BAB II
TINJAUAN PUSTAKA

2.1. Profil Tempat Kerja Praktek

Balai Pengkajian dan Pengembangan Komunikasi dan Informatika (BPPKI) Bandung seperti tertuang di dalam Peraturan Menteri Komunikasi dan Informatika No. 22/PER/M.KOMINFO/6/2008 adalah Unit Pelaksana Teknis (UPT) di lingkungan Badan Penelitian dan Pengembangan Sumber Daya Manusia (Badan Litbang SDM), Kementrian Komunikasi dan Informatika Republik Indonesia. BPPKI berada di bawah dan bertanggung jawab kepada Kepala Badan Penelitian dan Pengembangan SDM, dan secara administratif dibina oleh Sekretaris Badan Penelitian dan Pengembangan SDM.

Berikut ini adalah visi dan misi BPPKI Bandung :

Visi BPPKI Bandung

Berkembangnya tata informasi masyarakat berbasis telematika yang sehat, lancar, murah, dan bermanfaat melalui fasilitasi layanan informasi dan data *research.*

Misi BPPKI Bandung

- Mengembangkan hasil kegiatan pengkajian komunikasi dan informatika untuk terciptanya kualitas masukan (*inputs*) terhadap *user*.
- Meningkatkan pengembangan pengkajian komunikasi dan informatika sebagai daya dukung pembaruan sistem informasi masyarakat.
- Mengembangkan SDM profesional sesuai tuntutan zaman serta mampu menjalankan tugas dan fungsi pelayanan informasi kepada *user* secara prima.
- Menyediakan dan menyebarluarkan informasi nasional dan daerah sebagai bentuk komitmen pertanggungjawaban sosial ke masyarakat
- Mewujudkan standar aplikasi pemanfaatan telematika di masyarakat.

2.1.1. Sejarah Instansi

Bila melihat riwayat pendiriannya, BPPKI berasal dari sebuah bentukan lembaga yang bernama Lembaga Penelitian dan Pendapat Umum atau LPPU yang didirikan pada tahun 1975 dan berada dalam lingkup organisasi Kementerian Penerangan, dengan penggagas datang dari kalangan pers waktu itu antara lain Harian Umum Pikiran Rakyat Bandung. Pada tahun 1977, LPPU berganti nomenklatur menjadi Balai Penelitian dan Pendapat Umum atau BP3U. Tahun 2002 hingga tahun 2008 BP3U berganti nama menjadi Balai Pengkajian dan Pengembangan Informasi atau BPPI. Sejak Tahun 2008 hingga sekarang BPPI menjadi Balai Pengkajian dan Pengembangan Komunikasi dan Informatika Bandung (BPPKI). Sampai saat ini lembaga ini telah dipimpin oleh enam orang kepala balai.

Tabel 2.1. Nama-Nama Kepala Balai

No	Nama Pejabat	Jabatan	Periode
1.	Drs. Eyo Kahya	Kepala LPPU	1975 – 1977
2.	Drs. T.U. Pasaribu	Kepala BP3U	1977 – 1997
3.	Drs. H.Marullah Pribady	Kepala BP3U	1997 – 2002
4.	Drs. Maman Darisman	Kepala BP3U	2002 – 2005
5.	Drs. Sumarsono, M.Si.	Kepala BPPI	2005 – 2008
6.	Drs. Ramon, M.Si.	Kepala BPPKI	2008- sekarang

2.1.2. Logo Instansi

Visualisasi Logo Logo Kementerian Komunikasi dan Informatika (Kemkominfo) :

a. Bentuk dasar mengambil dari unsur-unsur sebagai berikut :

1. Secara menye1uruh bentuk logo ini terbentuk dari susunan tiga huruf C yang merupakan singkatan dari : *Communication, Content and Computer,* yang merupakan bidang utama tugas Kemkominfo.



Gambar 2.1. Logo Kementrian Komunikasi dan Informatika

2. Bentuk geometris yang membentuk tiga bidang yang secara optis bersumber dari satu titik pusat memutar menyebar/melebar, mengandung pengertian bahwa Kemkominfo mempunyai tugas untuk meningkatkan akses komunikasi dan pos yang berkualitas, merata dan terjangkau, juga menggambarkan unsur kegiatan penyiaran. Bentuk ini pun menyiratkan kesan 'berkembang', sesuai dengan visi Kemkominfo dalam peningkatan litbang dan industri. Bentuk inipun secara garis besar membentuk lingkaran, menyiratkan kemandirian.
3. Secara sepintas bentuk logo ini menyerupai sebuah kerang, terinspirasi oleh Nafiri, alat komunikasi tradisional yang sering dipakai oleh leluhur bangsa Indonesia untuk berkomunikasi.

b. Warna :

1. Merupakan kombinasi warna biru, yang mempunyai karakter, Lugas, Kokoh, Teknologis, Dinamis, Optimis dan profesionalisme.
2. Aksen warna biru muda, selain menambah kesan estetis, juga menyiratkan pengertian "perlindungan terhadap kepentingan public" (digambarkan dengan bidang biru muda yang 'dipayungi' oleh dua bidang biru).

