ANALISIS PENCEGAHAN AKSES WEBSITE KATEGORI DILARANG

Muhammad Sholeh
Teknik Informatika, Fakultas Teknologi Industri
Institut Sains & Teknologi AKPRIND Yogyakarta
Jl. Kalisahak 28 Komplek Balapan Yogyakarta
muhash@akprind.ac.id

ABSTRACT

Various current information easily found on the Internet, ranging from science, business, community information leading up to pornography. Internet is like a wilderness in which there are many problems and depending on the user whether to use the Internet as a positive side or use the internet from a negative side. Not all the information on the Internet has positive benefit, so that the efforts to make the prevention of harmful information must be done . Block processing of certain itus, is absolutely necessary to avoid accessing the site from users who are not eligible. Access restriction or certain considerations that a site is not allowed to access must be done carefully. In this research it will study how the process of blocking on certain sites and analysis of various applications or software that is often used to block. The research process will elaborate study of the site name blocks toth and blocks to the keyword search on search engines.

Keywords: Internet, block, site

INTISARI

Berbagai informasi saat ini dengan mudah ditemukan di Internet, mulai dari ilmu pengetahuan, bisnis, komunitas sampai informasi yang menjurus ke pornografi. Internet ibarat hutan belantara yang didalamnya terdapat berbagai macam persoalan dan tergantung dari pemakai apakah akan memanfaatkan internet sebagai sisi yang positif atau mempergunakan internet dari sisi yang negatif.

Tidak semua informasi yang ada di Internet bermanfaat positif , upaya untuk melakukan pencegahan terhadap informasi yang membahayakan harus dilakukan. Melakukan proses balokir terhadap itus tertentu, mutlak diperlukan untuk menghindari pengaksesan situs dari pemakai yang tidak berhak. Pembatasan pengaksesan atau pertimbangan tertentu agar suatu situs tidak diijinkan untuk diakses harus dilakukan dengan hati-hati.

Dalam penelitian ini akan diteliti bagaimana proses melakukan blokir terhadap situs tertentu serta analisis berbagai aplikasi atau software yang sering digunakan untuk blokir. Proses penelitian akan dikupas dari sisi blok nama situs serta blok kata kunci dalam proses pencarian di mesin pencari.

Kata kunci : Internet, blok, situs

PENDAHULUAN

Berbagai informasi saat ini dengan mudah ditemukan di Internet, mulai dari ilmu pengetahuan, bisnis, komunitas sampai informasi yang menjurus ke pornografi. Internet ibarat hutan belantara yang didalamnya terdapat berbagai macam persoalan dan tergantung dari pemakai apakah akan memanfaatkan internet sebagai sisi yang positif atau mempergunakan internet dari sisi yang negatif.

Berbagai slogan, himbauan bahkan undang-undang pun sudah dikeluarkan, agar internet tidak digunakan untuk hal-hal yang bersifat negatif, misal digunakan untuk mengakses situs-situs pornografi. Dalam undang-undang republik indonesia nomor 11 tahun 2008 tentang informasi dan transaksi elektronik, mengenai pornografi sudah diatu dalam bab VII perbuatan yang dilarang , pasal 27

(1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik adan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

Berbagai upaya baik himbauan dari Pemerintah ataupun lembaga lainnya agar penyebaran informasi atau pengaksesan

terhadap situs-situs yang dilarang (pornografi) sudah dilakukan. Himbauan moral sampai formal dalam bentuk undang-undang yang ada sanksi hukum sudah disahkan tetapi, dalam realita perkembangan internet yang berisi pronografi masih terus berkembang dan selalu tumbuh.

