

**APLIKASI PROXY UNTUK PEMBLOKIRAN IP,
DOMAIN DAN KONTEN**

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat

Untuk Mendapatkan Gelar Sarjana

Jurusan Teknik Informatika



Disusun Oleh:

Nama : Eko Laksono Prasetyo

No. Mahasiswa : 06 523 161

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA**

2011

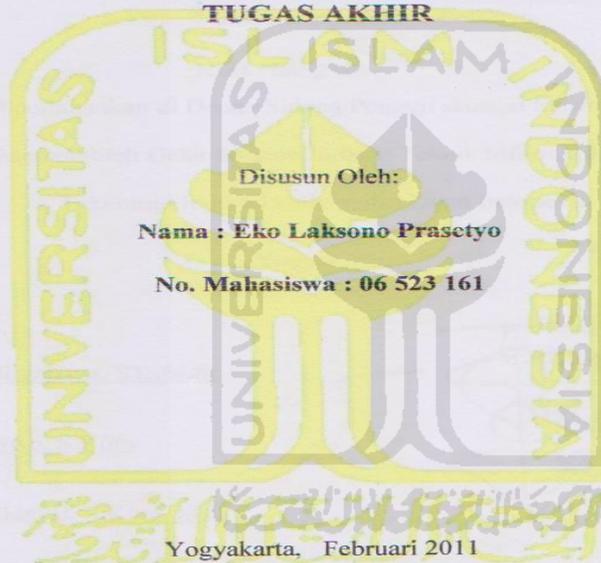
LEMBAR PENGESAHAN DOSEN PEMBIMBING

ii

LEMBAR PENGESAHAN DOSEN PEMBIMBING

APLIKASI PROXY UNTUK PEMBLOKIRAN IP,
DOMAIN DAN KONTEN

TUGAS AKHIR



Disusun Oleh:

Nama : Eko Laksono Prasetyo

No. Mahasiswa : 06 523 161

Yogyakarta, Februari 2011

Pembimbing

A handwritten signature in black ink, which appears to read 'Dirgahayu', is written over a faint circular stamp of the Yogyakarta State University.

Teduh Dirgahayu ST.,M.Sc

LEMBAR PENGESAHAN DOSEN PENGUJI

iii

LEMBAR PENGESAHAN DOSEN PENGUJI

TUGAS AKHIR

Oleh:

Nama : Eko Laksono Prasetyo

NIM : 06523161

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika Fakultas
Teknologi Industri Universitas Islam Indonesia
Yogyakarta,

Tim Penguji,

1. Teduh Dirgahayu, ST.,M.Sc
2. Ari Sujarwo, S.Kom
3. Syarif Hidayat, S.Kom.,M.IT

Tanda Tangan

Mengetahui,

Ketua Jurusan Teknik Informatika



Universitas Islam Indonesia

Yusuf Prayudi, S.Si., M.Kom

LEMBAR PERNYATAAN KEASLIAN HASIL

TUGAS AKHIR

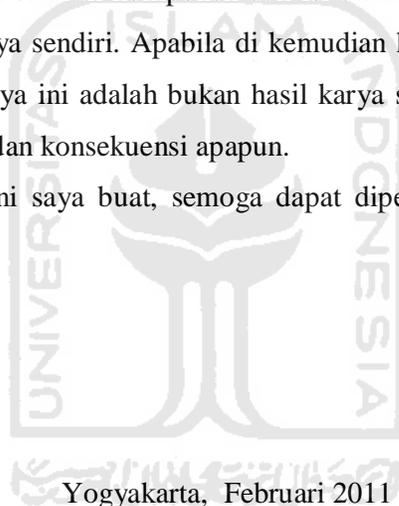
Saya yang bertanda tangan di bawah ini,

Nama: Eko Laksono Prasetyo

NIM: 06523161

Menyatakan bahwa seluruh komponen dan isi dalam Laporan Tugas Akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti bahwa ada beberapa bagian dari karya ini adalah bukan hasil karya saya sendiri, maka saya siap menanggung risiko dan konsekuensi apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.



Eko Laksono Prasetyo

HALAMAN PERSEMBAHAN

Kupersembahkan Karya Kecil ku Ini,

- ♥ Untuk Kedua orang tua ku tercinta atas segala doa, semangat serta Pengorbanannya...
- ♥ Untuk Adik-adikku tercinta Dyah dan Putri kalian adalah semangatku.
 - ♥ Untuk Novia kamu adalah inspirasiku.
 - ♥ Untuk semua orang yang membutuhkan.



MOTTO

- ☞ *"Allah tidak akan membebani seseorang kecuali sepadan dengan kemampuannya"* (Q.S Al Baqarah : 286)
- ☞ *"Sungguh, bersama kesukaran itu pasti ada kemudahan"* (Q.S Al Insyirah: 5)
- ☞ Anda tak pernah terlalu tua untuk belajar dan terlalu muda untuk tahu banyak (The Lion).
- ☞ Hambatan terbesar pada kebahagiaan adalah mengharapkan terlalu banyak kebahagiaan (Bernard De Fontenelle).
- ☞ Tujuan tidak tercapai bukan tragedy kehidupan, yang jadi tragedy adalah tidak mempunyai tujuan untuk dicapai (Benjamin Mays).
- ☞ Adalah mustahil melemparkan kotoran ke orang lain tanpa sedikitpun mengotori diri sendiri (Abigail Van Buren).
- ☞ Coba menyanyi seakan Anda tidak memerlukan uang, Coba mencintai seakan Anda tidak pernah akan disakiti, Coba menari seakan tak ada yang melihat. Jika Anda ingin sukses, semuanya harus berasal dari hati (Susana Clark).
- ☞ Orang-orang yang berhasil di dunia ini adalah orang-orang yang bangun dan mencari situasi yang mereka inginkan , dan jika tidak menemukannya, mereka menciptakannya. (George Bernard Shaw)
- ☞ "Tujuan ilmu pendidikan bukanlah ilmu pengetahuan, melainkan aksi nyata" (Herbert Spencer, Filusuf Inggris)

KATA PENGANTAR



Assalamu'alaikumWr.Wb.

Alhamdulillah, segala puji bagi Allah SWT atas segala rahmat, hidayah dan inayah-Nya sehingga penulisan laporan tugas akhir yang berjudul “Aplikasi Proxy Untuk Pemblokiran IP, Domain, dan Konten” dapat terselesaikan dengan baik.

Laporan tugas akhir ini disusun sebagai salah satu syarat guna memperoleh gelar Sarjana Teknik Informatika pada Universitas Islam Indonesia, serta sebagai sarana untuk mengaplikasikan ilmu dan teori yang telah diperoleh selama menjalani masa studi di jurusan Teknik Informatika Universitas Islam Indonesia.

Penyusunan laporan ini tidak lepas dari bimbingan, dukungan dan bantuan dari berbagai pihak. Dalam kesempatan ini, dengan penuh kerendahan hati, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT, Tuhan bagi seluruh alam yang melimpahkan rahmat dan karunianya sehingga penulis selalu diberi kesehatan dan kemudahan selama pembuatan tugas akhir ini.
2. Kedua orang tua yang selalu melimpahkan kasih sayang tulus, serta do'a yang tiada henti.
3. Bapak Prof. Dr Edy Suandi Hamid, M.Ec, selaku rektor Universitas Islam Indonesia dan seluruh jajaran Rektorat Universitas Islam Indonesia.
4. Bapak Gumbolo Hadi Susanto, Ir., M.Sc. selaku Dekan Fakultas Teknologi Industri, Universitas Islam Indonesia.
5. Bapak Yudi Prayudi , S.Si., M.Kom. selaku ketua Jurusan Teknik Informatika.

6. Bapak Teduh Dirgahayu, ST.,M.Sc selaku dosen pembimbing. Terima kasih atas segala bantuan, dukungan, semangat, dan pengetahuannya, serta kemudahan yang telah diberikan.
7. Staf Pengajaran dan Tata Usaha Fakultas Teknologi Industri, Universitas Islam Indonesia Yogyakarta, yang telah membantu dalam urusan administrasi di kampus.
8. Buat Novia yang selalu memberikan dukungan, semangat, keceriaan dan segala waktunya untuk membantu.
9. Buat adek-adek ku Dyah dan Putri yang selalu memberikan dukungan, semangat, keceriaan dan segala waktunya untuk membantu.
10. Sahabat yang sekaligus keluarga ku “D’Team-LO” (“maz Agus, Unix, Yaser, Pacul, Ardi, Putut, Happy, Rembo, Didit, Mamet, Rasha, Dodo. Maz Tyo“). yang selalu membawa keceriaan dan semangat selama ini.
11. Serta semua pihak yang telah turut membantu hingga selesainya penyusunan tugas akhir ini. Semoga Allah SWT membalas budi baik dan keikhlasannya, Amin.

Penulis menyadari sepenuhnya bahwa tugas akhir ini masih jauh dari kesempurnaan suatu tulisan ilmiah, oleh sebab itu dengan segala kerendahan hati penulis menerima kritik dan saran demi kesempurnaannya.

Wassalamu’alaikum Wr.Wb

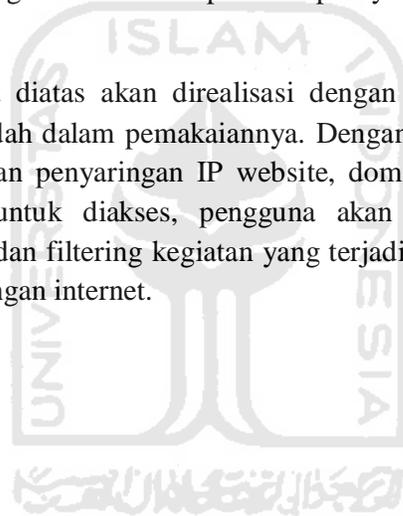
Yogyakarta, Februari 2011

Eko Laksono Prasetyo

SARI

Aplikasi proxy merupakan suatu aplikasi yang sangat penting dalam dunia internet. Aplikasi proxy ini merupakan pen jembatan aplikasi klien dengan internet. Proses pengkaitan ke dua jenis jaringan yang berbeda ini dilakukan secara sederhana melalui sebuah komputer atau alat yang menjalankan software proxy. Jadi pada komputer yang berfungsi sebagai perantara ini, selalu akan mempunyai dua interface (antar muka), biasanya satu berupa modem untuk menyambung ke jaringan Internet, dan sebuah Ethernet card untuk menyambung ke jaringan lokal yang sifatnya private. Penggunaan aplikasi proxy ini masih dirasa cukup sulit bagi sebagian pengguna internet dikarenakan pengaturannya yang masih rumit. Dengan adanya kendala ini, dibuat suatu penyelesaian masalah yaitu dengan membangun sebuah aplikasi proxy yang mudah dalam penggunaannya..

Aplikasi tersebut diatas akan direalisasi dengan cara membuat sebuah aplikasi proxy yang mudah dalam pemakaiannya. Dengan adanya aplikasi proxy ini yang dapat melakukan penyaringan IP website, domain konten-konten, dan port yang diijinkan untuk diakses, pengguna akan dapat dengan mudah melakukan pengawasan dan filtering kegiatan yang terjadi dalam sebuah jaringan lokal yang terhubung dengan internet.



TAKARIR

<i>Browser</i>	Perangkat lunak yang digunakan untuk menampilkan halaman web .
<i>Capture</i>	Menangkap .
<i>connection-oriented</i>	Bentuk hubungan antar unit dalam jaringan yang komunikasinya dilakukan secara bertahap.
<i>Domain</i>	Nama alamat situs web.
<i>Display</i>	Tampilan/ layar.
<i>Ethernet card</i>	Kartu jaringan.
<i>Hardware</i>	Perangkat keras / luar.
<i>Ip address</i>	Alamat IP .
<i>Layer</i>	Lapisan.
<i>Microsoft windows</i>	Salah satu sistem operasi .
<i>Mikroprosesor</i>	Mesin kecil sebagai pemroses dan pengendali.
<i>Receiver</i>	Penerima.
<i>router</i>	Perangkat yang digunakan untuk menghubungkan antar jaringan komputer.
<i>Software</i>	Perangkat lunak, sistem.
<i>Switch</i>	Alat penghubung beberapa LAN.
<i>Storage</i>	Penyimpanan.
<i>Sender</i>	Pengirim.
<i>Server</i>	Perangkat komputer yang bertugas sebagai menangani layanan
<i>Tool</i>	Alat, perangkat
<i>Unix</i>	Nama sebuah sistem operasi.

Website

Kumpulan data yang berisi informasi, data, gambar, dan suara .