2.1.3. Landasan Hukum Kelembagaan

Landasan Hukum kelembagaan BPPKI adalah sebagai berikut :

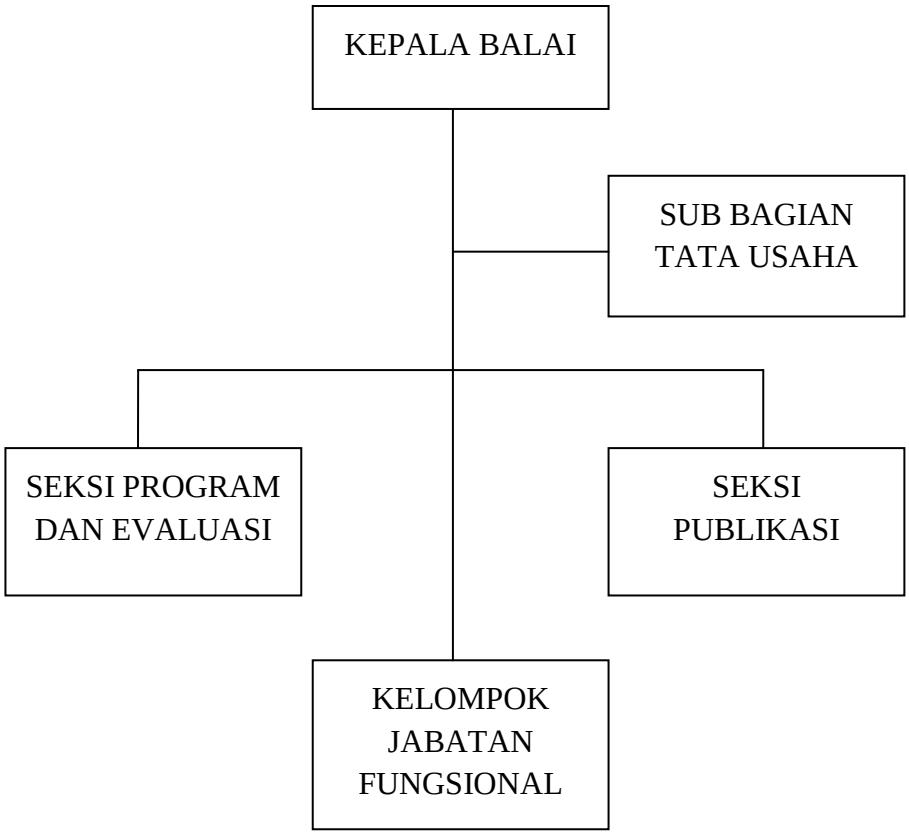
- Keputusan Presiden Nomor 187/M Tahun 2004 tentang Penetapan Pembentukan dan Pengangkatan Menteri-menteri Kabinet Indonesia Bersatu; sebagaimana telah diubah dengan Keputusan Presiden Nomor 8/M Tahun 2005;
- Peraturan Presiden RI Nomor 9 Tahun 2005 tentang Kedudukan, Tugas, Fungsi, Susunan Organisasi dan Tata Kerja Kementrian Negara RI;
- Peraturan Presiden RI Nomor 10 Tahun 2005 tentang Unit Organisasi dan Tugas Eselon I Kementrian Negara RI Nomor 15 Tahun 2005;
- Peraturan Mentri Komunikasi dan Informatika Nomor 01/P/M.KOMINFO/4/2005 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Informatika;
- Keputusan Menteri Komunikasi dan Informatika No. 84/Kep/M.Kominfo/10/2005 tentang Organisasi dan Tata Kerja Balai Pengkajian dan Pengembangan Informasi;
- Peraturan Menteri Komunikasi dan Informatika No. 22/PER/M.KOMINFO/6/2008 tentang Organisasi Dan Tata Kerja Unit Pelaksana Teknis Bidang Pengkajian Dan Pengembangan Komunikasi Dan Informatika.

2.1.4. Struktur Organisasi dan *Job Description*

Berikut ini adalah bagan organisasi Balai Pengkajian Dan Pengembangan Komunikasi Dan Informatika berdasarkan Lampiran II Peraturan Menteri Komunikasi dan Informatika No. 22/PER/M.KOMINFO/6/2008 tentang Organisasi Dan Tata Kerja Unit Pelaksana Teknis Bidang Pengkajian Dan Pengembangan Komunikasi Dan Informatika.