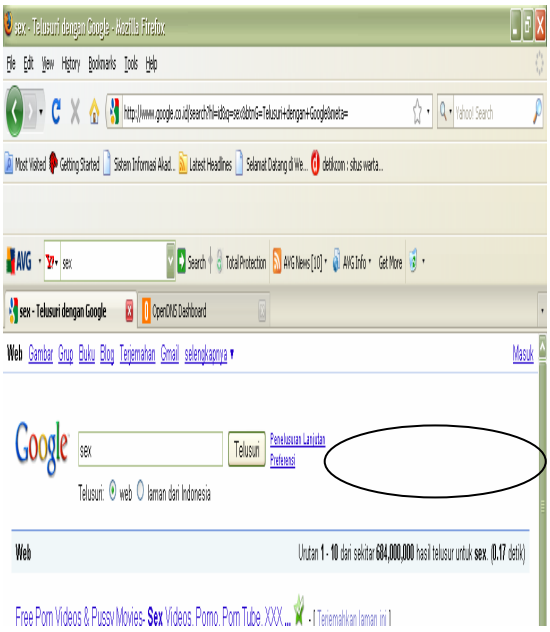
Pencegahan agar pengaksesan di situs-situs porno dapat diminimalkan harus selalu dilakukan baik dikomunitas kampus, warnet atau keluarga.

PERMASALAHAN

Konten pornografi atau yang dikategorikan dilarang dapat dilakukan proses *filtering*, tetapi proses ini akan selalu muncul soal efektifitas. Beberapa hal yang dapat menjadi penyebab keefektifan tersebut tidaklah selalu soal kecanggihan piranti lunak yang digunakan. Siapapun memang bisa mengunduh dan menginstal berlapis piranti lunak yang berfungsi memblok atau menyaring konten pornografi dari Internet, baik pada tingkat komputer personal (PC), server pada warnet hingga *Internet Service Provider* (ISP) sekalipun. Tetapi sangatlah naïf bila kita percaya bahwa konten pornografi di Internet dapat efektif dihalau hanya dengan melakukan pemblokiran ataupun penyaringan secara teknologi. Alasannya, bisa berangkat dengan mengkaji Materi yang Tidak Layak.

Pengguna Internet (anak-anak, remaja) bisa saja mendapatkan atau menemukan (sengaja atupun tidak) materi-materi yang tidak layak. Materi-materi tersebut misalnya materi pornografi, seksual, kebencian, rasisme, kejahatan, kekerasan perilaku ataupun hal-hal lain yang sifatnya menghasut untuk melakukan aktifitas yang berbahaya atau ilegal. Seseorang bisa saja secara tidak sengaja kesasar ke situs-situs negatif. Hal tersebut lantaran banyak situs-situs yang menggunakan nama domain / alamat yang menarik, atau bisa juga karena situs-situs tersebut mengelabui *search engine* melalui teknologi *meta-tags*. Salah satu cara untuk menghadapi resiko ini adalah dengan memasang *parental software*.

Khusus untuk perilaku pengguna Internet di Indonesia, Google Trends memaparkan sejumlah data. Ternyata meskipun jumlah pengguna Internet masih terkonsentrasi di ibukota, Jakarta hanya menduduki posisi ke-5 kota dengan jumlah pencari konten dewasa dengan memasukkan kata kunci yang sangat umum, ‘sex’. Setelah Jakarta, kemudian disusul oleh Bandung. Kota yang paling banyak adalah kota Semarang, kemudian Yogyakarta, Medan dan kemudian disusul Surabaya. Jika kita mencari dengan kata kunci ‘sex’ di Google, maka akan muncul 662.000.000 situs, 568.881 video, 157.000.000 gambar dan 111.057.569 blog. (diakses November 2009), Dari permasalahan tersebut, bagaimana upaya untuk menyaring informasi dari sekian banyak sumber tersebut. Apalagi jika harus dipilah antara informasi ‘sex’ yang layak untuk keperluan pendidikan kesehatan, ilmu bercinta ataupun sekedar sebagai pemuas birahi belaka. Data ini tentunya berubah seiring dengan berkembangan dari pemakai internet.



Gambar 1 Pencarian dengan kata kunci tertentu

PEMBAHASAN

Secara umum, software pengaman tersebut terdiri atas:

- *Software Parental* (Filter, Monitor dan Penjadwalan). Software ini untuk mencegah anak sengaja atau tidak sengaja membukan dan/atau melihat berbagai gambar yang tak layak (pornografi, sadisme, dan sebagainya) yang terdapat di situs Internet. Software ini juga akan memudahkan orang tua ataupun pengasuh untuk memonitor aktifitas anak selama online dengan berbagai variasi metode pengawasan. Fungsi lain dari software ini adalah untuk membatasi jumlah / durasi waktu anak dalam menggunakan Internet. Termasuk untuk pengaturan hari dan jam tertentu sehingga komputer dapat atau tidak dapat digunakan oleh anak untuk ber-Internet.