DAFTAR ISI

APLIKASI PROXY UNTUK PEMBLOKIRAN IP, DOMAIN DAN KONTEN ..i	i
LEMBAR PENGESAHAN DOSEN PEMBIMBING	ii
LEMBAR PENGESAHAN DOSEN PENGUJI.....	iii
LEMBAR PERNYATAAN KEASLIAN HASIL.....	iii
HALAMAN PERSEMBAHAN.....	v
MOTTO.....	vi
KATA PENGANTAR.....	vii
SARI.....	ix
TAKARIR.....	x
DAFTAR ISI.....	xii
DAFTAR GAMBAR.....	xv
BAB 1 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

1.6.1	Metode Pengumpulan Data	4
1.6.2	Perancangan Sistem	4
1.7	Sistematika Penulisan.....	5
BAB 2	LANDASAN TEORI.....	7
2.1	Jaringan Komputer.....	7
2.2	Protokol.....	9
2.3	Model Referensi Jaringan.....	10
2.4	IP Address	13
2.4.1	Kelas-kelas Alamat IP.....	15
2.5	Port.....	18
2.6	Proxy	19
BAB 3	PERANCANGAN APLIKASI.....	21
3.1	Gambaran Aplikasi	21
3.2	Analisis Kebutuhan.....	23
3.2.1	Perangkat Keras	23
3.2.2	Perangkat Lunak	23
3.3	Perancangan Sistem	24
3.3.1	Use Case Diagram.....	24
3.3.2	Activity Diagram.....	26
3.4	Perancangan Antarmuka	28
BAB 4	HASIL DAN PEMBAHASAN	31

4.1 Implementasi	31
4.1.1 Batasan Implementasi	31
4.1.2 Hasil	31
4.1.2.1 Aplikasi Proxy	32
4.1.2.2 Analisis Aplikasi	49
BAB 5 KESIMPULAN DAN SARAN	53
5.1 Kesimpulan.....	53
5.2 Saran.....	53
DAFTAR PUSTAKA.....	54



DAFTAR GAMBAR

Gambar 2.1 Model referensi TCP/IP	11
Gambar 2.2 Format IP Adress	15
Gambar 2.3 Network ID dan Host ID pada kelas alamat IP	16
Gambar 2.4 Server proxy	21
Gambar 3.1 Cara Kerja Server Proxy	21
Gambar 3.2 <i>Use Case Diagram</i> Aplikasi Prox	25
Gambar 3.3 <i>Activity Diagram</i> Aplikasi Proxy	26
Gambar 3.4 Perancangan Antarmuka Halaman Blokir IP	28
Gambar 3.5 Perancangan Antarmuka Halaman Blokir Domain	29
Gambar 3.6 Perancangan Antarmuka Halaman Blokir Konten	30
Gambar 3.7 Perancangan Antarmuka Halaman <i>Log</i>	30
Gambar 4.1 Halaman Awal Aplikasi Proxy.....	32
Gambar 4.2 Halaman Aplikasi Saat Dijalankan.....	33
Gambar 4.3 Halaman Blokir IP.....	34
Gambar 4.4 Hasil Masukan Blokir IP.....	35
Gambar 4.5 Hasil Hapus Blokir IP	36
Gambar 4.6 Tampilan Halaman Blokir Domain	39

Gambar 4.7 Hasil Masukkan Blokir Domain.....	40
Gambar 4.8 Hasil Hapus Blokir Domain.....	41
Gambar4.9 Halaman Blokir Konten.....	43
Gambar 4.10 Hasil Masukkan Blokir Konten.....	44
Gambar 4.11 Hasil Hapus Blokir Konten.....	45
Gambar 4.12 Halaman Log.....	48
Gambar 4.13 Tampilan Peringatan Pada Browser Klien.....	49
Gambar 4.14 Peringatan Input Blokir IP.....	50
Gambar 4.15 Peringatan Hapus Blokir IP.....	50
Gambar 4.16 Peringatan Blokir Domain.....	51
Gambar4.17 Peringatan Hapus Blokir Domain.....	51
Gambar 4.18 Peringatan Input Blokir Konten.....	52
Gambar 4.19 Peringatan Hapus Blokir Konten.....	52

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Internet merupakan salah satu jendela dunia yang dapat menghubungkan antara pengguna satu dengan yang lainnya. Berbagai macam kegunaan internet, antara lain sebagai media informasi pembelajaran, bisnis, media pendidikan, dan masih banyak lagi kegunaannya. Selain menyediakan banyak informasi yang bermanfaat, internet juga mengandung konten yang berbahaya salah satunya pornografi. Tentunya kondisi ini perlu diwaspadai. Untuk menghindari pengaksesan konten-konten yang berbahaya dalam hal ini konten pornografi maka perlu dilakukan pemblokiran.

Port pada komputer bisa diibaratkan sebagai pintu atau lubang masuk dan keluarnya service atau layanan jalur transfer data dari komputer satu ke komputer lain. Pada sistem komputer terdapat dua jenis port yaitu port fisik dan port logika. Port fisik adalah soket atau slot yang ada pada komputer sebagai penghubung peralatan input-output komputer, misalnya mouse, keyboard, dan printer. Port logika (non fisik) adalah port yang di gunakan oleh perangkat lunak sebagai jalur untuk melakukan koneksi dengan komputer lain termasuk untuk koneksi internet. Port logika ini bersifat logika tidak nyata seperti port fisik akan tetapi port logika ini dapat dipantau dengan menggunakan aplikasi pemantauan port.

Port berperan dalam pertukaran data-data yang berbeda layanan antara dua komputer atau lebih agar tidak tertukar atau tumpang tindih. Dengan adanya port maka data HTTP tidak akan tertukar dengan data FTP atau pun tertukar dengan data SMTP. Setiap port memiliki nomor port masing-masing, diklasifikasikan dengan jenis protokol transport apa yang digunakan, ke dalam port TCP dan port UDP. Dengan port maka penerimaan paket data oleh suatu alamat IP tidak akan tertukar karena akan secara otomatis masuk sesuai port layanan yang diakses pengguna internet.

Dari latar belakang diatas maka penulis bermaksud merancang sebuah aplikasi proxy yang dirancang dan dibuat untuk melakukan pemantauan aktivitas pengaksesan suatu alamat IP, selain itu aplikasi ini juga dapat digunakan untuk pemblokiran berdasarkan alamat IP, pemblokiran berdasarkan domain dan pemblokiran berdasarkan konten. Dan dalam aplikasi ini juga terdapat log yang berfungsi untuk memantau kegiatan pengaksesan. Sehingga penggunaan aplikasi ini dapat membantu mengurangi adanya penyalahgunaan penggunaan internet yang seharusnya digunakan untuk media informasi, hiburan, bisnis dan pendidikan.

1.2 Rumusan Masalah

Bagaimana merancang dan membangun sebuah aplikasi proxy untuk pemblokiran alamat IP, domain dan konten.

1.3 Batasan Masalah

Batasan masalah yang ditentukan :

1. Sistem ini tidak memiliki form login.
2. Sistem ini hanya mampu berjalan di jaringan lokal (satu network).
3. Sistem ini tidak memiliki *cache* untuk penyimpanan data pengaksesan.
4. Sistem ini tidak memiliki file penyimpanan untuk pengaturan.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah membuat aplikasi proxy menggunakan Visual Basic untuk pemantauan pengaksesan internet yang kemudian dapat dilakukan pemblokiran berdasarkan alamat IP, domain, dan konten.

1.5 Manfaat Penelitian

Beberapa manfaat dari tugas akhir ini yaitu:

1. Dengan aplikasi proxy ini admin jaringan dapat melakukan pemantauan aktifitas pengaksesan data klien yang mengakses internet.
2. Dengan aplikasi proxy ini admin jaringan dapat menentukan alamat IP, domain, dan konten yang dapat diakses oleh pengguna internat dalam jaringan.

1.6 Metodologi Penelitian

Beberapa metode yang digunakan dalam penelitian ini adalah sebagai berikut :

1.6.1 Metode Pengumpulan Data

Metode pengumpulan data yang dipakai adalah dengan mempelajari teori-teori yang berhubungan dengan sistem manajemen jaringan dan literatur-literatur lain yang dapat membantu dalam menyelesaikan permasalahan.

1.6.2 Perancangan Sistem

Dalam metode ini meliputi:

1. Analisa dan rekayasa sistem

Pada tahap ini dilakukan analisa kebutuhan sistem, perancangan input, proses dan output serta mengumpulkan data sesuai dengan sumber yang ada kaitannya dengan data-data yang diperlukan dalam membangun aplikasi proxy.

2. Perancangan sistem

Pada tahapan perancangan ini mendefinisikan bagaimana sistem dibentuk untuk membangun Aplikasi Proxy, yang meliputi perancangan desain kinerja sistem, perancangan atarmuka, dan perancangan output.

3. Implementasi sistem

Pada tahap dilakukan implementasi perancangan yang telah dibuat kedalam bahasa komputer menggunakan bahasa pemrograman Visual Basic 6.0

4. Pengujian

Pada tahapan ini perangkat lunak yang dibangun berdasarkan tahapan implementasi sistem, dilakukan pengujian untuk melihat sejauh mana aplikasi yang telah dibangun dapat berjalan sesuai dengan yang dikehendaki.

1.7 Sistematika Penulisan

Sistematika penulisan bertujuan untuk menggambarkan secara singkat isi laporan pada tiap-tiap bagian sehingga laporan menjadi utuh dan jelas.

BAB I PENDAHULUAN.

Bab ini memuat latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat penelitian, metodologi yang digunakan dalam penelitian, serta sistematika penulisan laporan tugas akhir.

BAB II LANDASAN TEORI.

Bab ini membahas tentang landasan teori yang berhubungan dengan penelitian ini, yaitu menjelaskan tentang jaringan komputer, internet, protokol, model referensi jaringan, TCP/IP, alamat IP, dan port.

BAB III PERANCANGAN APLIKASI.

Bab ini membahas tentang analisis kebutuhan perangkat lunak, perancangan perangkat lunak. Bab ini meliputi metode analisis, hasil analisis, masukan sistem, keluaran sistem, proses sistem, dan antarmuka yang diinginkan dalam pembuatan sistem.

BAB IV HASIL DAN PEMBAHASAN.

Bab ini berisi penguraian dari hasil implementasi yang dibuat, diantaranya proses kerja sistem dan pengujian sistem serta analisis kesalahan.

BAB V KESIMPULAN DAN SARAN.

Bab ini merupakan bab terakhir yang menguraikan kesimpulan dari tugas akhir serta dikemukakan beberapa saran untuk dilaksanakan lebih lanjut guna pengembangan penelitian tugas akhir ini



BAB 2

LANDASAN TEORI

2.1 Jaringan Komputer

Perkembangan dunia komputer sekarang ini sangatlah pesat. Komputer masuk dalam semua aspek kehidupan manusia, baik dalam dalam ekonomi, pendidikan maupun sosial. Perkempangan komputer ini meliputi perkembangan perangkat lunak dan perangkat keras. Perkembangan dunia komputer yang semakin cepat ini mengakibatkan pengguna kompuer semakin banyak. Hal ini memunculkan keinginan antar pengguna komputer untuk dapat saling terhubung dengan pengguna komputer lain.

Jaringan komputer adalah suatu sistem yang terdiri dari kumpulan komputer yang saling berhubungan menggunakan perangkat lunak dan perangkat jaringan dengan menggunakan media komunikasi tertentu misalnya kawat tembaga, serat optik, gelombang mikro, dan satelit komunikasi. Informasi yang melintas sepanjang media komunikasi memungkinkan pengguna jaringan untuk saling bertukar data, berbagi media penyimpanan serta menggunakan perangkat lunak dan perangkat keras secara berbagi. Dalam perangkat keras pengenalan jaringan komputer meliputi jenis transmisi, dan bentuk-bentuk jaringan komputer atau topologi. Sedangkan dalam pembahasan perangkat lunaknya akan meliputi susunan protokol dan perjalanan data dari satu komputer ke komputer lain dalam suatu jaringan.

Tujuan utama dari sebuah jaringan komputer adalah sharing resource dimana sebuah komputer dapat memanfaatkan sumber daya yang dimiliki komputer lain yang berada dalam jaringan yang sama. Perkembangan teknologi komunikasi data dan jaringan komputer dewasa ini sudah tidak terbatas hanya pada komputer. Berbagai perangkat komunikasi yang hadir saat ini berkembang mengikuti perkembangan teknologi jaringan komputer, banyak diantaranya mengintegrasikan perangkat komputer seperti *mikroprosesor*, memori, *display*, *storage*, dan teknologi komunikasi ke dalamnya, padahal dulunya teknologi ini dikembangkan untuk komputer yang dapat kita temui saat ini, dan sekarang sudah ikut digunakan pada teknologi jaringan komputer.

