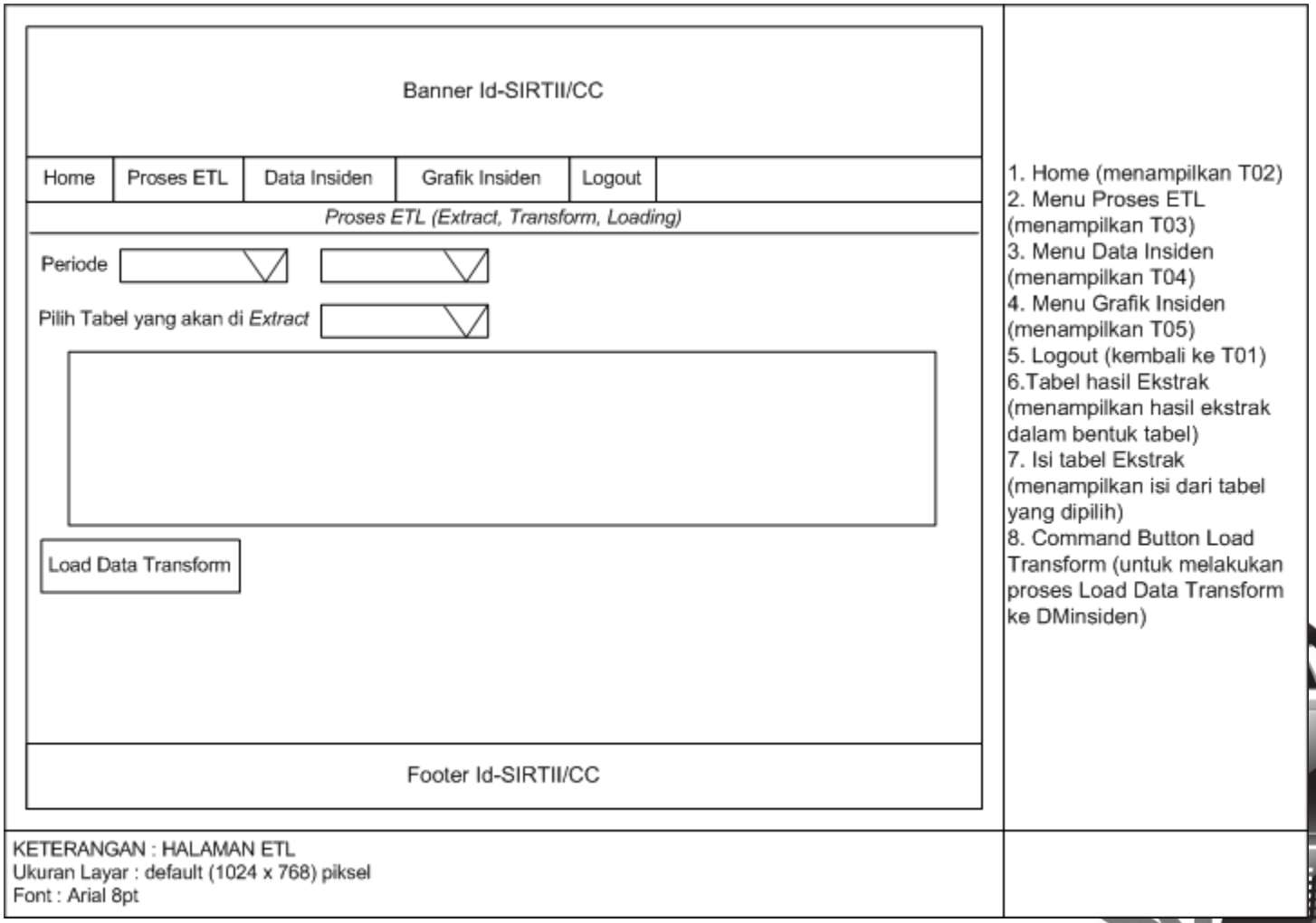
Perancangan Antarmuka

HALAMAN MENU UTAMA



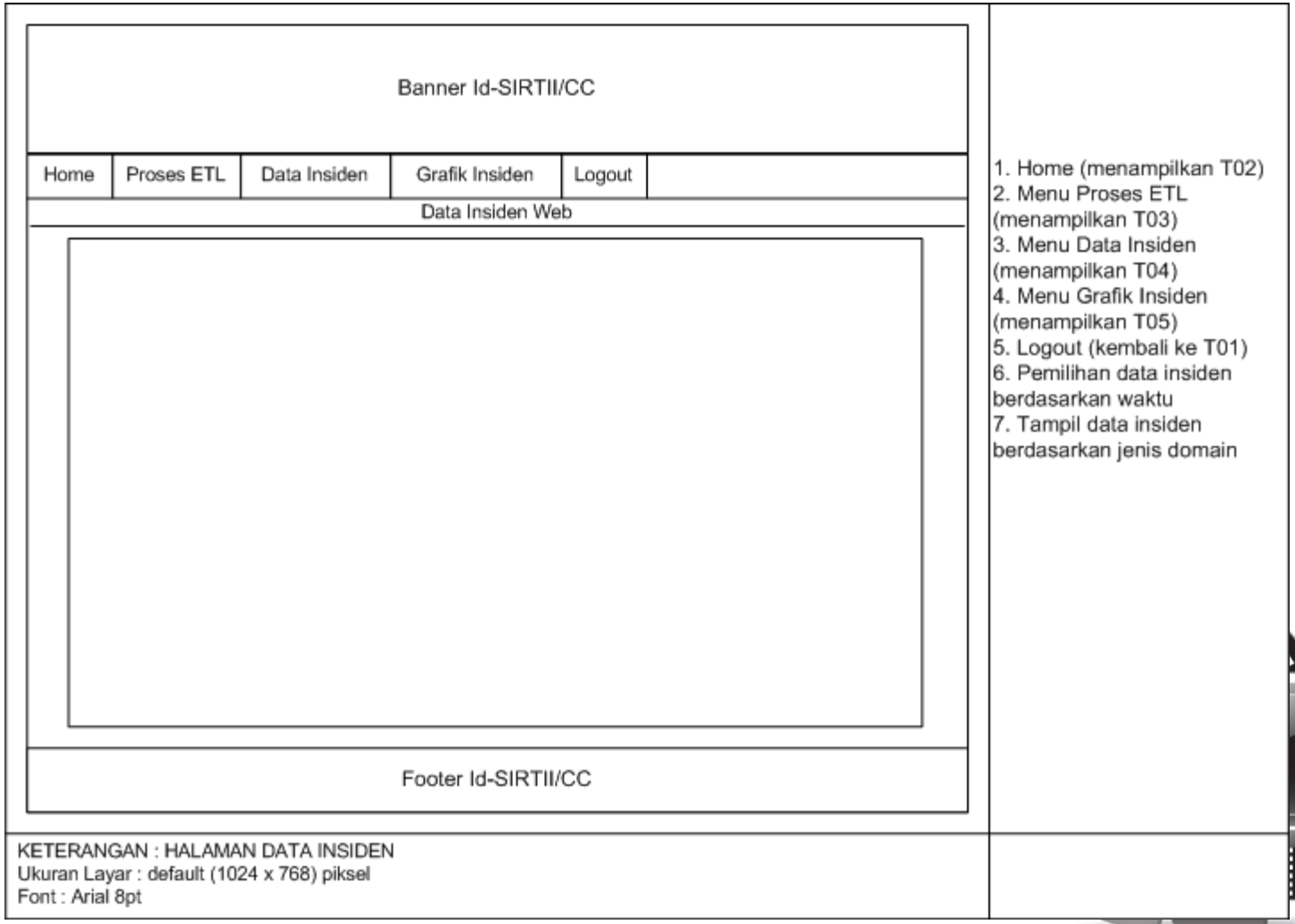
Perancangan Antarmuka

HALAMAN MENU PROSES ETL



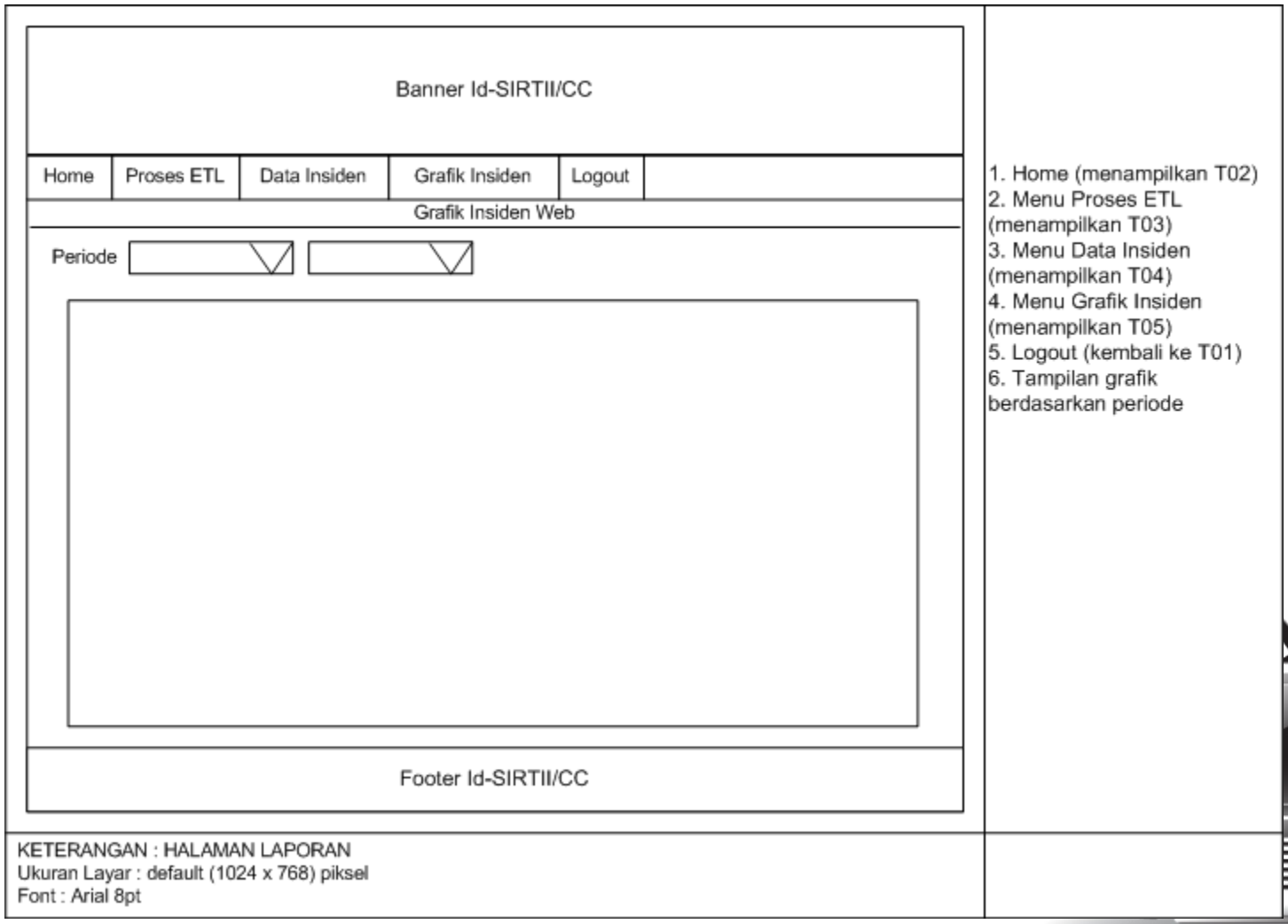
Perancangan Antarmuka