- *Software Browser* Anak. *Software browser* adalah yang menjadi perantara utama antara Internet dengan komputer yang digunakan. *Browser* anak secara umum telah dirancang untuk semaksimal mungkin menyaring berbagai situs, gambar atau teks yang tak layak diterima anak. Browser anak juga didisain untuk menarik dan mudah digunakan oleh anak. Contoh software: Kid Rocket (www.kidrocket.org)
- *Software Anti-Spyware*. Software ini secara khusus akan berfungsi mendeteksi dan mencegah program jahat seperti *sypware* dan *adware* yang gemar menyedot data-data rahasia / privasi kita secara diam-diam. Contoh software: *Ad-Aware* (www.lavasoft.de)
- Software Anti-Virus. Software ini untuk mencegah agar program jahat perusak data semisal virus, *worm* dan *trojan horse* bercokol dan berkembang-biak di komputer kita. Contoh software: AVG anti-virus (www.grisoft.com)

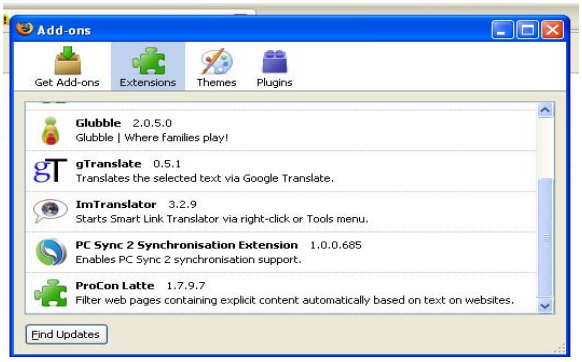
HASIL PENELITIAN

Add-on Internet Filter pada browser Mozilla Firefox

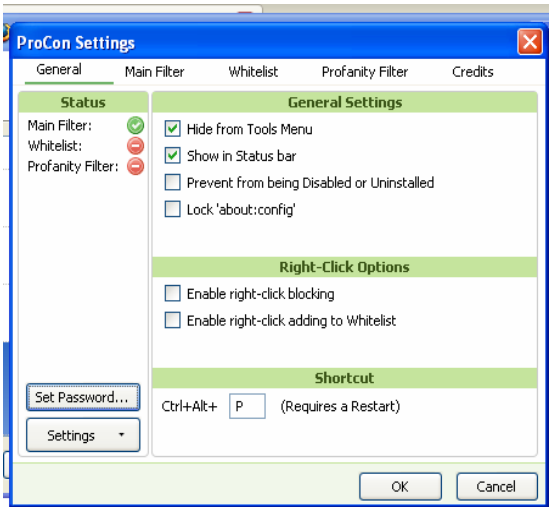
ProCon Latte

ProCon Latte, adalah sebuah *addon content filter browser* firefox. Ia dapat menyaring segala jenis situs-situs berbahaya (pornografi, judi, *hacking*, *cracking*, dan sebagainya), juga dapat memblokir semua lalu lintas data lainya, tersedia White List. ProCon juga memiliki proteksi password. Bisa diakses di https://addons.mozilla.org/id/firefox/addon/1803. Support Firefox: 2.0 – 3.5.*

Agar *software procon latte* dapat digunakan di dalam browser, khususnya browser monzilla, pengguna harus melakukan proses penginstalan aplikasi tersebut dan melakukan proses konfigurasi. Adapun hasil instalasi dapat di lihat pada gambar 2 dan proses konfigurasi pada gambar 3..