Jumlah pengguna Internet yang besar dan semakin berkembang, telah mewujudkan budaya Internet. Internet juga mempunyai pengaruh yang besar atas ilmu, dan pandangan dunia. Internet tidak hanya berpengaruh positif tetapi juga banyak pengaruh negatif yang ditimbulkan dari internet. Untuk mengurangi pengaruh negatif maka perlu dilakukan pembatasan hak akses. Aplikasi proxy adalah aplikasi yang mempunyai kemampuan untuk melakukan penyaringan terhadap situs yang dikunjungi maupun penyaringan terhadap pengunjung, dan dapat dilakukan pembatasan hak akses.

Dalam mengatur integrasi dan komunikasi jaringan komputer ini digunakan protokol yaitu TCP/IP. TCP (*Transmission Control Protocol*) bertugas memastikan bahwa semua hubungan bekerja dengan benar, sedangkan IP (*Internet Protocol*) yang mentransmisikan data dari berbagai perangkat jaringan,

bisa dikatakan bahwa IP ini merupakan alamat dari perangkat jaringan komputer, karena peralatan jaringan seperti komputer, router, server dan berbagai macam peralatan jaringan lainnya dikenali dengan alamat IP

2.2 Protokol

Agar jaringan berjalan dengan semestinya selain perangkat keras harus ada aturan standar yang mengaturnya karena itu diperlukan suatu protokol. Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras.

Penggunaan protokol berfungsi agar komunikasi antar perangkat yang saling terhubung menggunakan bahasa yang sama. Bagi komputer pengirim (*sender*) maupun penerima (*receiver*) yang terlibat dalam sebuah proses pengiriman data, mereka harus menggunakan protokol yang sama. Jadi setiap perangkat yang saling terhubung dan saling bertukar data dalam komunikasi, pertukaran datanya dapat berlangsung dengan baik, sehingga data yang dikirim oleh komputer pengirim sesuai dengan data yang diterima komputer tujuan.

Protokol dalam jaringan tersusun dalam bentuk lapisan-lapisan (*Layer*). Hal ini bertujuan agar dalam tiap lapisan protokol mudah dipahami. Dalam susunan layer ini menunjukkan tahapan-tahapan dalam komunikasi data antar

komputer. Dalam setiap lapisan protokol ini mempunyai fungsi masing-masing dalam komunikasi antar komputer.

2.3 Model Referensi Jaringan

Model referensi jaringan bertujuan agar berbagai perangkat keras dan perangkat lunak dari berbagai macam vendor dapat saling beroperasi dengan baik. Dalam jaringan komputer terdapat istilah model referensi jaringan ada dua macam model referensi jaringan OSI (*Open System Interconnect*) dan TCP/IP (*Transmission Control Protocol/Internet Protocol*). Tujuan dari model ini untuk memberikan gambaran yang jelas mengenai fungsi dan kerangka kerja komunikasi jaringan secara terstruktur dan logis.

Pada awalnya model TCP/IP hanya dipergunakan pada sistem berbasis UNIX. Model yang sederhana dan implementasi yang cukup mudah menjadikan model referensi ini sering dipakai.

TCP/IP (*Transmission Control Protokol/Internet Protokol*) adalah standar komunikasi data yang digunakan dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protokol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Protokol TCP/IP diimplementasikan dalam bentuk perangkat lunak di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP stack.



Gambar 2.1 Model referensi TCP/IP

Berikut penjelasan lapisan layanan pada TCP/IP:

1. Lapisan Application: menyediakan komunikasi antar proses atau aplikasi pada komputer yang berjauhan namun terhubung pada jaringan.
2. Lapisan Transport: menyediakan layanan transfer. Lapisan ini juga termasuk mekanisme untuk menjamin kehandalan transmisi datanya. Layanan ini tentu saja akan menyembunyikan segala hal yang terlalu detail untuk lapisan di atasnya.
3. Lapisan Internetwork: menyediakan layanan pemilihan jalur (*routing*) data dari komputer sumber ke komputer tujuan yang melewati satu atau lebih jaringan yang berbeda dengan menggunakan *router*. Layer ini berisi protokol yang bertanggung jawab dalam pengalamatan dan routing paket.
4. Lapisan Network Access: mendefinisikan antarmuka logika antara sistem dan jaringan.

Beberapa alasan mengapa protokol TCP/IP banyak digunakan adalah protokol ini memiliki banyak keunggulan. Diantaranya adalah:

1. TCP/IP menggunakan standar protokol terbuka sehingga tersedia secara luas dan semua pengembang dapat menggunakannya dengan bebas tanpa terikat oleh plat-form. Semua pengembang bisa mengembangkan perangkat lunak untuk dapat berkomunikasi menggunakan protokol ini.
2. TCP/IP tidak tergantung pada perangkat keras atau sistem operasi jaringan tertentu. TCP/IP tidak terikat dengan perangkat keras maupun perangkat lunak tertentu dan mampu berjalan dalam model jaringan apapun. TCP/IP juga dapat digunakan dalam berbagai media transmisi apapun.
3. TCP/IP mempunyai cara pengalamatan yang bersifat unik, jadi memungkinkan komputer dapat mengidentifikasi secara unik komputer yang lain dalam seluruh jaringan, artinya setiap komputer dan perangkat jaringan yang tersambung dengan jaringan TCP/IP dalam hal ini internet akan memiliki alamat yang berbeda.
4. TCP/IP mempunyai kehandalan dalam menghubungkan antar jaringan komputer yaitu dengan fasilitas routing.

Protokol TCP/IP memiliki kehandalan dalam proses pengiriman data. TCP merupakan protokol *connection-oriented* karena mekanisme dalam proses pengiriman data protokol TCP selalu meminta konfirmasi apakah data yang dikirim sudah sampai kekomputer tujuan atau terjadi kegagalan dalam pengiriman. Jika konfirmasi data telah terkirim maka TCP akan mengirimkan

data berikutnya sesuai urutan data. Sedangkan jika terjadi kegagalan dalam proses pengiriman data maka protokol ini akan mengirim ulang data tersebut.

Agar komputer bisa berkomunikasi dengan komputer lainnya, maka menurut aturan TCP/IP, komputer tersebut harus memiliki suatu *address* yang unik. Alamat tersebut dinamakan alamat IP. alamat IP memiliki format sbb: *aaa.bbb.ccc.ddd*.

Suatu jaringan internal bisa saja menggunakan alamat IP sembarang. Namun untuk tersambung ke Internet, jaringan itu tetap harus menggunakan alamat IP legal. Jika tidak menggunakan alamat IP yang maka saat kita mengirim paket data ke sistem lain, sistem tujuan itu tidak akan bisa mengembalikan paket data tersebut, sehingga komunikasi tidak akan terjadi.

Dalam berkomunikasi di Internet antar jaringan komputer dibutuhkan *gateway/router* sebagai jembatan yang menghubungkan simpul-simpul antar jaringan sehingga paket data bisa diantar sampai ke tujuan.

2.4 IP Address

Seperti halnya pada pengiriman surat secara konvensional untuk dapat sampai kepada orang yang tepat diperlukan sebuah alamat dalam pengiriman surat. Begitu juga dalam pengiriman paket data antar komputer dalam jaringan komputer, agar data yang dikirim sampai pada komputer tujuan yang tepat maka diperlukan mekanisme pengalamatan yang dapat menjamin pengiriman paket data sampai ke komputer yang tepat.

Peralatan-peralatan yang ada dalam sistem jaringan berbasis TCP/IP dikenali dengan alamat IP yaitu pengalamatan dengan menggunakan nilai biner 32bit atau 128 bit. IP versi empat atau disebut IPv4 menggunakan 32 bit, yang terbagi dalam empat kelompok bagian, sehingga masing-masing kelompok terdiri dari bilangan biner 8 bit. Dan tiap alamat dibedakan dalam kelas-kelasnya sendiri. Sedangkan 128bit digunakan pada IP versi 6 atau disebut IPv6.

Alamat IP terdiri atas 8 byte data yang mempunyai nilai dari 0-255 yang sering ditulis dalam bentuk [xx.xx.xx.xx] (xx mempunyai nilai dari 0-255). Masing-masing kelompok bit biner terdiri dari 8 bit, sehingga jika diubah menjadi bilangan desimal, maka bilangan yang mungkin adalah dari 0 (biner = 00000000) sampai 255 (biner = 11111111) yaitu ada 256 bilangan desimal. Alamat IP merupakan bilangan biner 32 bit yang terbagi menjadi empat kelompok, sehingga masing-masing kelompok terdiri dari bilangan biner 8 bit. Ini merupakan implementasi alamat IP yang disebut IPv4 . (Wagito, 2007).

Dalam format penulisan alamat IP tiap kelompok dipisahkan oleh tanda titik (.), dan tiap 8 bit kelompok disebut *oktet*. Untuk memudahkan pembacaan IP yang menggunakan bilangan biner maka bilangan biner dikonversi ke bilangan decimal, ditulis dalam 4 bilangan desimal yang lebih dikenal dengan “notasi desimal bertitik”. Setiap bilangan desimal merupakan nilai dari satu oktet IP address. Sebagai contoh :

Desimal	167	205	206	100
Biner	10100111	11001101	11001110	01100100

Gambar 2.2 Format IP Adress

Nilai terbesar dari 8 bit bilangan biner adalah 255 dengan perhitungan tiap kelompok $(2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2 + 1) = (128 + 64 + 32 + 16 + 8 + 4 + 2 + 1)$, jadi jumlah IP yang tersedia adalah $255 \times 255 \times 255 \times 255$ yaitu sebanyak 4.228.250.625 . Artinya terdapat IP address sekitar 4 milyar lebih yang harus dibagikan ke seluruh pengguna jaringan internet di seluruh dunia. Untuk memudahkan pembagian alamat IP maka alamat IP dikelompokkan berdasarkan kelas-kelas, yaitu kelas A, kelas B, kelas C, kelas D, dan kelas E. Perbedaan antar kelas alamat IP ini terletak pada ukuran dan jumlahnya.

2.4.1 Kelas-kelas Alamat IP

Alamat IP dapat dipisahkan menjadi dua bagian, yakni bagian network (net ID) dan bagian host (host ID). Network ID menunjukkan ID alamat jaringan tempat host-host berada, sedangkan host ID adalah bagian yang menunjukkan host itu berada. Sederhananya, network ID seperti nama jalan sedangkan host ID adalah nomor rumah di jalan tersebut. [ABI09]

Jadi seluruh *host* yang tersambung dalam suatu alamat jaringan memiliki *network ID* yang sama. Berikut pemisahan *network ID* dan *host ID* berdasarkan kelas alamat IP :

Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host
Class D	Multicast			
Class E	Research			

Gambar 2.3 Network ID dan Host ID pada kelas alamat IP

1. Alamat IP kelas A

Alamat IP kelas A ini memiliki *network ID* yang relatif kecil dibandingkan kelas yang lain tetapi memiliki *host ID* yang sangat besar. IP kelas A mempunyai panjang *network ID* 8 bit dan panjang *Host ID* 24 bit. IP kelas A memiliki rentang *Network ID* antara 0-127, jadi pada IP kelas A terdapat 127 *network* dengan jumlah IP yang tersedia $255 \times 255 \times 255$ yaitu sebanyak 16.777.214. Jadi tiap *network* dapat menampung sekitar 16 juta host, alamat IP kelas ini diberikan kepada suatu jaringan yang berukuran sangat besar.

2. Alamat IP kelas B

Alamat IP kelas B mempunyai rentang IP 128.0.xxx.xxx - 191.155.xxx.xxx. IP kelas B ini memiliki sekitar 65.255 *network* dengan jumlah *host* tiap *network* sekitar 65 ribu *host*. IP kelas B ini memiliki panjang *network ID* 16 bit dan *host ID* 16 bit. Sebagai contoh alamat IP 168.100.25.25, maka *network ID*-nya adalah 168.100 dan *host ID*-nya adalah 25.25.

3. Alamat IP kelas C

Alamat IP kelas C ini memiliki jaringan yang sangat banyak sekali dengan *host* yang kecil. *Network ID* kelas C ini terdiri dari 24 bit dan *host ID* 8 bit sehingga IP kelas C ini dapat terbentuk sekitar 2 juta *network* dengan tiap-tiap *network* memiliki 256 *host*.

4. Alamat IP kelas D

Alamat IP kelas D di antara rentang 224-247, IP kelas D ini digunakan untuk keperluan *multicasting*. Dalam *multicast* tidak dikenal istilah *network ID* dan *host ID*. Alamat IP kelas D ini digunakan sebagai alamat *multicast* yaitu sejumlah komputer memakai bersama suatu aplikasi.

5. Alamat IP kelas E

Alamat IP kelas E berada pada 248-255, alamat IP kelas ini tidak diperuntukkan untuk keperluan umum dan hanya digunakan untuk penelitian.