BPPKI dipimpin oleh seorang Kepala, dengan jabatan eselon IIIa. Susunan organisasi BPPKI terdiri dari Kepala Subbagian dan Kepala Seksi setingkat jabatan eselon IVa; yaitu;

- *Subbagian Tata Usaha* yang mempunyai tugas melakukan urusan tata usaha, kepegawaian, keuangan, perlengkapan, dan rumah tangga serta penyusunan laporan;



Gambar 2.2. Bagan Organisasi Balai Pengkajian Dan Pengembangan Komunikasi Dan Informatika

- *Seksi Program dan Evaluasi* meliputi penyusunan rencana program dan anggaran, pelaksanaan evaluasi, dan laporan di bidang pengkajian dan pengembangan komunikasi dan informatika;
- *Seksi Publikasi* melaksanakan publikasi hasil pengkajian dan pengembangan komunikasi dan informatika;
- *Kelompok Jabatan Fungsional* yang terdiri dari sejumlah jabatan fungsional yang terbagi dalam berbagai kelompok sesuai dengan bidang keahliannya, di mana setiap kelompok dikoordinasikan oleh pejabat fungsional senior yang ditunjuk oleh Kepala BPPKI. Kelompok Jabatan Fungsional terdiri dari sejumlah jabatan fungsional yang terbagi dalam berbagai kelompok sesuai dengan bidang keahliannya. Jumlah jabatan fungsional tersebut ditentukan berdasarkan kebutuhan dan beban kerja.

Sedangkan jenjang jabatan fungsional diatur sesuai dengan peraturan perundang-undangan yang berlaku.

Dalam melaksanakan tugasnya, BPPKI Bandung menyelenggarakan fungsi yang meliputi; penyusunan program pengkajian dan pengembangan informasi; pelaksanaan pengkajian dan pengembangan serta publikasi hasil pengkajian dan pengembangan informasi; evaluasi dan penyusunan laporan pelaksanaan pengkajian dan pengembangan informasi di daerah; serta pelaksanaan administrasi.

Kegiatan yang dilakukan BPPKI Bandung meliputi pengkajian dan pengembangan informasi. Pengkajian adalah aktivitas yang dilakukan dengan metode ilmiah terhadap objek tertentu sehingga dapat dihasilkan pengertian mendalam tentang objek tersebut. Sedangkan pengembangan adalah aktivitas ilmiah yang menghasilkan temuan baru dan model aplikatif yang dapat dipergunakan secara pragmatis.

Produk yang dihasilkan BPPKI Bandung tidak saja berupa data yang terdiri dari data dan informasi hasil kajian isu daerah dari media cetak - dilaksanakan setiap minggu atau 52 minggu dalam satu tahun - dan data serta informasi hasil penelitian lapangan, tetapi juga meliputi jasa berupa, layanan data dan informasi melalui perpustakaan, layanan jasa penelitian dan pengumpulan data.

Selain produk-produk dan layanan di bidang penelitian yang disebutkan sebelumnya, BPPKI Bandung juga memberikan layanan jasa informasi melalui akses internet gratis bagi pelajar dan mahasiswa berupa Galeri Internet. Galeri Internet ini dibuka sejak tahun 2009 dan mempunyai fasilitas ruangan khusus yang dilengkapi 15 komputer yang terkoneksi dengan internet.

2.2. Landasan Teori

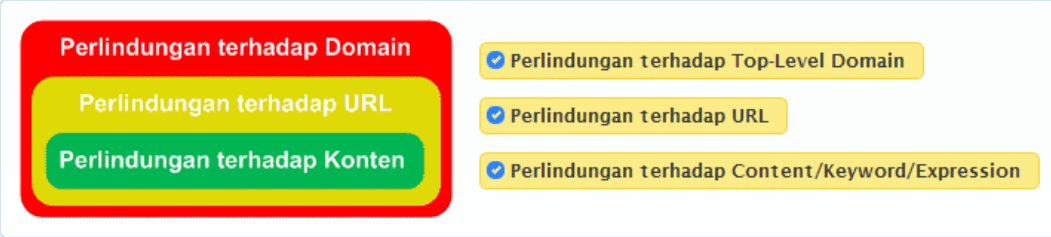
2.2.1. TRUST^{+} Positif

TRUST^{+} Positif (Terpercaya, Referensi Utama, Sehat, Teramankan) bertujuan memberikan akses internet yang aman dan sehat dengan perlindungan berdasarkan daftar informasi sehat dan terpercaya (TRUST^{+} List) sehingga

memberikan perlindungan pada masyarakat terhadap nilai-nilai etika, moral dan kaedah-kaedah yang tidak sesuai dengan citra Bangsa Indonesia; dan melakukan penghematan terhadap pemborosan penggunaan akses internet (*internet utilization*) di Indonesia (http://trustpositif.depkominfo.go.id/).