Gambar 2 . Tampilan add on di browser Mozilla firefox



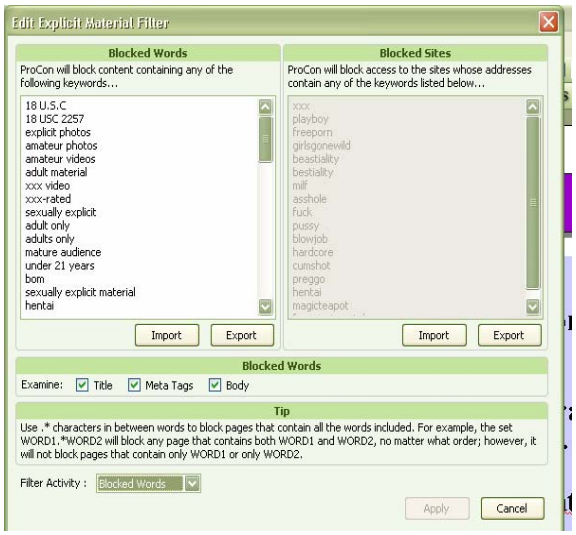
Gambar 3. Tampilan proses konfigurasi

Blokir Kata Kunci

Proses konfigurasi yang sangat penting dalam aplikasi Procon diantaranya adalah memasukan kata/kalimat yang dikategorikan dilarang.

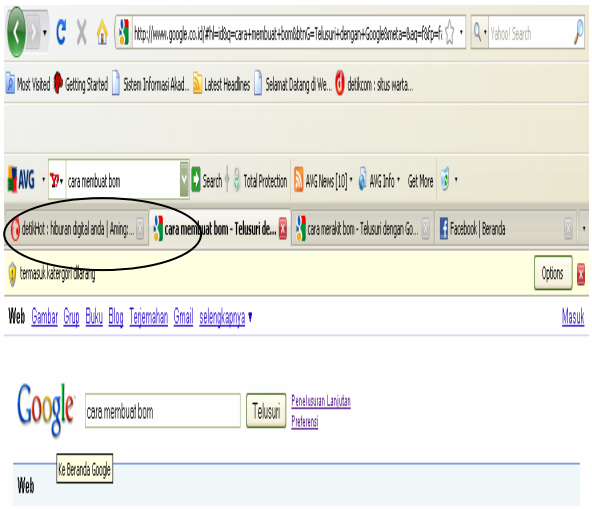
Google sebagai salah satu mesin pencari, memberikan andil yang cukup besar dalam menjawab rasa ingin tahu dari pemakai Internet. Dengan mesin pencari tersebut pemakai dapat mendapatkan *link-link* yang kadang menuju *link* yang berisi informasi negatif.

Cara kerja dari memblokiran ini, setiap kata yang dimasukan dalam mesin pencari akan dilakukan proses pengecekan dalam basis data. Bila kata tersebut terdapat dalam kategori yang dilarang, pencarian tersebut tidak akan diteruskan ke mesin pencari.



Gambar 4. Pemasukan kata kunci

Dengan melakukan blokir kata kunci, pemakai internet dapat dihindarkan dari hasil pencarian yang akan mengarahkan ke halaman website yang bersifat negatif.