HALAMAN MENU DATA INSIDEN



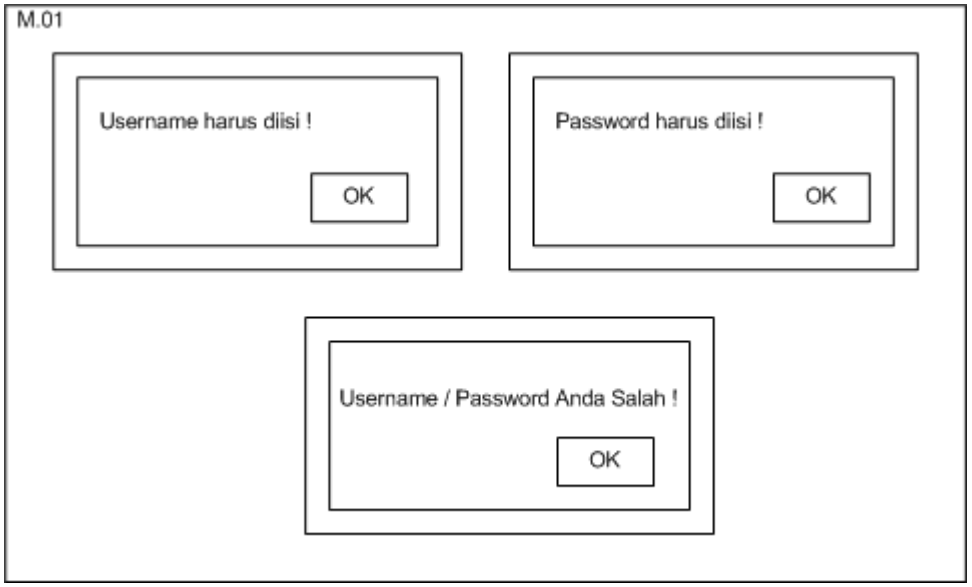
Perancangan Antarmuka

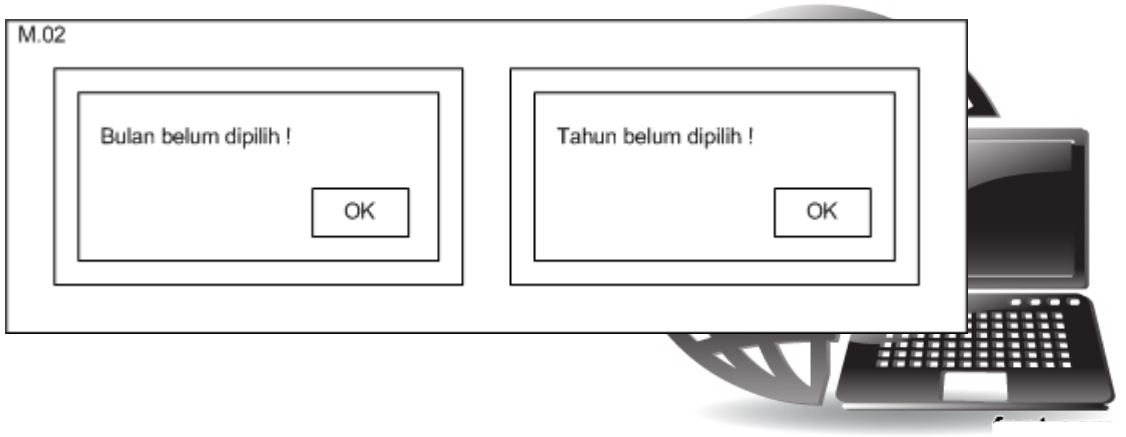
HALAMAN MENU GRAFIK INSIDEN



Perancangan Antarmuka

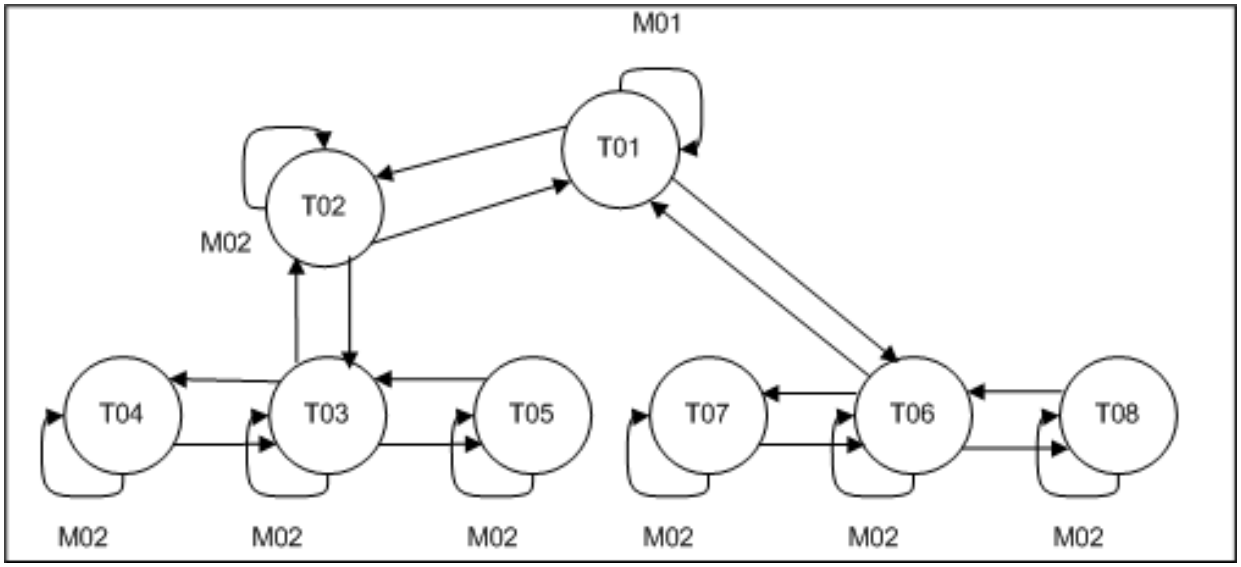