2.2.1.1. Model Perlindungan Dan Arsitektur TRUST+ Positif

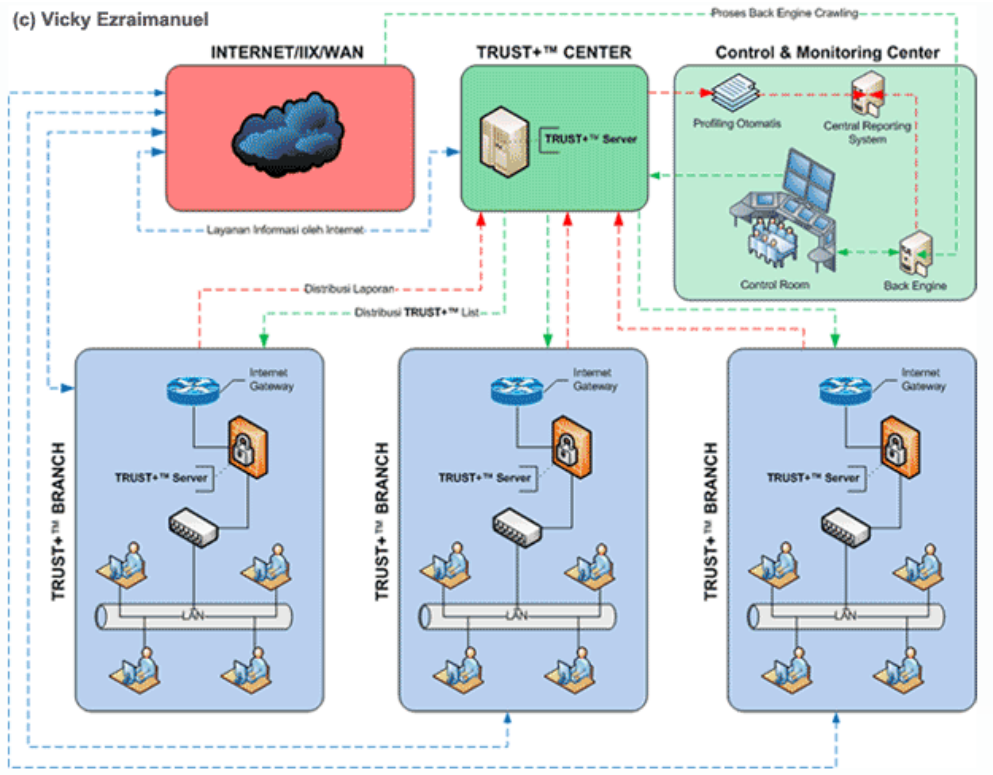
Sistem TRUST+ Positif menerapkan mekanisme kerja adanya server pusat yang akan menjadi acuan dan rujukan kepada seluruh layanan akses informasi publik (fasilitas bersama), serta menerima informasi-informasi dari fasilitas akses informasi publik untuk menjadi alat analisa dan profiling penggunaan internet di Indonesia.



Gambar 2.3. Model Perlindungan (TRUST+ List)

Dari segi arsitektur server TRUST+ Positif pusat bukan merupakan "*Single Gateway"* ataupun "*Traffic Relay"* untuk koneksi internet seluruh Indonesia dan Kementerian Komunikasi dan Informatika tidak mengakomodir trafik internet bagi seluruh ISP ataupun Organisasi pengguna TRUST+ Positif yang ada di Indonesia. Masing-masing pengguna akan menyediakan infrastruktur sesuai dengan kebutuhan yang ada pada zona masing-masing, di mana TRUST+ Positif Pusat akan berfungsi sebagai referensi atau rujukan database URL internet sehat.

Untuk meringankan beban koneksi antara server pusat (TRUST+ Center) dengan pusat layanan akses informasi publik, maka daftar informasi terpercaya dan positif (TRUST+ List) ditempatkan secara distribusi dan merata di seluruh server layanan akses informasi publik.



Gambar 2.4. Arsitektur TRUST^{+} Positif

2.2.1.2. Aplikasi dan Informasi Database TRUST^{+} Positif

TRUST^{+} Positif pada implementasinya memanfaatkan penggabungan antara 2 aplikasi, yaitu ***Proxy/Caching System*** dipadu dengan ***Content Filtering System***. Adapun aplikasi yang dipakai adalah : **Squid-Cache** sebagai Proxy/Caching System, dan **SquidGuard** sebagai Content Filtering System. Seperti disebutkan dalam http://trustpositif.depkominfo.go.id , paket aplikasi tersebut adalah tidak wajib untuk diimplementasikan jika hanya ingin memanfaatkan daftar URL dari database TRUST^{+} Positif, tanpa merubah konfigurasi ataupun sistem yang telah digunakan dengan menggunakan aplikasi lain yang mungkin sudah dgunakan. Walaupun tetap dianjurkan untuk menggunakan paket aplikasi tersebut, dengan tujuan pemaksimalan performa.

Jenis database yang ada bukanlah semata-mata hanya berisi Domain/URL/Keyword yang akan difilter atau diblock, tetapi merupakan jenis database secara umum, yang penggunaannya nanti bisa diarahkan kepada daftar yang dipercaya (daftar putih/terpercaya) ataupun daftar yang disaring (daftar hitam/tersaring).