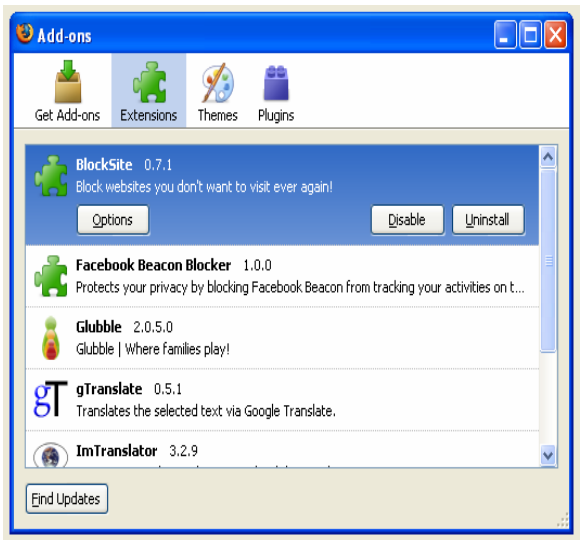


Gambar 5 Hasil pencarian yang tidak diteruskan

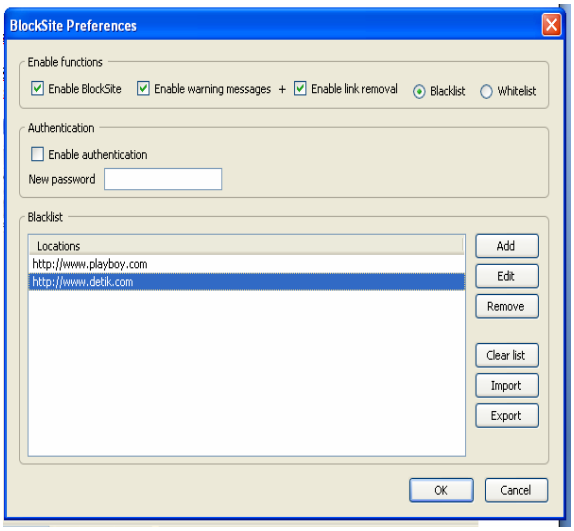
Blocksite

Berbeda dengan procon, aplikasi BlockSite, digunakan untuk memblok situs-situs yang kita inginkan. *Add-on* ini tidak difungsikan sebagai parental control utama.

Langkah awal dalam pemakaian aplikasi blocksite adalah melakukan proses instalasi dan proses pengaturan konfigutrasi, terutama halaman-halaman situs yang dilarang.



Gambar 6 *Add on blocksite* di browser mozilla firefox

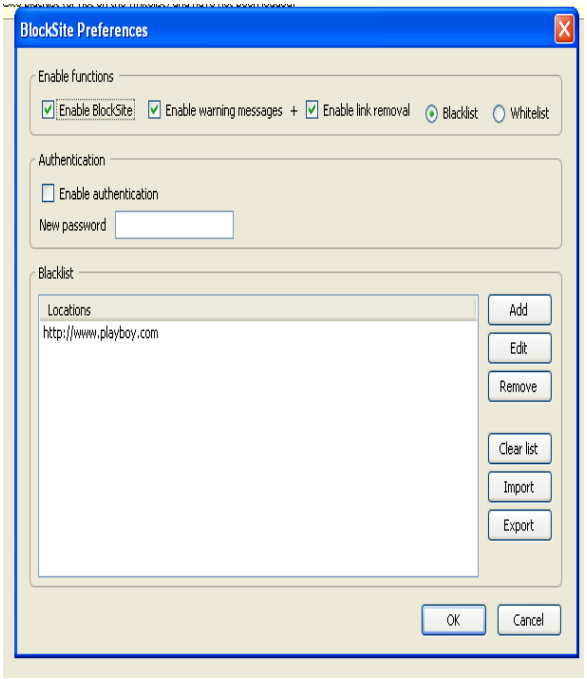


Gambar 7 Konfigurasi situs dilarang di *blocksite*

Hasil dari konfigurasi dapat dicek dengan melakukan pengaksesan terhadap situs yang di blok, dalam contoh di atas, dilakukan proses pemblokiran pada www.detik.com. Hasil pemblokan ini akan terlihat bila melakukan pemanggilan terhadap www.detik.com (gambar 10)

Gambar 8 Hasil pemblokiran

Bila diinginkan halaman www.detik.com dapat kembali diakses, maka proses konfigurasi harus dilakukan dengan menghilangkan www.detik.com dari blok. Gambar 90 dilakukan proses konfigurasi dengan melakukan perubahan www.detik.com yang semula diblok dihilangkan dari pemblokiran. Pada gambar 10, www.detik.com kembali dapat digunakan



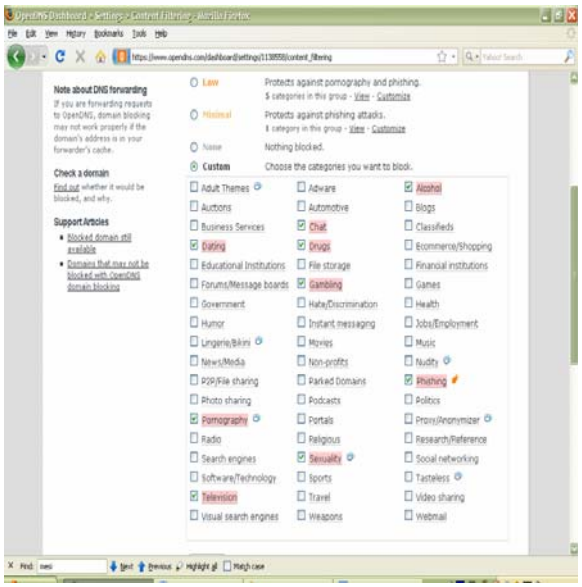
Gambar 9 Konfigurasi untuk menghilangkan situs yang diblok