Penggunaan alamat IP dalam membangun sebuah jaringan komputer harus secara benar maksudnya adalah menggunakan *network ID* dan *host ID* dengan tepat. Beberapa aturan untuk menentukan *network ID* dan *host ID* yaitu :

1. *Network ID* tidak boleh sama dengan 127 karena *network* ini secara *default* digunakan sebagai alamat lokal komputer.
2. *Network ID* dan *Host ID* tidak boleh sama dengan nol atau 255 karena jika 0 maka akan diartikan sebagai alamat *network* dan jika 255 maka akan diartikan sebagai alamat *broadcast*.

3. *Host ID* dalam satu jaringan harus unik artinya dalam satu jaringan tidak boleh ada *host ID* yang sama.

2.5 Port

Port berperan dalam pertukaran data-data dalam suatu alamat IP yang berbeda layanan, jadi pertukaran data antara dua komputer atau lebih yang menggunakan layanan yang berbeda dalam pertukaran, datanya tidak tertukar atau terjadi penumpukan data. Dengan adanya port maka data HTTP tidak akan tertukar dengan data FTP atau pun tertukar dengan data SMTP. Setiap port memiliki nomor port masing-masing, Dengan port maka penerimaan paket data oleh suatu alamat IP tidak akan tertukar karena akan secara otomatis masuk sesuai port yang tertera di akhir alamat IP.

Dalam protokol jaringan TCP/IP, port mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. Port dapat mengidentifikasi aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, port juga mengidentifikasi sebuah proses tertentu di mana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam *server*.

Port dibedakan menjadi tiga, yaitu:

1. *Well known*

Well known Port ditetapkan oleh IANA (*Internet Assigned Number Authority*). Port ini merupakan inti dari layanan yang secara default ada di internet. Port ini pada awalnya memiliki nomor 0 sampai 255 kemudian diperlebar hingga 0 sampai 1023.

2. *Registered Port*

Registered Port berkisar antara 1024 sampai 49151 yang beberapa port diantaranya merupakan *Dynamically Assigned Port*. *Registered port* ada dalam daftar IANA. Pada *Registered Port* memiliki hak istimewa, yaitu port yang sama dapat digunakan oleh beberapa vendor komputer dan jaringan.

3. *Dynamically Assigned Port*

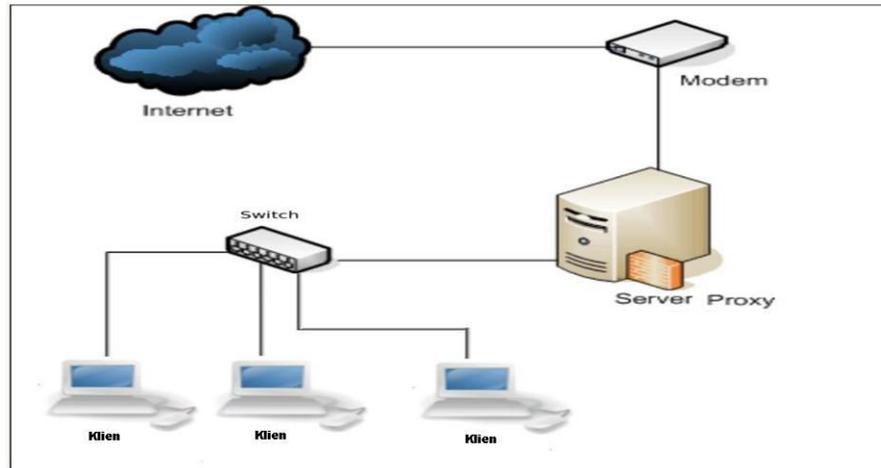
Dynamically Assigned Port merupakan port-port yang ditetapkan oleh sistem operasi atau aplikasi yang digunakan untuk melayani *request* dari pengguna sesuai dengan kebutuhan. *Dynamically Assigned Port* berkisar dari 1024 hingga 65536. port ini biasanya dipakai oleh program komersial seperti anti virus.

2.6 Proxy

Dalam jaringan komputer, server proxy adalah server (sistem komputer atau program aplikasi) yang bertindak sebagai perantara permintaan dari klien mencari sumber daya dari server lain. Klien A terhubung ke server proxy, meminta

beberapa layanan, seperti file, koneksi, halaman web, atau sumber daya lainnya, yang tersedia dari server yang berbeda. Server proxy mengevaluasi permintaan menurut aturan penyaringan. Sebagai contoh, menyaring lalu lintas dengan alamat IP atau protokol. Jika permintaan divalidasi oleh penyaringan, server proxy menyediakan sumber daya dengan menghubungkan ke server yang relevan dan meminta layanan atas nama klien.

Server proxy diletakkan antara aplikasi klien dan aplikasi server yang dihubungi. Aplikasi klien dapat berupa *browser*, sedangkan aplikasi server berupa situs web. Server proxy berperan menjembatani interaksi klien server, server proxy juga mempunyai kemampuan untuk melakukan penyaringan terhadap suatu situs web yang diakses oleh klien. Hal ini bertujuan untuk menghindari penyalahgunaan hak akses oleh klien dalam hal ini konten yang dilarang untuk diakses. . Berikut merupakan gambaran umum dari server proxy. Dapat dilihat pada gambar 2.4:



Gambar 2.4 Server proxy

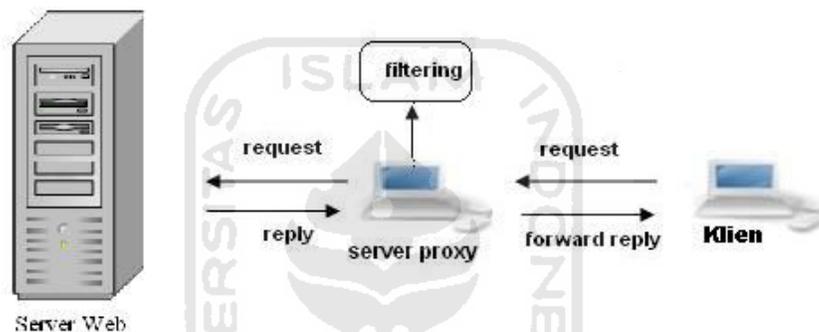
Dikarenakan manfaat penggunaan server proxy pada jaringan komputer sangatlah besar sebagian besar jaringan komputer menerapkan server proxy pada jaringan mereka. Hal ini bertujuan untuk memonitor jaringan, melakukan pembatasan-pembatasan akses dan mengurangi penyalahgunaan oleh klien dalam melakukan akses data baik dari internet maupun lokal.

BAB 3

PERANCANGAN APLIKASI

3.1 Gambaran Aplikasi

Berikut merupakan gambaran cara kerja aplikasi proxy:



Gambar 3.1 Cara Kerja Server Proxy

Semua permintaan klien yang menggunakan *browser* diarahkan ke aplikasi proxy. Kemudian permintaan tersebut diteruskan oleh aplikasi proxy ke alamat situs web tujuan. Selanjutnya balasan dari permintan situs web tujuan akan diterima kembali oleh aplikasi proxy. Apabila balasan dari situs web tujuan termasuk dalam aturan penyaringan IP, domain atau konten pada aplikasi proxy, maka balasan tidak akan diteruskan ke klien. Sebagai gantinya, klien akan menerima peringatan yang ditampilkan lewat *browser* yang menginformasikan bahwa akses ditolak. Apabila balasan dari situs web tujuan tidak termasuk dalam

aturan penyaringan IP, domain atau konten, maka balasan dari *website* tujuan akan diteruskan kepada klien.

Dari pengaturan yang sudah dilakukan diatas kemudian dapat dilakukan penyaringan pada pengaksesan yang dilakukan oleh klien yaitu dengan mengisikan mengatur pada fitur penyaringan pada aplikasi proxy meliputi blokir alamat IP, blokir *domain*, dan blokir konten. Selain itu pengguna juga dapat mengganti port *default* proxy yang menggunakan port 88 dengan yang dikehendaki dan melihat *log* data pengaksesan oleh klien melalui fitur *log* pada aplikasi proxy. Berikut merupakan penjelasan dari fitur penyaringan pada aplikasi proxy :

1. Blokir IP

Blokir IP merupakan fitur penyaringan untuk melakukan pemblokiran alamat IP situs web tujuan. Pengguna dapat memasukkan dan mengeluarkan alamat IP *website* ke dalam dan dari daftar blokir IP.

2. Blokir Domain

Blokir *domain* merupakan fitur penyaringan untuk melakukan pemblokiran nama *domain* situs web tujuan. Pengguna dapat memasukkan dan mengeluarkan nama *domain* ke dalam dan dari daftar blokir *domain*.

3. Blokir Konten

Blokir konten merupakan fitur penyaringan untuk melakukan pemblokiran terhadap konten situs web. Pengguna dapat memasukkan dan menghapus daftar

kata yang akan digunakan dalam pemblokiran konten. Situs web dengan konten yang mengandung kata pada daftar kata tersebut akan terblokir.

3.2 Analisis Kebutuhan

Dalam pengembangan aplikasi proxy ini dibutuhkan beberapa perangkat keras dan perangkat lunak.

3.2.1 Perangkat Keras

Perangkat keras yang dibutuhkan untuk implementasi aplikasi proxy ini adalah sebuah komputer dengan spesifikasi sebagai berikut:

1. Perangkat komputer
 - a. Minimal Pentium IV 2.1 MHz
 - b. Harddisk dengan kapasitas 80 GB
 - c. Mouse
 - d. Keyboard
 - e. Network interface card
2. Perangkat tambahan
 - a. Kabel UTP sebagai media penghubung komputer dalam jaringan lokal
 - b. *Switch*
 - c. Modem

3.2.2 Perangkat Lunak

Perangkat lunak yang dibutuhkan untuk implementasi aplikasi proxy ini adalah sebuah komputer dengan spesifikasi sebagai berikut:

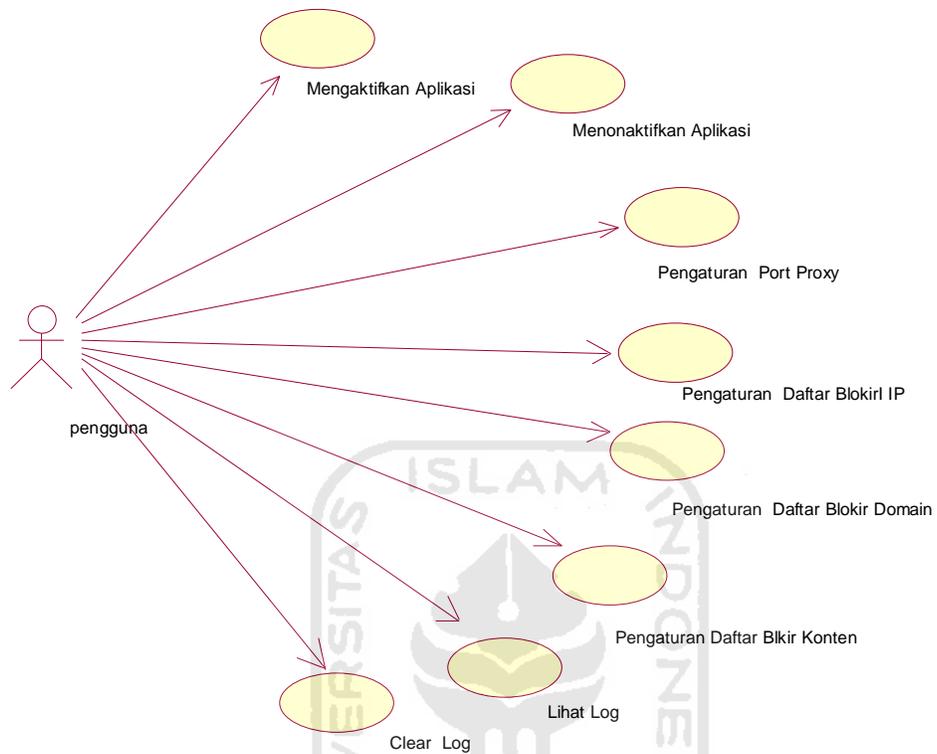
1. Wampp adalah aplikasi web server yang dapat dioperasikan di sistem operasi Windows. Wampp merupakan aplikasi pendukung
2. Visual Basic 6.0
Visual Basic adalah suatu bahasa pemrograman turunan bahasa BASIC yang menawarkan pengembangan aplikasi komputer berbasis grafik. Sintaks dalam Visual Basic adalah bahasa pemrograman tingkat tinggi, yaitu sintaks-sintaknya menyerupai bahasa sehari-hari (dalam hal ini bahasa Inggris).
3. Rational Rose
Rational Rose adalah perangkat lunak untuk perancangan suatu sistem. Hasil perancangan dapat berupa *activity diagram* ataupun *use case diagram*.