Adapun jenis database yang dipakai dalam sistem TRUST^{+} Positif adalah sebagai berikut:

1. Daftar Domain

   Berisi daftar *Top-Level Domain*, misalkan '*facebook.com*'. Jika top-level domain ada pada daftar ini, maka seluruh virtual domain, URL, ataupun kata-kata/keyword yang berada pada domain yang bersangkutan (misalkan '**.facebook.com*', atau '*www.facebok.com/home.php*'), akan secara otomatis masuk dalam proses pemeriksaan.

2. Daftar URL

   Berisi daftar *URL tunggal*, misalkan '*www.facebook.com/pages/Everybody-Draw-Mohammed-Day/*'. URL yang ada pada daftar ini secara spesifik akan masuk dalam proses pemeriksaan,tanpa melibatkan pemeriksaan terhadap top-level domain ataupun URL lainnya pada domain yang sama.

3. Daftar Keyword

   Berisi daftar kata-kata/konten/keyword, tunggal ataupun gabungan, misalkan 'bokep', 'tante girang', dan lain sebagainya. Jika keyword yang dimaksud berada pada daftar ini, maka akan secara otomatis diperiksa tanpa melibatkan pemeriksaan terhadap top-level domain atau URLnya. Daftar keyword ini secara khusus berisikan 'regular expression', sehingga memungkin kita untuk melakukan kombinasi dari berbagai kata. Misalkan, jika kita mencari kata 'girang', maka akan lolos penyaringan, tapi jika kita menggabungkan kata tersebut menjadi 'tante girang', maka akan tersaring.

Berikut ini adalah kategori database yang dipakai dalam sistem TRUST^{+} Positif :

1. Daftar Putih (Positif/Terpercaya**)**

   Daftar dalam kategori database ini adalah daftar **Domain/URL positif yang terpercaya,** misalkan domain pemerintah, media online, dan lain sebagainya. Pada TRUST+™ Positif database ini dinamakan 'whitelist'.

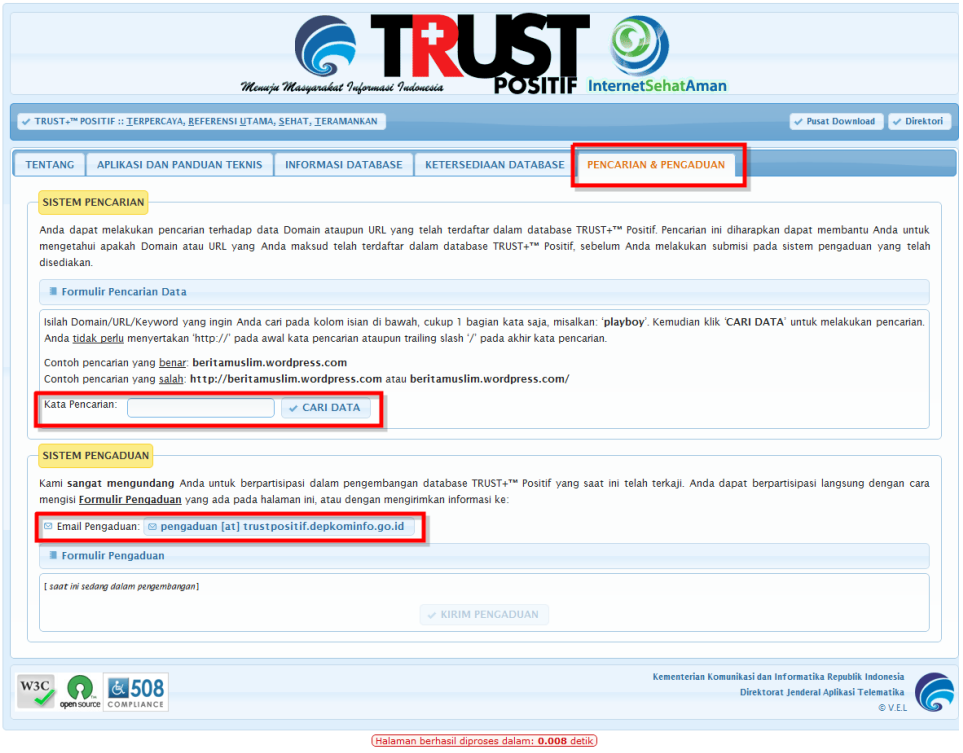
2. Daftar Hitam (Negatif/Tersaring)

Daftar dalam kategori database ini adalah daftar **Domain/URL/Keyword negatif yang akan disaring**, misalkan pornografi, dan lain sebagainya. Daftar Hitam yang ada saat ini dibagi menjadi 3 sub-kategori, yaitu:

- Database dari **Hasil Pelaporan dan Kajian** (Pada TRUST$^+$ Positif database ini dinamakan 'blacklist').
- Database **Pornografi Internasional** secara spesifik (Pada TRUST$^+$ Positif database ini dinamakan 'porn').
- Database **Open-Proxy** secara spesifik (Pada TRUST$^+$ Positif database ini dinamakan 'redirector').