Gambar 10 Situs yang tidak diblok

Blokir dengan OpenDNS

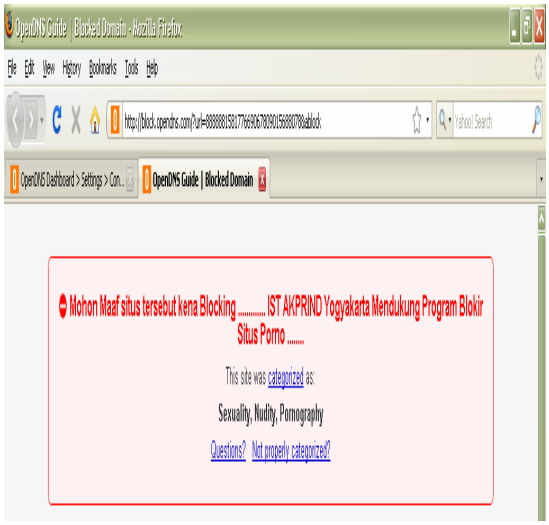
Proses pemblokiran di atas hanya bisa digunakan pada pengguna tunggal dan berlaku hanya untuk satu komputer saja. Proses pemblokiran dapat dilakukan pada *proxy*. Pemblokiran dengan *proxy* berlaku untuk semua pengguna yang menggunakan *proxy* yang telah di*setting*.

Pemblokiran dengan *proxy* sangat penting terutama untuk komputer yang ada di kantor, sekolah ataupun warung interne t. Layanan blokir ini bersifat gratis dan online. Pemakai dapat melakukan pendaftaran untuk mengaktifkan layanan ini. Dalam proses memblokiran ini, banyak jenis pilihan yang dapat ditentukan untuk mendefinisikan situs yang dikategorikan dalam larangan pengaksesan.



Gambar 11 Kategori Pemblokiran dengan OpenDNS

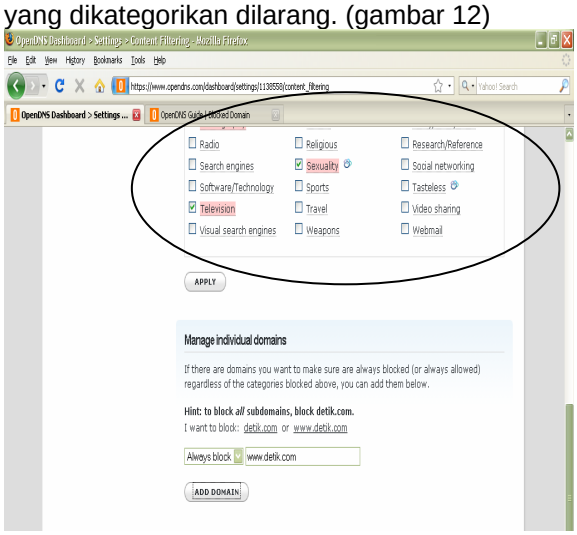
Hasil konfigurasi tersebut, akan dilakukan proses pengecekan dari setiap ada pengguna yang melakukan pengaksesan suatu web. Jika web yang diakses termasuk kategori yang diblok, maka website tersebut tidak akan diteruskan.



Gambar 12 Hasil Pemblokiran dengan OpenDNS

Blokir nama domain tertentu.

Seiring dengan makin banyaknya pengguna Internet, openDNS kadang tidak bisa memfilter nama domain yang sebenarnya masuk kategori dilarang. Hal ini disebabkan nama domain tersebut baru dan belum masuk di basis data openDNS. Antisipasi untuk nama domain yang belum masuk ini, dapat dilakukan dengan membuat basisdata sendiri yang berisi domain-domain yang dikategorikan dilarang. Didalam openDNS sendiri sebenarnya disediakan fasilitas untuk menambahkan nama *domain* yang dikategorikan dilarang. (gambar 12)



