

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
23 August 2007 (23.08.2007)

PCT

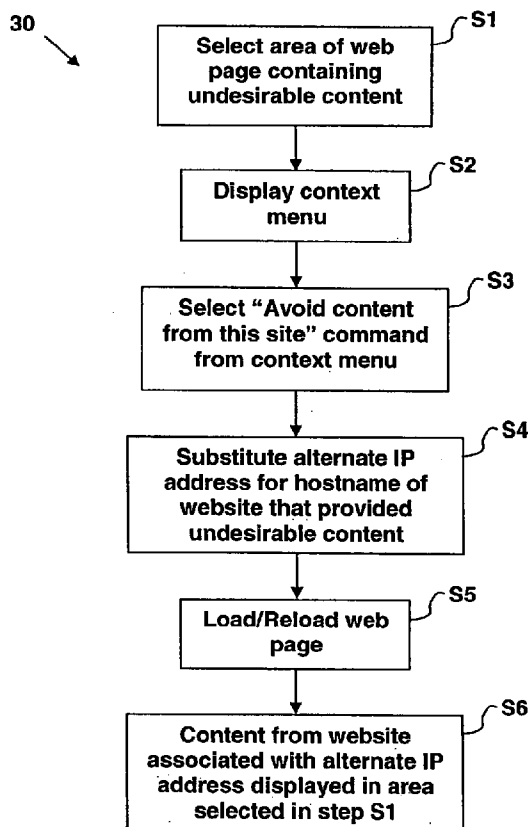
(10) International Publication Number  
**WO 2007/093550 A1**

- (51) International Patent Classification:  
*G06F 21/00* (2006.01)
- (21) International Application Number:  
PCT/EP2007/051208
- (22) International Filing Date: 8 February 2007 (08.02.2007)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
11/352,665 13 February 2006 (13.02.2006) US
- (71) Applicant (for all designated States except US): INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).
- (71) Applicant (for MG only): IBM UNITED KINGDOM LIMITED [GB/GB]; Po Box 41, Portsmouth Hampshire PO6 3AU (GB).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): DANIELS, Fonda [US/US]; 104 Brush Stream Drive, Cary, NC 27511 (US).

- GUIDO, Patrick [US/US]; 514 Windstream Way, Cary, NC 27511 (US). GYURE, Wesley Jerome [US/US]; 9320 Dansforeshire Way, Wake Forest, NC 27587 (US). HAYES JR, Kent Fillmore [US/US]; 9309 Bracken Lane, Chapel Hill, NC 27516 (US). LEAH, Robert, Charles [US/US]; 102 High Slope Drive, Cary, NC 27511 (US). MCMAHAN, Paul, Franklin [US/US]; 2122 Frissell Avenue, Apex, NC 27502 (US).
- (74) Agent: ROBERTS, Scott; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester Hampshire SO21 2JN (GB).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) Title: PREVENTING A WEB BROWSER FROM LOADING CONTENT FROM UNDESIRABLE SOURCES



(57) Abstract: The present invention provides a method, system, and computer program product for preventing a browser from loading content from undesirable sources. A method in accordance with an embodiment of the present invention includes: selecting an area of a web page containing undesirable content; substituting an alternate Internet Protocol (IP) address for a hostname of a website that provided the undesirable content based on a profile; and redisplaying the web page with content from the alternate IP address displayed in the selected area of the web page.

WO 2007/093550 A1



(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

**Published:**

— with international search report

**PREVENTING A WEB BROWSER FROM LOADING CONTENT FROM  
UNDESIRABLE SOURCES**

**Field of the Invention**

5

The present invention generally relates to the Internet, and more specifically relates to a method, system, and computer program product for preventing a web browser from loading content from undesirable sources.

10

**Background of the Invention**

15

Web pages often include banner advertisements and popup windows that originate from third party sources (e.g., ad servers). For the most part, such banner advertisements and popup windows are well behaved and do not significantly intrude on an end user's experience. However at other times (and this is becoming much more common) banner advertisements and popup windows can be very distracting and annoying to a user and can contain undesirable content. Flashy multimedia in banner advertisements and popup windows can consume significant bandwidth and can even infect a user's computer with unwanted software. Such unwanted software can include, for example, software that covertly gathers user information through a user's Internet connection without his or her knowledge, usually for advertising purposes (e.g., spyware), software (often malicious) that installs itself surreptitiously on a user's computer (e.g., a Trojan horse), or software that causes a popup window to spawn one or more subsequent popup windows when closed by a user. Banner advertisements and popup windows can also contain undesirable content (e.g., pornography) that is offensive to some users.