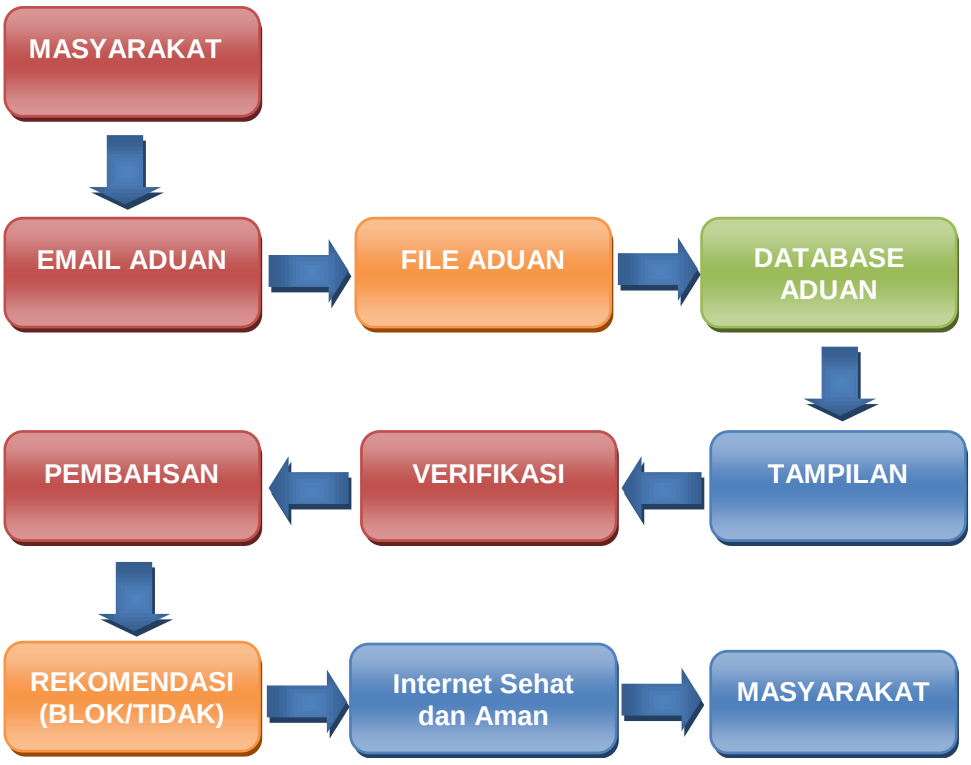
2.2.1.3. Sistem Pencarian dan Pengaduan TRUST$^+$ Positif

Informasi ketersediaan database yang dipakai dalam sistem TRUST$^+$ Positif selalu di-*update* setiap hari bedasarkan kategorinya (hal ini dapat dilihat di situs http://trustpositif.depkominfo.go.id pada menu "KETERSEDIAAN DATABASE").



Gambar 2.5. Situs Sistem Pencarian dan Pengaduan TRUST$^+$ Positif (http://trustpositif.depkominfo.go.id)

Update yang dipakai dalam sistem TRUST^{+} Positif mengikut-sertakan peran aktif pengguna internet khususnya pengguna internet di Indonesia dengan mengikuti prosedur pencarian dan pengaduan yang terdapat di http://trustpositif.depkominfo.go.id pada menu "**PENCARIAN & PENGADUAN**". Untuk melakukan pengaduan, pengguna internet disarankan untuk melakukan pencarian terlebih dahulu pada situs tersebut dan apabila memang tidak terdapat dalam database terkini, maka pengguna internet dapat melakukan pengaduan dengan menggunakan sistem pengaduan yang telah disediakan (saat laporan kerja praktek ini dibuat sistem pengaduan hanya dapat diakses dengan menggunakan mengirimkan email pengaduan ke pengaduan@trustpositif.depkominfo.go.id).



Gambar 2.6. Mekanisme Pengaduan TRUST^{+} Positif

2.2.2. Proxy Server

Proxy Server adalah server yang berguna sebagai perantara antara pengguna sebelum terhubungan ke Internet. Proxy server bertindak sebagai

penyaring/*filter* paket yang datang dari Internet, baik itu melalui port http atau ftp, sebelum sampai ke pengguna. Dengan adanya proxy server ini, maka url/situs yang sering di-*browsing* akan semakin terasa semakin cepat terakses oleh user, karena telah disimpan di dalam *cache proxy.* Selain itu, proxy server juga memiliki fungsi lainnya, di antaranya autentifikasi pengguna mana saja yang diperbolehkan *browsing*, memblok situs-situs porno yang sering membawa *spyware*, memblok *banner*, membatasi ukuran *file* yang diunduh pengguna, me-*redirect* suatu situs porno ke situs lainnya, dan lain-lain. Salah satu software proxy terbaik yang ada di GNU/Linux adalah **Squid.** Squid adalah software proxy server open source dengan banyak fitur.