Gambar 13 Pemblokiran dengan OpenDNS berdasarkan Nama Domain

Disamping menggunakan openDNS memblokiran nama domain dapat juga dilakukan dengan memanfaatkan fasilitas *file host* yang ada di dalam Windows XP (gambar 13). Proses pemblokiran dengan *file Host* ini dapat dilakukan karena setiap pengaksesan internet, browser akan mengirimkan *request* ke sebuah *server DNS* dan *server* tersebut akan mencari alamat IP yang tepat dan kemudian mengirim alamat IP tersebut ke *browser*. Pada saat mengakses dengan mengetikan alamat website, Windows XP akan mencari data pada *DNS cache* untuk melihat apakah terdapat informasi DNS. Jika terdapat informasi tersebut maka Windows XP tidak akan mengirimkan request data ke DNS tujuan untuk mendapatkan alamat IP-nya. Alamat website dapat diakses lewat *DNS cache* ini. *Data cache* tersebut dibuat berdasarkan informasi yang terdapat dalam *file host*.

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to computernames
# (NetBIOS) names.  Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# This file is compatible with Microsoft LAN Manager 2.x TCP/IP lmhosts
# files and offers the following extensions:
#
#       #PRE
#       #DOM:<domain>
#       #INCLUDE <filename>
#       #BEGIN_ALTERNATE
#       #END_ALTERNATE
#       \0xnn (non-printing character support)
#
# Following any entry in the file with the characters "#PRE" will cause
# the entry to be preloaded into the name cache. By default, entries are
# not preloaded, but are parsed only after dynamic name resolution fails.
#
# Following an entry with the "#DOM:<domain>" tag will associate the
# entry with the domain specified by <domain>. This affects how the
# browser and logon services behave in TCP/IP environments. To preload
# the host name associated with #DOM entry, it is necessary to also add a
# #PRE to the line. The <domain> is always preloaded although it will not
# be shown when the name cache is viewed.
#
# Specifying "#INCLUDE <filename>" will force the RPC NetBIOS (NBT)
# software to seek the specified <filename> and parse it as if it were
# local. <filename> is generally a UNC-based name, allowing a
# centralized lmhosts file to be maintained on a server.
# It is ALWAYS necessary to provide a mapping for the IP address of the
# server prior to the #INCLUDE. This mapping must use the #PRE directive.
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97     rhino         #PRE #DOM:networking  #net group's DC
# 102.54.94.102    "appname  \0x14"                     #special app server
# 102.54.94.123    popular            #PRE              #source server
# 102.54.94.117    localsrv           #PRE              #needed for the include

# 192.168.1.254   www.situsbanyak.com
```

Gambar 14 Isi File Host

KESIMPULAN

Dalam pemanfaaran Internet, pemakai akan disodorkan dua alternatif yang masing-masing dapat menimbulkan dampak positif maupun negatif. Pengguna tidak bisa menginginkan manfaat positifnya saja. Dalam pemakaian internet kadang tidak disengaja mendapatkan informasi yang bersifat negatif.

Menutup situs yang negatif bukanlah solusi yang jitu untuk memberantas sisi negatif internet, bentuk himbuanpun tidak bisa menjadi solusi. Alternatif yang dapat diimplemntasikan adalah secara rutin memantau website yang termasuk dilarang. Berbagai cara dan metode dapat dilakukan untuk memblokir situs terlarang, baik dengan memblokir nama domain maupun dengan memfilter kata kunci.

DAFTAR PUSTAKA

Aji, R.K., Hartanto, A., Siswano, D., Wiratama, T.C., 2002, Kejahatan Internet Trik Aplikasi dan Tip Penanggulangannya, PT Elex Media Komputindo, Jakarta.

Sadono, B., 2003, Tinjauan tentang Buffer Overflow dan Denial of Service Attack, Megister Teknik Elektro, Bidang Khusus Teknologi Informasi, Program Pasca Sarjana, Institut Teknologi Bandung, Bandung.

.....,Blok Situs dengan OpenDNS , http://hudata.imagistudio.com/, Januari 2009

....., Blok Situs dan Keyword dengan ACL,http://slackerbox.com, Januari 2009

……., How to Block a Website in Internet Explorer 7, http://www.wikihow.com, Januari 2009

……..,Block Website Software, http://www.filesland.com/software/block-website.html, Januari 2009

www.detik.com, diakses November 2009