PESAN ERROR





Perancangan Antarmuka

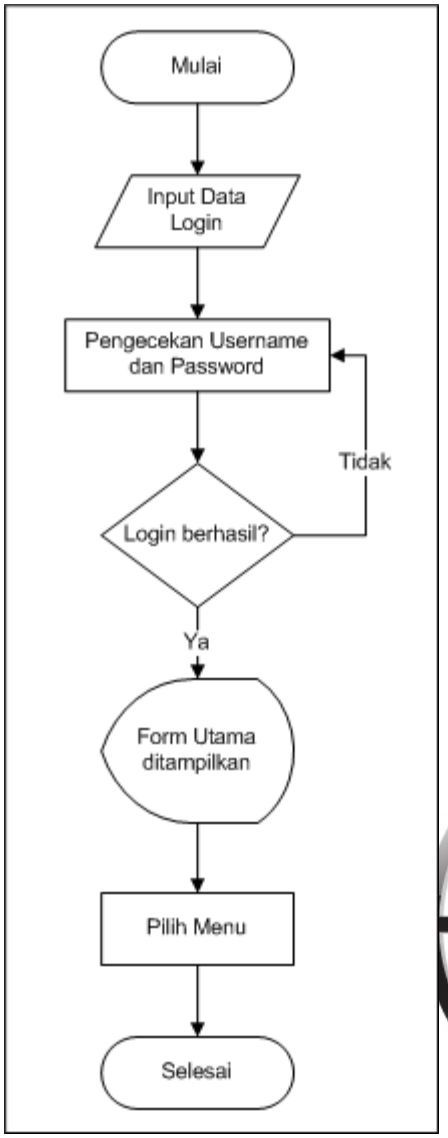
JARINGAN SEMANTIK





Perancangan Prosedural

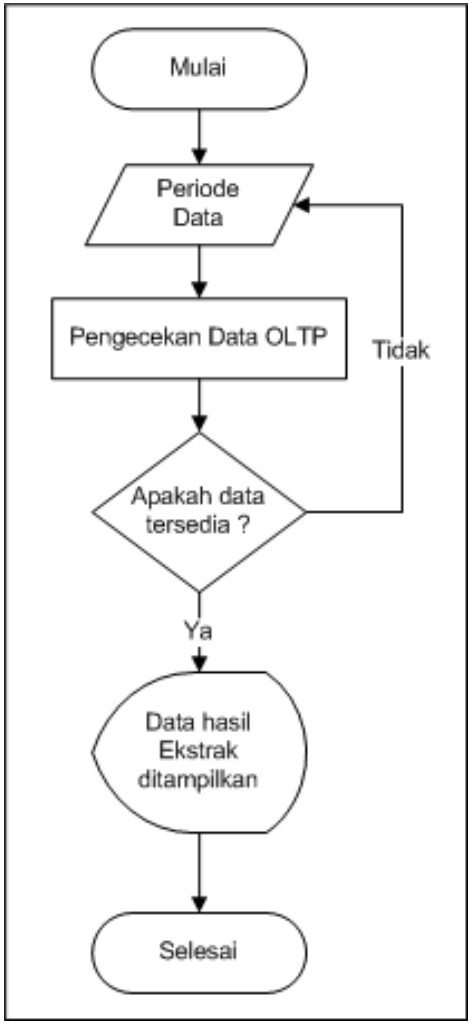
Prosedural Login





Perancangan Prosedural