2.2.2.1. Squid

Squid adalah sebuah daemon yang digunakan sebagai *proxy server* dan *web cache*. Squid memiliki banyak jenis penggunaan, mulai dari mempercepat server web dengan melakukan *caching* permintaan yang berulang-ulang, *caching* DNS, *caching* situs web, dan *caching* pencarian komputer di dalam jaringan untuk sekelompok komputer yang menggunakan sumber daya jaringan yang sama, hingga pada membantu keamanan dengan cara melakukan penyaringan (*filter*) lalu lintas. Meskipun seringnya digunakan untuk protokol HTTP dan FTP, Squid juga menawarkan dukungan terbatas untuk beberapa protokol lainnya termasuk *Transport Layer Security* (TLS), Secure Socket Layer(SSL), Internet Gopher, dan HTTPS. Versi Squid 3.1 mencakup dukungan protokol IPv6 dan Internet Content Adaptation Protocol (ICAP).

Squid pada awalnya dikembangkan oleh Duane Wessels sebagai "**Harvest object cache**", yang merupakan bagian dari proyek Harvest yang dikembangkan di University of Colorado at Boulder. Pekerjaan selanjutnya dilakukan hingga selesai di University of California, San Diego dan didanai melalui National Science Foundation. Squid kini hampir secara eksklusif dikembangkan dengan cara usaha sukarela.

Squid umumnya didesain untuk berjalan di atas sistem operasi mirip UNIX, meski Squid juga bisa berjalan di atas sistem operasi Windows. Karena

dirilis di bawah lisensiGNU General Public License, maka Squid merupakan perangkat lunak bebas.

2.2.2.2. Web Proxy

Caching merupakan sebuah cara untuk menyimpan objek-objek Internet yang diminta (seperti halnya data halaman web) yang bisa diakses melalui HTTP, FTP dan Gopher di dalam sebuah sistem yang lebih dekat dengan situs yang memintanya. Beberapa penjelajah web dapat menggunakan *cache* Squid lokal untuk sebagai *server proxy HTTP*, sehingga dapat mengurangi waktu akses dan juga tentu saja konsumsi *bandwidth*. Hal ini sering berguna bagi para penyedia layanan Internet untuk meningkatkan kecepatan kepada para pelanggannya, dan LAN yang membagi saluran Internet. Karena memang bentuknya sebagai *proxy* (ia berlaku sebagaimana layaknya klien, sesuai dengan permintaan klien), *web cache* bisa menyediakan anonimitas dan keamanan. Tapi, *web cache* juga bisa menjadi masalah yang signifikan bila melihat maslah privasi, karena memang ia dapat mencatat banyak data, termasuk URL yang diminta oleh klien, kapan hal itu terjadi, nama dan versi penjelajah web yang digunakan klien serta sistem operasinya, dan dari mana ia mengakses situs itu.

Selanjutnya, sebuah program klien (sebagai contoh adalah penjelajah web) bisa menentukan secara ekplisit *proxy server* yang digunakan bila memang hendak menggunakan proxy (umumnya bagi para pelanggan ISP) atau bisa juga menggunakan proxy tanpa konfigurasi ekstra, yang sering disebut sebagai "*Transparent Caching*", di mana semua permintaan HTTP ke jaringan luar akan diolah oleh *proxy server* dan semua respons disimpan di dalam *cache*. Kasus kedua umumnya dilakukan di dalam perusahaan dan korporasi (semua klien berada di dalam LAN yang sama) dan sering memiliki masalah privasi yang disebutkan di atas.

Squid memiliki banyak fitur yang bisa membantu melakukan koneksi secara anonim, seperti memodifikasi atau mematikan beberapa *field header* tertentu dalam sebuah permintaan HTTP yang diajukan oleh klien. Saat itu terpenuhi, apa yang akan dilakukan oleh Squid adalah tergantung orang yang

menangani komputer yang menjalankan Squid. Orang yang meminta halaman web melalui sebuah jaringan yang secara transparan yang menggunakan biasanya tidak mengetahui bahwa informasi semua permintaan HTTP yang mereka ajukan dicatat oleh Squid.

2.2.3. SquidGuard

SquidGuard adalah kombinasi *filter*, *redirector* dan *access controller plugin* untuk Squid. SquidGuard bersifat : *free* (GPLv2), sangat fleksibel, sangat cepat, mudah diinstal, portabel. SquidGuard dapat digunakan untuk :

- membatasi akses web untuk beberapa pengguna sehingga hanya dapat mengakses web yang masuk dalam daftar diterima/web server yang terkenal dan/atau URL saja.
- memblokir akses ke beberapa server web yang terdaftar atau masuk dalam daftar hitam dan/atau URL untuk beberapa pengguna.
- memblokir akses ke URL yang cocok dengan suatu daftar ekspresi reguler atau kata-kata untuk beberapa pengguna.
- menegakkan penggunaan *domain names*/melarang penggunaan alamat IP dalam URL.
- Mengalihkan URL yang diblokir ke halaman lain.
- mengarahkan pengguna yang belum terdaftar ke formulir pendaftaran pengguna proxy server.
- pengalihan *link* download popule ke link lokal dalam negeri.
- pengalihan gambar *banner* ke file GIF kosong.
- memiliki aturan akses yang berbeda berdasarkan waktu hari, hari minggu, tanggal, dan lain-lain.
- memiliki aturan yang berbeda untuk kelompok pengguna yang berbeda.
- dan banyak lagi.