3.3 Perancangan Sistem

Perancangan yang digunakan dalam penelitian ini dibagi dalam dua kategori, yaitu perancangan sistem dan perancangan antarmuka pengguna. Perancangan sistem dilakukan menggunakan Use Case Diagram dan Activity Diagram.

3.3.1 Use Case Diagram

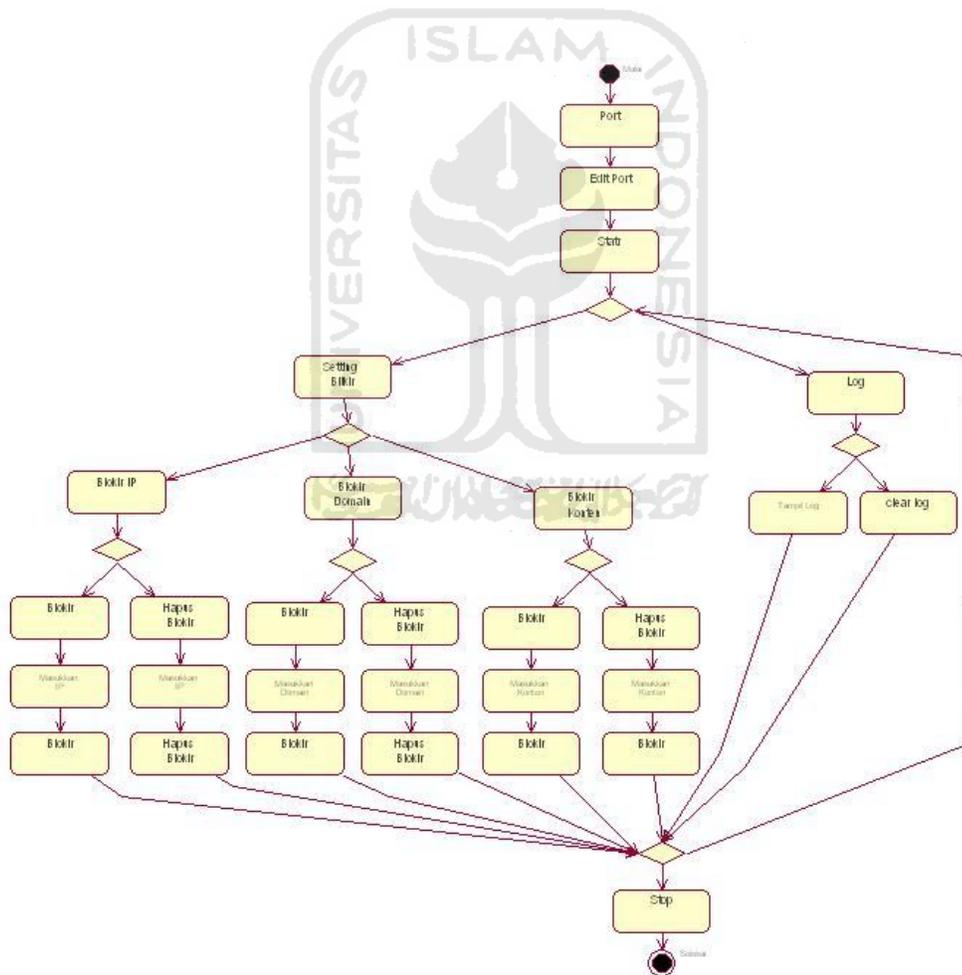
Use case diagram adalah suatu bentuk diagram yang menggambarkan fungsionalitas yang diharapkan dari sebuah aplikasi, dilihat dari perspektif pengguna di luar aplikasi. Aplikasi proxy dapat digambarkan dengan use case diagram seperti pada gambar berikut.



Gambar 3.2 Use Case Diagram Aplikasi Prox

Use case diagram di atas menunjukkan bahwa dalam aplikasi proxy hanya terdapat satu aktor yaitu pengguna dan tujuh use case yang meliputi mengaktifkan aplikasi proxy, menonaktifkan aplikasi proxy, pengaturan daftar blokir IP, pengaturan daftar blokir *domain*, pengaturan daftar blokir konten, mengganti port aplikasi proxy dan melihat *log* data pengaksesan klien serta menghapus *log*.

3.3.2 Activity Diagram



Gambar 3.3 Activity Diagram Aplikasi Proxy

Activity diagram di atas menunjukkan bahwa Aplikasi Proxy ini memiliki tiga komponen utama yaitu setting blokir, log, dan port.

Saat pertama kali pengguna membuka aplikasi ini akan tampil halaman utama. pada halaman utama ini pengguna dapat memilih setting blokir, log atau port. Pada penggunaan aplikasi proxy, pengguna harus mengaktifkan aplikasi terlebih dahulu dengan menekan tombol Start.

Proses kedua dalam aplikasi ini adalah setting blokir. pada proses ini terdapat tiga pengaturan pemblokiran. Pengguna dapat melakukan pengaturan pemblokiran yang meliputi:

1. Blokir IP, dengan mengisikan alamat IP dari situs-situs web yang akan diblokir.
2. Blokir Domain, dengan mengisikan nama domain dari situs-situs web yang akan diblokir.
3. Blokir Konten, dengan mengisikan daftar kata yang ingin diblokir pada konten situs-situs web

Proses ketiga dalam aplikasi proxy ini adalah log. Pada proses ini pengguna dapat melihat log data pengaksesan oleh *browser* klien. Selain itu pengguna juga dapat membersihkan tampilan log dengan menekan tombol clear.

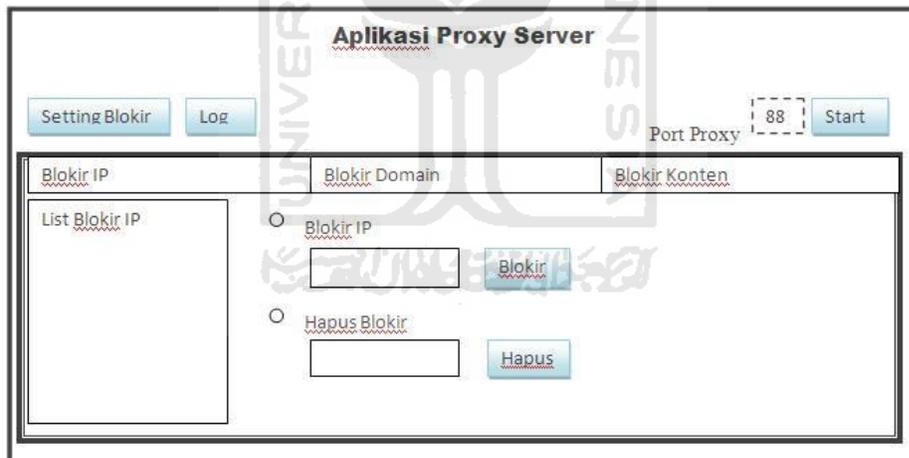
Proses terakhir pada aplikasi proxy ini adalah port. Pada proses ini pengguna dapat menentukan nomor port *default* proxy yang di kehendaki.

3.4 Perancangan Antarmuka

Rancangan antarmuka aplikasi proxy ini dibuat sederhana agar memudahkan penggunaan aplikasi ini. antarmuka aplikasi terdiri dari beberapa halaman sebagai berikut:

1. Antarmuka Halaman Blokir IP

Halaman ini merupakan halaman yang akan muncul pada saat pengguna memilih tab blokir IP untuk melakukan pengaturan pemblokiran alamat IP situs-situs web. Pada halaman ini, pengguna dapat memasukkan dan mengeluarkan alamat IP situs-situs web ke dalam dan dari daftar blokir IP. Rancangan halaman blokir IP dapat dilihat pada gambar 3.4.

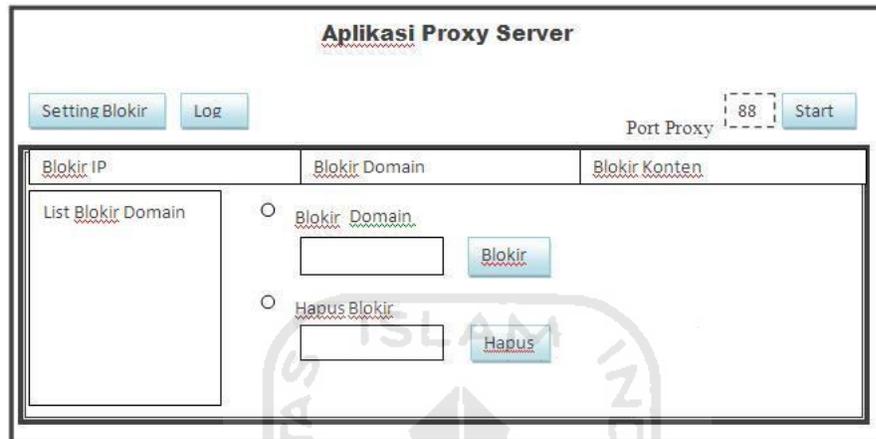


Gambar 3.4 Perancangan Antarmuka Halaman Blokir IP

2. Antarmuka Halaman Blokir Domain

Halaman ini merupakan halaman yang akan muncul pada saat pengguna memilih tab blokir *domain* untuk melakukan pengaturan pemblokiran *domain* situs-situs web. Pada halaman ini, pengguna dapat memasukkan dan

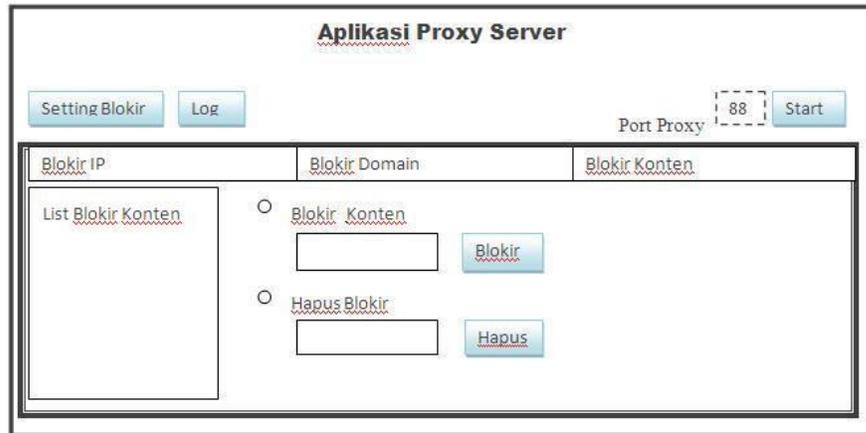
mengeluarkan nama *domain* situs-situs web ke dalam dan dari daftar blokir *domain*. Rancangan halaman blokir *domain* dapat dilihat pada gambar 3.5 :



Gambar 3.5 Perancangan Antarmuka Halaman Blokir Domain

3. Antarmuka Halaman Blokir Konten

Halaman ini merupakan halaman yang akan muncul pada saat pengguna memilih tab blokir Konten untuk melakukan pengaturan pemblokiran konten situs-situs web. Pada halaman ini, pengguna dapat memasukkan dan mengeluarkan daftar kata pada ke dalam dan dari daftar blokir konten. Rancangan halaman blokir konten dapat dilihat pada gambar 3.6 :

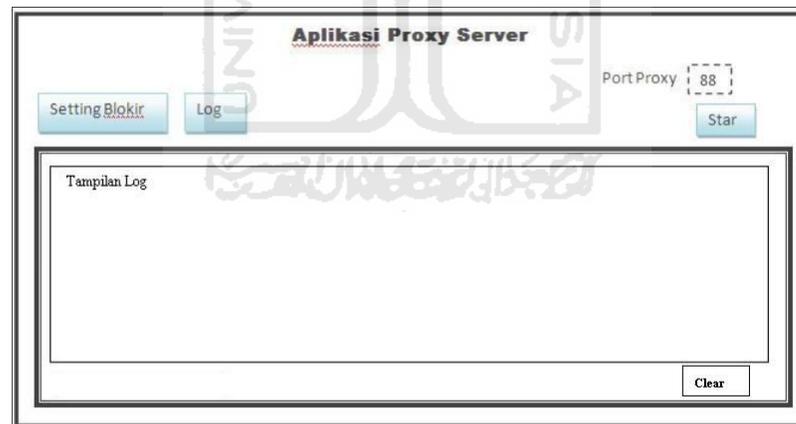


Gambar 3.6 Perancangan Antarmuka Halaman Blokir Konten

4. Antarmuka Halaman Log

Halaman ini akan muncul pada saat pengguna menekan tombol *log*. Pada halaman ini, pengguna dapat melihat *log* pengaksesan internet oleh klien.