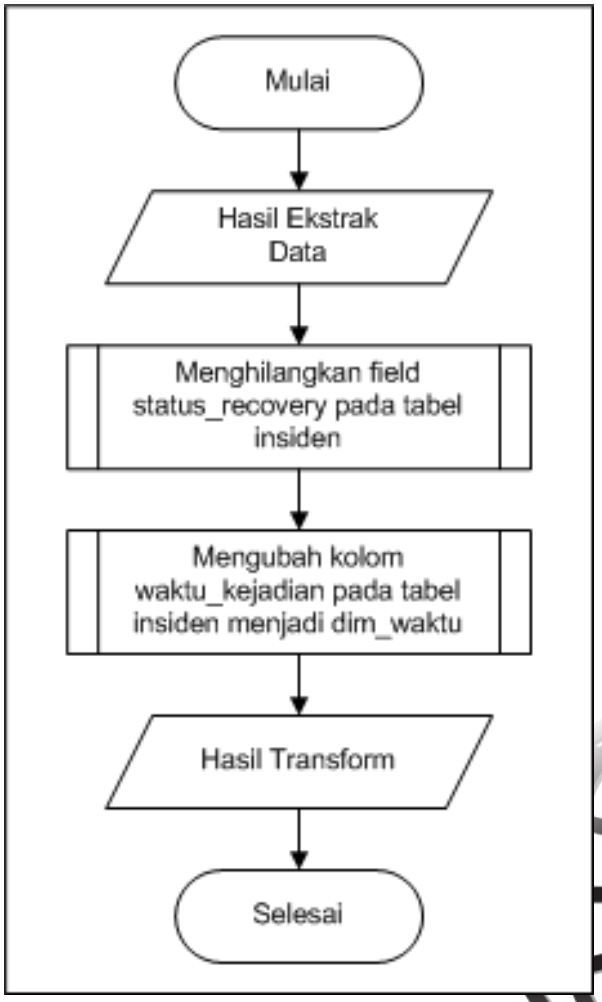
Prosedural Ekstrak





Perancangan Prosedural

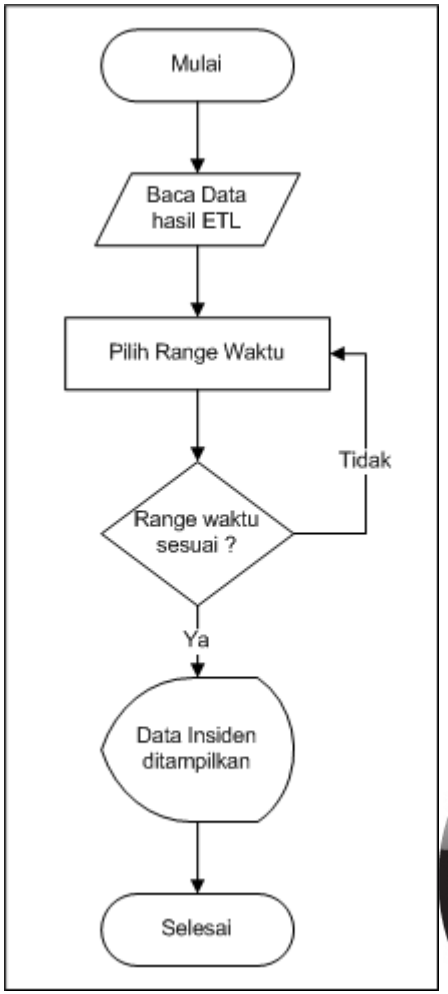
Prosedural Transform





Perancangan Prosedural

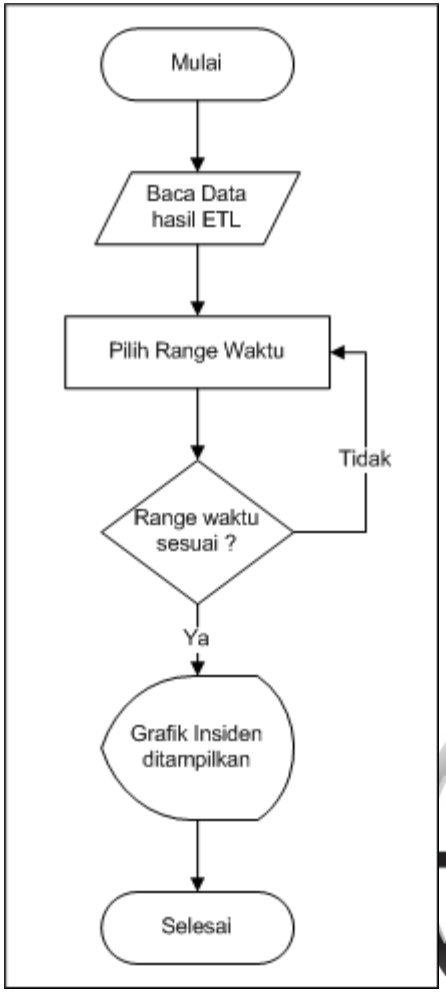
Prosedural Data Insiden





Perancangan Prosedural

Prosedural Grafik Insiden





KESIMPULAN DAN SARAN

Kesimpulan

1. Aplikasi ini dapat memudahkan staf *Laboratorium Data Mining Deputy of Research and Development* Id-SIRTII/CC dalam menganalisa data insiden web.
2. Aplikasi ini dapat memudahkan Wakil Ketua Id-SIRTII/CC dalam memonitoring insiden web yang berdomain Indonesia.
3. Aplikasi ini dapat membantu Wakil Ketua Id-SIRTII/CC dalam menghasilkan laporan yang digunakan untuk melihat insiden web yang berdomain Indonesia.

Saran

1. Aplikasi untuk kedepannya bisa dikembangkan menjadi aplikasi website dengan menerapkan sistem *data warehouse* terdistribusi (*Distributed Data Warehouse).*



Terima kasih ☺