Baik SquidGuard maupun Squid dapat digunakan untuk :

- filter/sensor/mengedit teks dalam dokumen

- filter/sensor/edit bahasa *scripting* di-*embed* seperti JavaScript atau VBScript dalam HTML.

SquidGuard mempunyai banyak konfigurasi pilihan *powerfull* yang memungkinkan untuk :

1. menentukan ruang waktu yang berbeda didasarkan kombinasi yang wajar terhdap :
   - waktu dalam satu hari (misalnya : 0:00-8:00, 17:00-24:00)
   - hari dalam satu minggu (misalnya : sun, sa)
   - tanggal (misalnya : 1999/5/13)
   - rentang tanggal (misalnya :1999-04-01-1999-04-05)
   - tanggal *wildcard* (misalnya : 01-01 *- *- *- 05-17 12-25)
2. pengelompokan grup (pengguna/klien) ke dalam kategori yang berbeda seperti "manajer", "karyawan", "guru", "mahasiswa", "pelanggan", "tamu" dll berdasarkan kombinasi yang wajar :
      - Alamat IP dengan rentang
        - notasi awalan (172.16.0.0/12)
        - notasi *netmask* (172.16.0.0/255.240.0.0)
        - notasi awal-terakhir (172.16.0.11-172.16.0.35)
      - daftar alamat (172.16.134.54 172.16.156.23 ...)
      - daftar domain (foo.bar.com ...)
      - daftar user id *(*dfhj weho Asef sdgh ...)
   - dan secara opsional link kelompok untuk ruang waktu tertentu
      - positif (dalam jam kerja)
      - negatif (di luar waktu kerja)
3. pengelompokan tujuan (URL/server) ke dalam kategori yang berbeda seperti "lokal", "pelanggan", "vendor", "banner", "dilarang" dll berdasarkan jumlah yang tidak terbatas dalam daftar terbatas :
      - domain, termasuk subdomain *(foo.bar.com)*
      - host *(host.foo.bar.com)*
      - URL direktori, termasuk subdirektori *(foo.bar.com / beberapa direktori /)*

- file URL *(foo.bar.com / suatu tempat / file.html)*
- regular expressions *((expr1 | expr2 |...))*

dan secara opsional link kelompok untuk ruang waktu tertentu:

- positif (dalam jam kerja*)*
- negatif (di luar waktu kerja)

4. menulis ulang/*redirect URL* didasarkan pada kombinasi yang wajar :
   - pengeditan string/ekspresi reguler dengan :
     - *silent squid redirecting rewrite* (*s@from@to@[i]*)
     - *visible client redirecting rewrite* (*s@from@to@[i]r*) ***)
   - Penggantian URL dengan cara :
     - *silent squid redirect to a common URL* (*redirect "new_url"*)
     - *visible client redirect to a common URL* (*redirect "302:new_url"*)

   diaktifkan oleh :
   - URL redirection
   - Kecocokan tujuan suatu grup
   - sebuah *fallback/default* untuk URL yang diblokir
   - sebuah *fallback/default* untuk pengguna yang diblokir/tidak diketahui

   dan secara opsional dengan :
   - penempatan *string runtime* **strftime** atau **printf**
5. Mendefinisikan access control lists (acl) berdasarkan kombinasi yang wajar dari definisi di atas dengan :
   - memberikan setiap kelompok pengguna :
     - daftar lulus dengan kombinasi yang wajar :
       - kelompok tujuan yang diterima *(good-dests ...)*
       - kelompok tujuan yang tidak dapat diterima *(...!bad-dests)*
       - memblok alamat URL yang menggunakan *IP-Address* (untuk membiasakan pengguna selalu menggunakan nama domain) *(!in-addr)*
       - wildcards/nothing (*any*|*all*|*none*)
     - opsional aturan penulisan ulang yang umum ditetapkan untuk sebuah grup pengguna

    - opsional pengganti *default* URL untuk URL tujuan yang diblokir bagi sebuah grup pengguna

  dan secara opsional:

- acl link ke batas waktu tertentu
    - positif (dalam jam kerja)
    - negatif (di luar waktu kerja)
- mendefinisikan *fallback/default ruleset*

6. dapat menghasilkan *log* yang selektif berdasarkan :
    - grup pengguna
    - URL tujuan sutu grup pengguna. Biasanya digunakan untuk mencatat akses ke daftar URL yang telah di-*blacklist*
    - penulisan ulang aturan yang ditetapkan untuk suatu grup pengguna
    - dan secara opsional anonim untuk melindungi privasi individu