Rancangan halaman log dapat dilihat pada gambar 3.7 :



Gambar 3.7 Perancangan Antarmuka Halaman Log

BAB 4

HASIL DAN PEMBAHASAN

4.1 Implementasi

Implementasi sistem bertujuan untuk memastikan bahwa sistem yang dibangun dapat bekerja dengan baik dan sesuai yang diharapkan. Sebelum sistem diimplementasikan dalam kehidupan sehari-hari maka sistem harus dipastikan telah bebas dari kesalahan. Kesalahan-kesalahan yang mungkin terjadi yaitu penulisan bahasa, kesalahan tampilan, dan kesalahan proses pada saat dioperasikan. Untuk dapat mengetahui kesalahan-kesalahan pada sistem yang dibangun maka harus dilakukan pengujian terhadap sistem tersebut.

4.1.1 Batasan Implementasi

Batasan implementasi pada Aplikasi Proxy adalah sebagai berikut,

1. Aplikasi proxy dapat berjalan dalam Local Area Network atau LAN.
2. Aplikasi proxy hanya dapat berjalan dalam sistem operasi Microsoft Windows XP.
3. Pengujian aplikasi proxy hanya menggunakan aplikasi *browser* pada klien.

4.1.2 Hasil

Pengujian aplikasi dilakukan untuk mengetahui bahwa aplikasi yang dibangun dapat bekerja dengan baik. pengujian dilakukan menggunakan aplikasi *browser* pada klien.

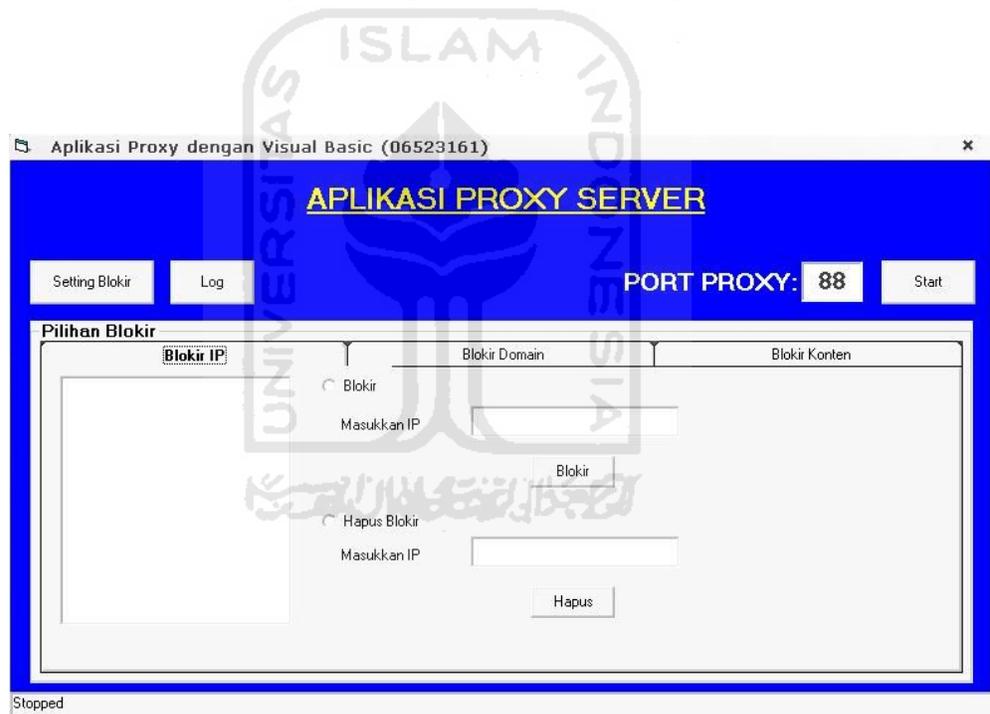
4.1.2.1 Aplikasi Proxy

Penggunaan aplikasi proxy yang dapat diakses oleh pengguna meliputi tampilan halaman pengaturan sampai hasil keluaran oleh aplikasi proxy.

1. Halaman Awal Aplikasi Proxy

Pada halaman awal ini, terdapat empat pilhan operasi yaitu setting blokir, log, edit port proxy, dan start untuk mengaktifkan aplikasi proxy.

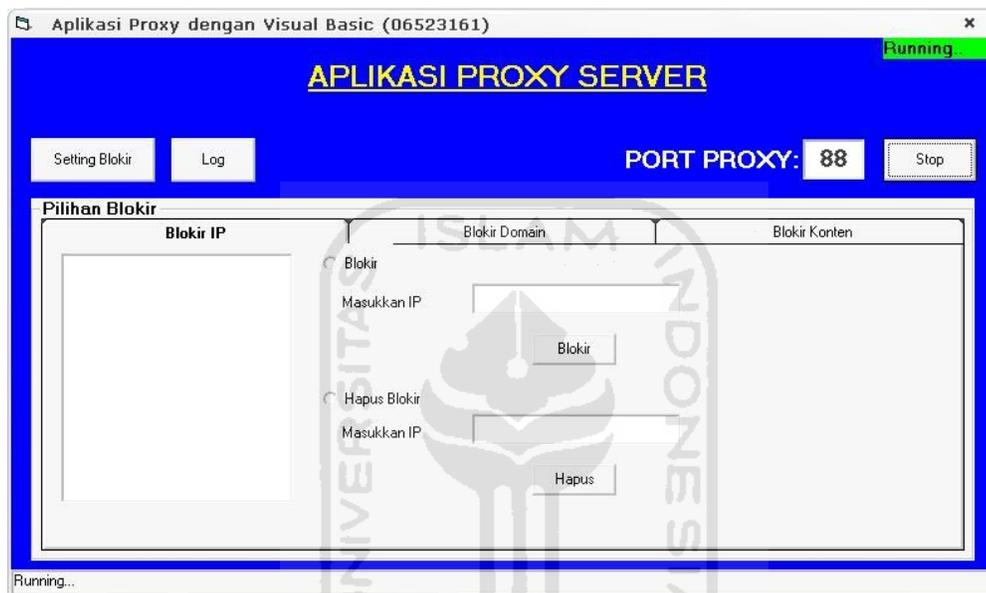
Gambar 4.1 berikut merupakan tampilan halaman awal Aplikasi Proxy



Gambar 4.1 Halaman Awal Aplikasi Proxy

2. Halaman Saat Aplikasi Dijalankan

Halaman ini merupakan tampilan saat aplikasi proxy dijalankan. Pengguna dapat mengaktifkan fungsi proxy dan penyaringan dengan menekan tombol start. pengguna dapat melihat seperti yang ditunjukkan pada gambar seperti gambar 4.2



Gambar 4.2 Halaman Aplikasi Saat Dijalankan

Berikut merupakan code dari proses Start dan Stop:

```
' TOMBOL START & STOP
Private Sub cmdStart_Click()
    If cmdStart.Caption = "Start" Then
        wsTCP(0).LocalPort = txtPort
        wsTCP(0).Listen
        lblStatus = "Running..."
        status.BackColor = &HFF00&
        status = "Running.."
        status.Visible = True
        cmdStart.Caption = "Stop"
```

```
Else
    cmdStart.Caption = "Start"
    wsTCP(0).Close
    lblStatus = "Stopped"
    status = ""
    status.Visible = False
End If
End Sub
```

3. Halaman Blokir

a. Halaman Blokir IP

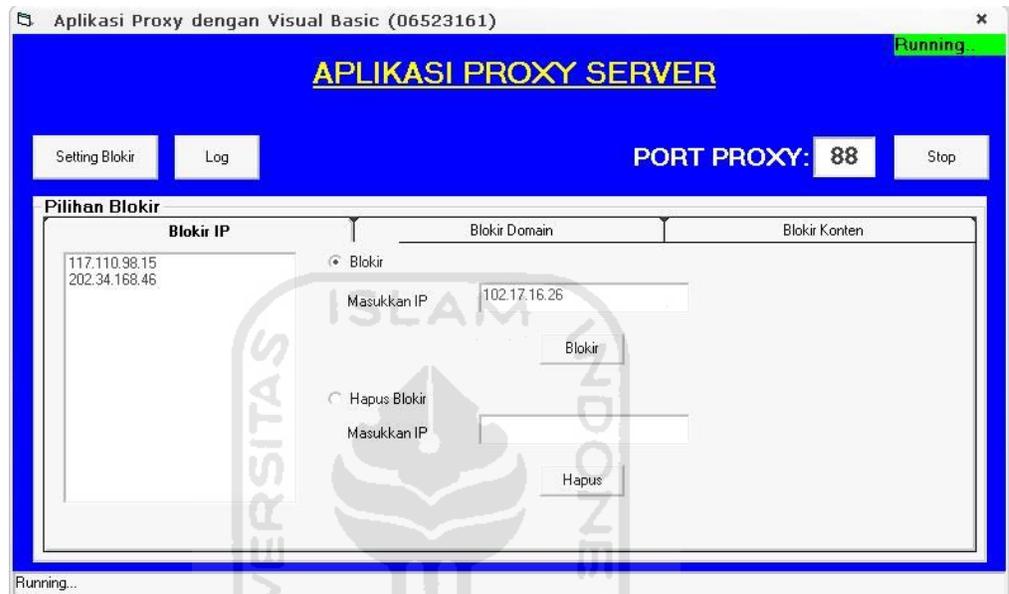
Halaman Blokir IP digunakan untuk melakukan pengaturan blokir IP.

Halaman Blokir IP ditunjukkan pada gambar 4.3 :



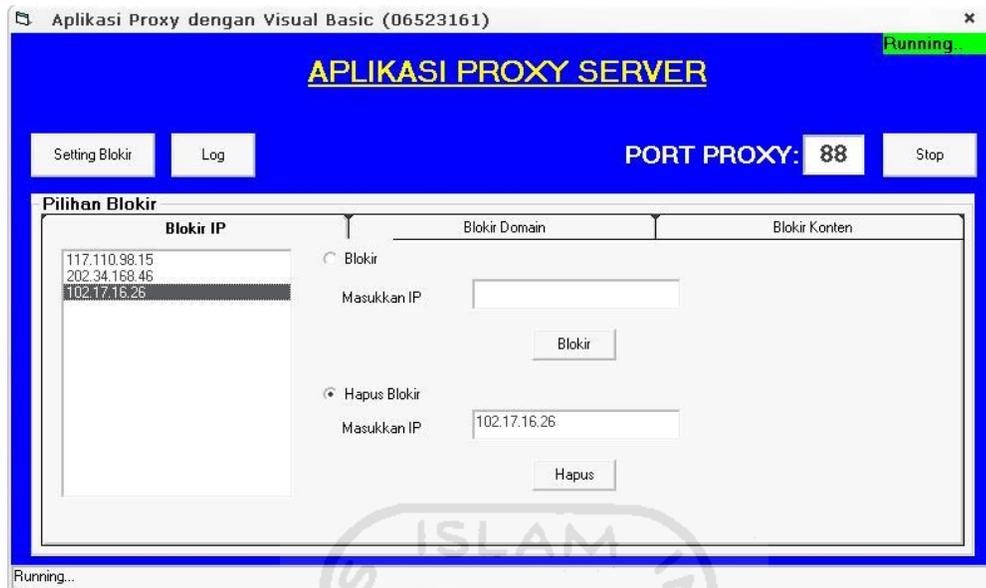
Gambar 4.3 Halaman Blokir IP

Pada halaman blokir IP, pengguna dapat mengisi alamat IP suatu situs web yang akan diblokir. Pengguna dapat melihat daftar IP yang diblokir seperti pada gambar 4.4 berikut.



Gambar 4.4 Hasil Masukan Blokir IP

Selain dapat mengisi alamat IP, pengguna juga dapat menghapus alamat IP dari dalam daftar blokir IP. Hal ini bertujuan untuk membuka kembali akses klien ke alamat IP tersebut, seperti ditunjukkan pada gambar 4.5 berikut.



Gambar 4.5 Hasil Hapus Blokir IP

Berikut ini adalah code dari proses blokir IP,

```
' SETTING BLOKIR IP
Dim hostname As String * 256
Dim hostent_addr As Long
Dim host As HOSTENT
Dim hostip_addr As Long
Dim temp_ip_address() As Byte
Dim i As Integer
Dim ip_address As String
Dim blockedByIp As Boolean

blockedByIp = False

hostent_addr = gethostbyname(hostname)
If hostent_addr = 0 Then
```

```

        MsgBox "Winsock.dll is not responding." &
vbNewLine

        Exit Sub

    End If

    RtlMoveMemory host, hostent_addr, LenB(host)
    RtlMoveMemory hostip_addr, host.hAddrList, 4

    blockedByIp = False

    'melihat semua ip address yang dimiliki oleh
    remote server apabila server memiliki alamat lebih
    dari 1
    Do
        ReDim temp_ip_address(1 To host.hLength)
        RtlMoveMemory temp_ip_address(1), hostip_addr,
host.hLength
        For i = 1 To host.hLength
            ip_address = ip_address & temp_ip_address(i) &
"."
        Next

        ip_address = Mid$(ip_address, 1, Len(ip_address) -
1)

        For i = 0 To listBlokirIp.ListCount - 1 Step 1
            If listBlokirIp.List(i) = ip_address Then
                blockedByIp = blockedByIp Or True
            Else
                'Lolos filter
            End If
        
```

```
Next i

If blockedByIp = True Then strHost = "exco-ganteng"

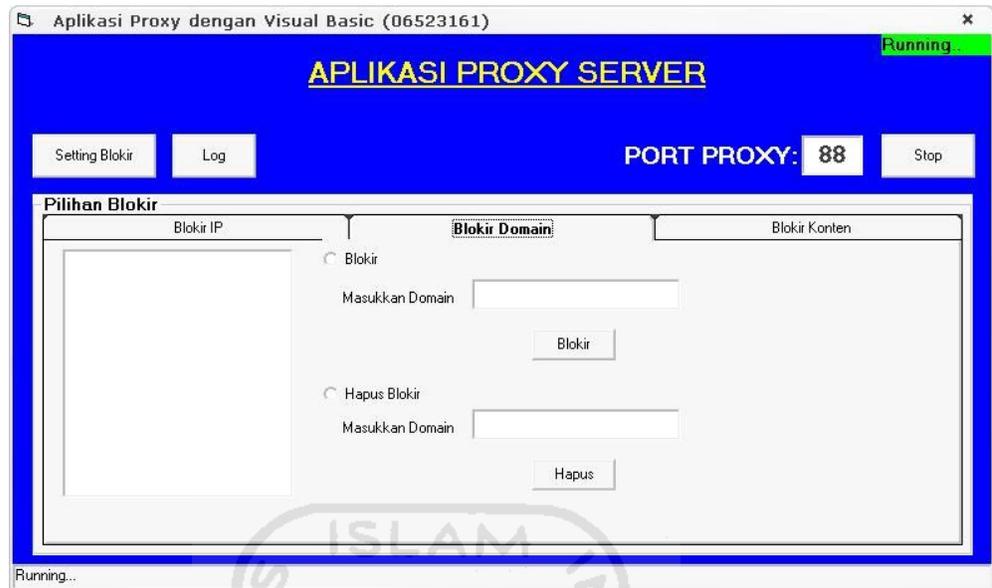
With wsProxy(Index)
    .RemoteHost = strHost
    .RemotePort = iPort
    .Connect
End With

strHost = ""
strHostFix = ""

End Sub
```

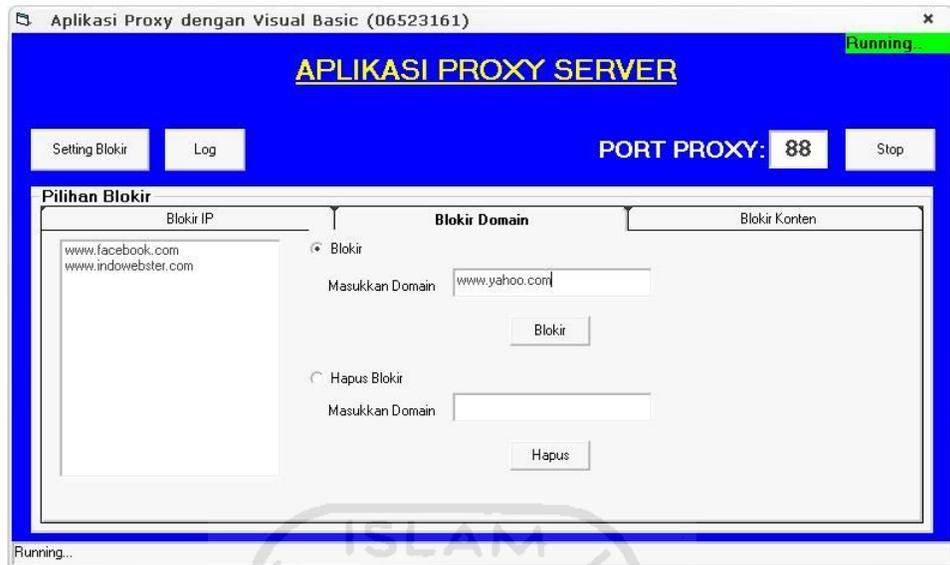
b. Halaman Blokir Domain

Halaman Blokir domain digunakan untuk melakukan pengaturan pada blokir domain. Gambar 4.6 berikut merupakan tampilan dari halaman blokir domain.



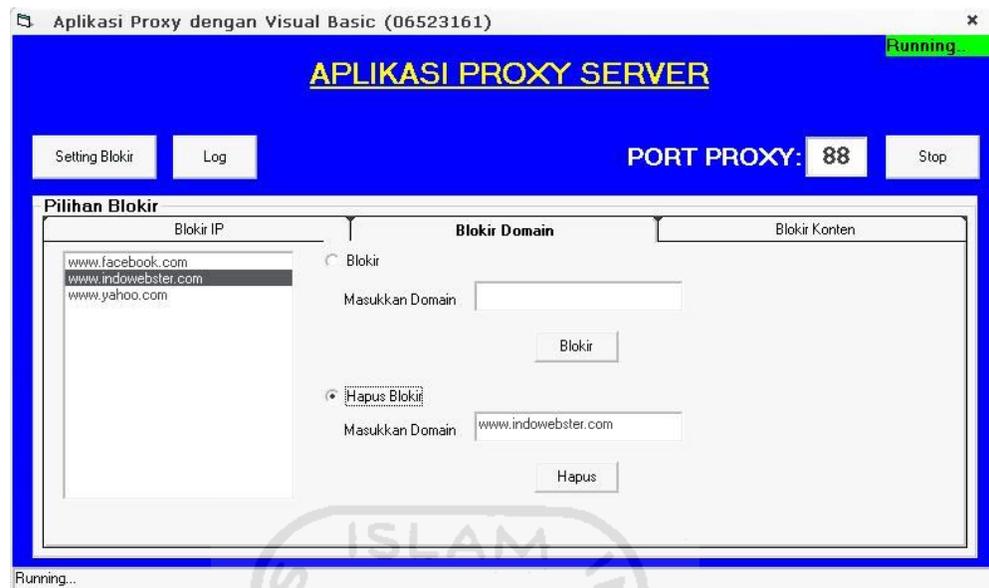
Gambar 4.6 Tampilan Halaman Blokir Domain

Pada halaman blokir domain, pengguna dapat mengisi nama domain suatu situs web yang akan diblokir. Pengguna dapat melihat daftar nama domain yang diblokir seperti pada gambar 4.7 :



Gambar 4.7 Hasil Masukkan Blokir Domain

Selain dapat mengisikan nama domain, pengguna juga dapat menghapus masukan domain dari daftar blokir domain. Hal ini bertujuan untuk membuka kembali akses klien yang ke nama domain tersebut, seperti ditunjukkan pada gambar 4.8 :



Gambar 4.8 Hasil Hapus Blokir Domain

Berikut ini adalah code dari proses blokir domain,

```
' SETTING BLOKIR DOMAIN

Dim hostname As String * 256

Dim hostent_addr As Long

Dim host As HOSTENT

Dim hostip_addr As Long

Dim temp_ip_address() As Byte

Dim i As Integer

Dim j As Integer

Dim ip_address As String

Dim blockedByDomain As Boolean
```

```
        blockedByDomain = False

        hostent_addr = gethostbyname(hostname)

        If hostent_addr = 0 Then
            MsgBox "Winsock.dll is not responding." &
vbNewLine
            Exit Sub
        End If

        RtlMoveMemory host, hostent_addr, LenB(host)
        RtlMoveMemory hostip_addr, host.hAddrList, 4

        If InStr(strHost, "/") > 0 Then strHost =
Left(strHost, InStr(strHost, "/") - 1)

        For j = 0 To listBlokirDomain.ListCount - 1 Step 1
            If listBlokirDomain.List(j) = strHost Then
                blockedByDomain = blockedByDomain Or True
            Else
                'lolos filter
            End If
        Next j

        If blockedByDomain = True Then strHost = "exco-
ganteng"
```

```

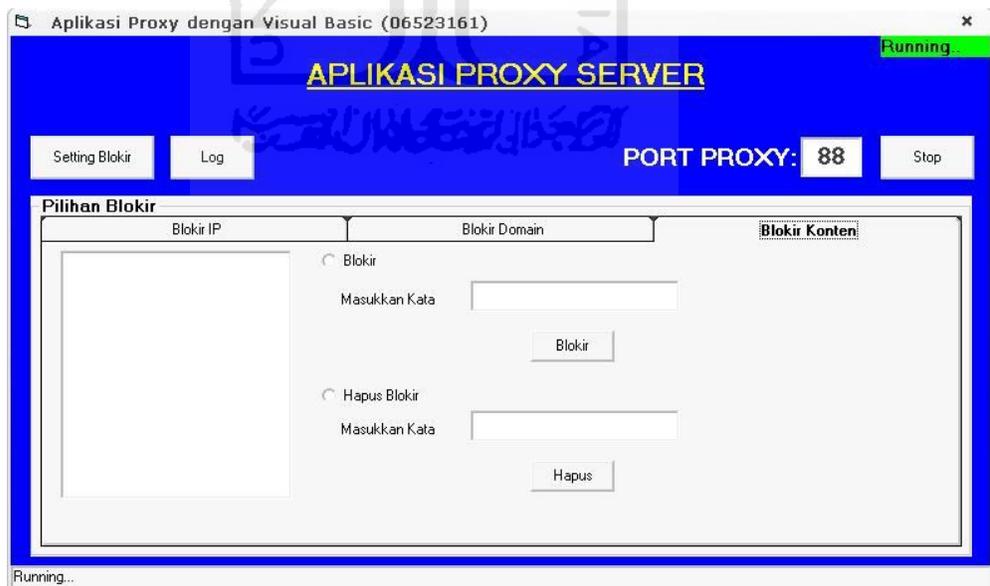
With wsProxy(Index)
    .RemoteHost = strHost
    .RemotePort = iPort
    .Connect
End With
strHost = ""
strHostFix = ""

End Sub

```

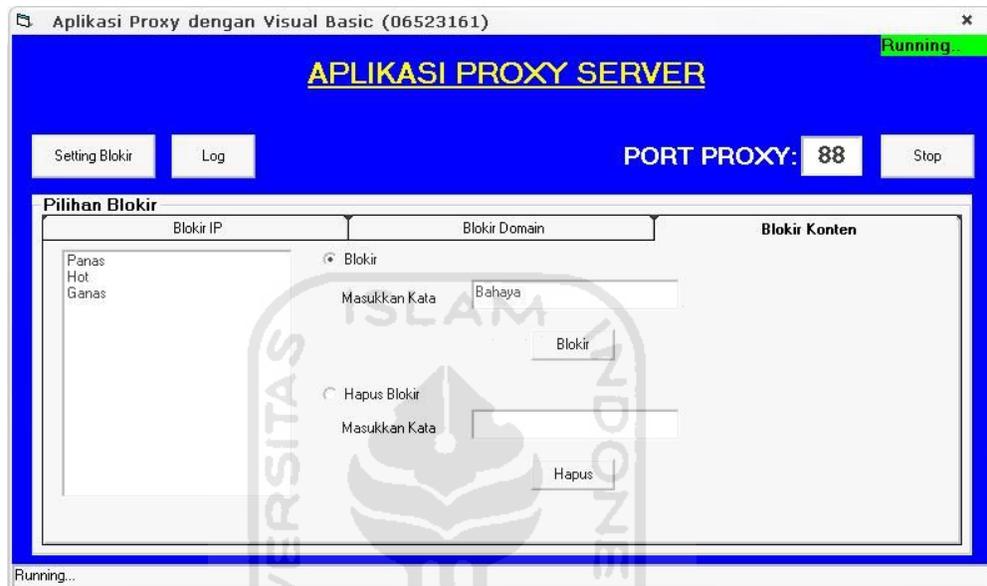
c. Halaman Blokir Konten

Halaman blokir konten digunakan untuk melakukan pengaturan pada blokir konten. Halaman blokir konten ditunjukkan pada gambar 4.9 :



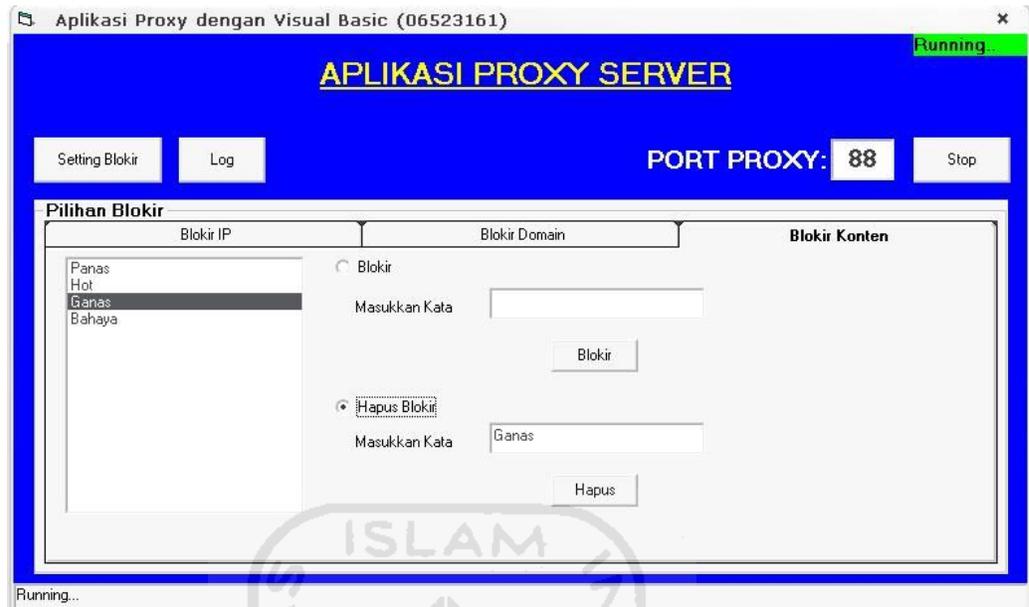
Gambar4.9 Halaman Blokir Konten

Pada halaman blokir konten , pengguna dapat mengisikan daftar kata akan diblokir . Pengguna dapat melihat daftar kata yang digunakan untuk memblokir konten situs web, seperti pada gambar gambar 4.10 :



Gambar 4.10 Hasil Masukkan Blokir Konten

Selain dapat mengisikan daftar kata yang akan diblokir, pengguna juga dapat menghapus kata dari daftar kata tersebut. Hal ini bertujuan untuk membuka kembali akses klien yang ke situs web yang mengandung kata-kata tersebut, seperti ditunjukkan pada gambar 4.11 :



Gambar 4.11 Hasil Hapus Blokir Konten

Berikut ini adalah code dari proses blokir konten,

```

' Blokir Konten
Dim sURL As String
Dim sHost As String
Dim sPage As String
Dim lPort As Long
Dim txtSource As String
Dim blockedByContent As Boolean
Private Sub GetHTMLSource(ByVal sURL As String)
    txtSource = ""
    sHost = Mid(sURL, InStr(sURL, "://") + 3)
    If InStr(sHost, "/") > 0 Then
        sPage = Mid(sHost, InStr(sHost, "/"))
        sHost = Left(sHost, InStr(sHost, "/") - 1)
    Else

```

```

        sPage = "/"
    End If

    If InStr(sHost, ":") > 0 Then
        lPort = Mid(sHost, InStr(sHost, ":") + 1)
        sHost = Left(sHost, InStr(sHost, ":") - 1)
    Else
        lPort = 80
    End If

    With wsLoadCode
        If .State <> sckClosed Then .Close
        .RemoteHost = sHost
        .RemotePort = lPort
        .Connect
    End With
End Sub

Private Sub wsLoadCode_Connect()
    Timer1.Enabled = True

    wsLoadCode.SendData "GET " & sPage & " HTTP/1.0" &
Chr(10) & Chr(10)

End Sub

Private Sub wsLoadCode_DataArrival(ByVal bytesTotal As
Long)

    Timer1.Enabled = False

    Dim sBuffer As String

    wsLoadCode.GetData sBuffer

    txtSource = txtSource & sBuffer

    txLog = txLog & vbNewLine & vbNewLine & sBuffer &
vbNewLine

    Dim n As Integer

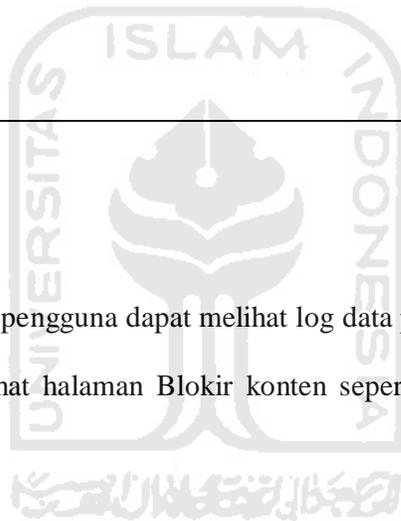
```

```
        blockedByContent = False
    For n = 0 To listBlokirKonten.ListCount - 1 Step 1
        If InStr(txtSource, listBlokirKonten.List(n)) > 0
Then
            blockedByContent = blockedByContent Or True
        Else
            'lolos filter
        End If
    Next n

End Sub
```

4. Halaman Log

Pada halaman log ini pengguna dapat melihat log data pengaksesan oleh klien. Pengguna akan melihat halaman Blokir konten seperti gambar 4.8 dibawah ini.





Gambar 4.12 Halaman Log

Berikut ini adalah code dari log,

```
' LOG DATA

    txLog.Text = txLog.Text & "(" & Index & ") " &
s(Index) & vbNewLine

'melihat domain dan IP destination & client

    txLog.Text = txLog.Text & "==== strHost :" &
strHostFix & " =====" & vbNewLine

    txLog.Text = txLog.Text & "IP Client :" &
wsTCP(Index).RemoteHostIP & vbNewLine

    txLog.Text = txLog.Text & "IP Client :" &
wsTCP(Index).LocalIP & "(" & wsTCP(Index).LocalHostName &
")" & vbNewLine & vbNewLine
```

Setelah aplikasi proxy diaktifkan dan pengguna telah melakukan pengaturan pada aplikasi proxy yang meliputi pengaturan blokir IP, blokir domain, dan blokir konten maka jika klien melakukan pengaksesan suatu situs web yang mengandung

aturan dari pengaturan yang telah dilakukan oleh pengguna maka aplikasi proxy akan mengirimkan peringatan pada *browser* klien yang menyatakan akses dilarang. Seperti yang dapat dilihat pada gambar 4.13 :



Gambar 4.13 Tampilan Peringatan Pada Browser Klien

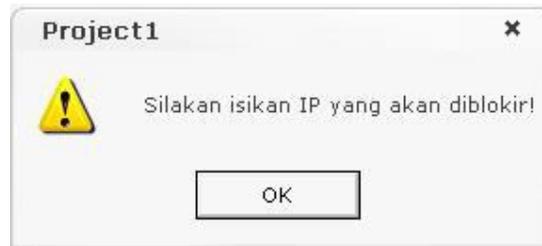
4.1.2.2 Analisis Aplikasi

Analisa aplikasi adalah merupakan proses pengujian aplikasi untuk mengetahui kinerja aplikasi terhadap kebenaran data pada aplikasi.

1. Pengujian Blokir IP

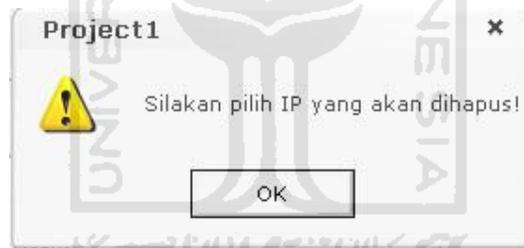
Pada pengaturan blokir IP, pengguna harus memasukkan alamat IP dari situs web yang akan diblokir. Apabila textbox masukkan IP tidak diisi dan

pengguna sudah menekan tombol blokir, maka aplikasi akan menampilkan pesan. Seperti yang dapat dilihat pada gambar 4.14 :



Gambar 4.14 Peringatan Input Blokir IP

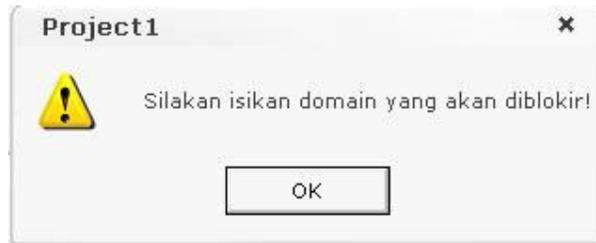
Sama halnya dengan hapus blokir IP , jika textbox hapus ini belum terisi oleh pengguna dan pengguna sudah menekan tombol hapus maka aplikasi akan menampilkan pesan. Seperti yang dapat dilihat pada gambar 4.15.



Gambar 4.15 Peringatan Hapus Blokir IP

2. Pengujian Blokir Domain

Pada pengaturan blokir domain, pengguna harus menginputkan domain dari situs web yang akan diblokir. Apabila textbox masukkan IP tidak terisi dan pengguna sudah menekan tombol blokir, maka aplikasi akan menampilkan pesan. Seperti yang dapat dilihat pada gambar 4.16 :



Gambar 4.16 Peringatan Blokir Domain

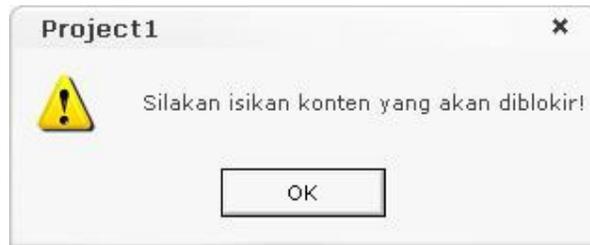
Sama halnya pada penghapusan blokir domain, jika textbox hapus ini belum terisi oleh pengguna dan pengguna sudah menekan tombol hapus, maka aplikasi akan menampilkan pesan. Seperti yang dapat dilihat pada gambar 4.17 :



Gambar4.17 Peringatan Hapus Blokir Domain

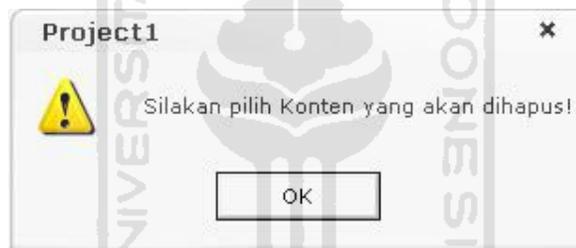
3. Pengujian Blokir Konten

Pada pengaturan blokir konten, pengguna harus menginputkan daftar kata yang akan diblokir. Apabila textbox masukkan konten tidak terisi dan pengguna sudah menekan tombol blokir, maka aplikasi akan menampilkan pesan. Seperti yang dapat dilihat pada gambar 4.18 :



Gambar 4.18 Peringatan Input Blokir Konten

Sama halnya pada penghapusan blokir konten , jika textbox hapus ini belum terisi oleh pengguna dan pengguna sudah menekan tombol hapus maka aplikasi akan menampilkan pesan. Seperti yang dapat dilihat pada gambar 4.19 :



Gambar 4.19 Peringatan Hapus Blokir Konten

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pembahasan pada bab-bab sebelumnya, maka dapat diambil kesimpulan sebagai berikut:

1. Aplikasi proxy yang dibangun telah dapat melakukan pemblokiran terhadap ip situs web.
2. Aplikasi proxy yang dibangun telah dapat melakukan pemblokiran terhadap domain situs web.
3. Aplikasi proxy yang dibangun telah dapat melakukan pemblokiran terhadap konten situs web.

5.2 Saran

Beberapa saran yang dapat digunakan untuk pengembangan aplikasi proxy ini antara lain:

1. Menyempurnakan tampilan aplikasi sehingga terlihat lebih menarik.
2. Menambahkan kemampuan penyimpanan pengaturan ke file.
3. Mengembangkan sistem agar tidak hanya dapat berjalan pada sistem operasi microsoft windows xp, tapi juga mampu berjalan pada microsoft windows 7 dan microsoft windows vista.
4. Mengembangkan sistem agar menjadi lebih bermanfaat lagi dengan menambahkan fitur yang lebih komplek lagi seperti fitur pemblokiran port.

DAFTAR PUSTAKA

- Asisten Laboratorium Sistem dan Jaringan Komputer. 2007. **Modul Praktikum Jaringan Komputer**. Yogyakarta.
- [ABI09] Abisono, Dimas. 2009. **Jaringan Komputer**. <http://ucaimut.wordpress.com/2009/11/18/ip-address/> diakses pada 28 jan 2011 jam 11.30
- Hirin, A. M. 2008. **Seni Pemrograman Aplikasi Xtreme Coding Menggunakan Visual Basic**. DSI Publishing.
- MADCOM. 2008. **Microsoft Visual Basic 6.0 & Crystal Report 2008**. Yogyakarta: Andi.
- Retna Prasetia dan Catur Edi Widodo. 2004. *Interfacing Port Paralel dan Port Serial Komputer dengan Visual Basic 6.0*. Yogyakarta: Andi.
- VygoriViva CR. 2008. **Trik Pemrograman Jaringan dengan Visual Basic 6**. Yogyakarta: Gava Media.
- Wagito. 2007. **Jaringan Komputer Teori dan Implementasi Berbasis Linux**. Yogyakarta: Gava Media.