20

25

30

35

40

An illustrative web page 10 assembled by a web browser using content retrieved from a plurality of different sources is depicted in FIG. 1. One or more sections of the web page 10 are used to display information that is not necessarily relevant to the main content 12 of the web page 10. In this example, the information is provided in the form of banner advertisements 14, 16 and a popup window 18, which have been delineated from the main content 12 using dotted lines for illustrative purposes only. The information displayed in the banner advertisements 14, 16 and the popup window 18 is retrieved by the web browser rendering the web page 10 from one or more web servers 20. The typically "undesired" content 24 for the banner advertisements 14, 16 and the popup window 18 is obtained by the web browser by pointing to a respective website (e.g., adsitel.com,

adsite2.com, adsite3.com) on a respective web server 20 using a hostname  
(via a domain name service (DNS) or hosts file) or an Internet Protocol  
(IP) address 26. The "desired" main content 12 of the web page 10 is  
obtained in a similar manner from one or more websites (e.g.,  
5 contentsite(s).com) on one or more web servers 20.

Since the undesirable content in a web page usually comes from third  
party sources, the website hosting the web page is often oblivious to the  
problems experienced by an end user that are associated with banner  
10 advertisements and popup windows. Accordingly, there is a need for a way  
for a user to selectively block out content from undesirable third party  
sources while still retaining desirable content in place on a web page.

#### **SUMMARY OF THE INVENTION**

15 Provided is a method, system, and computer program product for  
preventing a web browser from loading content from undesirable sources.

A first aspect of the present invention is directed to a method for  
20 preventing a web browser from loading content from an undesirable source,  
comprising:

selecting an area of a web page containing undesirable content;  
substituting an alternate Internet Protocol (IP) address for a  
hostname of a website that provided the undesirable content based on a  
25 profile;

and redisplaying the web page with content from the alternate IP  
address displayed in the selected area of the web page.

A second aspect of the present invention is directed to a system for  
30 preventing a web browser from loading content from an undesirable source,  
comprising:

a system for selecting an area of a web page containing undesirable  
content;

a system for substituting an alternate Internet Protocol (IP)  
35 address for a hostname of a website that provided the undesirable content  
based on a profile;

and a system for displaying the web page with content from the  
alternate IP address displayed in the selected area of the web page.

40 A third aspect of the present invention is directed to a program  
product stored on a computer readable medium for preventing a web browser

from loading content from an undesirable source, the computer readable medium comprising program code for performing the steps of:

selecting an area of a web page containing undesirable content;  
substituting an alternate Internet Protocol (IP) address for a  
5 hostname of a website that provided the undesirable content based on a profile;

and redisplaying the web page with content from the alternate IP address displayed in the selected area of the web page.

10 A fourth aspect of the present invention is directed to a method for deploying an application for preventing a web browser from loading content from an undesirable source, comprising:

providing a computer infrastructure being operable to:  
select an area of a web page containing undesirable content;  
15 substitute an alternate Internet Protocol (IP) address for a hostname of a website that provided the undesirable content based on a profile;

and redisplay the web page with content from the alternate IP address displayed in the selected area of the web page.

20 A fifth aspect of the present invention is directed to computer software embodied in a propagated signal for preventing a web browser from loading content from an undesirable source, the computer software comprising program code for causing a computer system to perform the following steps:

selecting an area of a web page containing undesirable content;  
substituting an alternate Internet Protocol (IP) address for a  
hostname of a website that provided the undesirable content based on a  
profile;

30 and redisplaying the web page with content from the alternate IP address displayed in the selected area of the web page.

The illustrative aspects of the present invention are designed to solve the problems herein described and other problems not discussed.

#### 35 BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present invention are described by way of example only with reference to the following drawings in which:

40 FIG. 1 depicts an illustrative web page including banner advertisements and a popup window;

FIG. 2 depicts an illustrative flow diagram of a method in accordance with an embodiment of the present invention;

FIGS. 3-5 depict an illustrative operational example in accordance with an embodiment of the present invention; and

FIG. 6 depicts an illustrative computer system for implementing embodiment(s) of the present invention.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Provided is a method, system, and computer program product for preventing a web browser from loading content from undesirable sources.

A flow diagram 30 of a method in accordance with an embodiment of the present invention is depicted in FIG. 2. In step S1, a user selects an area (e.g., banner advertisement, popup window, etc.) of a web page containing undesirable content. As shown in FIG. 3, for example, the user has selected the banner advertisement 14 on the web page 10 by positioning a mouse pointer 32 over the banner advertisement 14 and actuating (e.g., right-clicking) a designated button on the mouse. Other selection methodologies are also possible. In response, a context menu 34 is displayed in step S2. A context menu 34 may also be displayed, for example, in response to an actuation of a function key, keyboard shortcut, etc. In step S3, the user selects the "Avoid content from this site" command 36 from the context menu 34.

In step S4, in response to the user selection of the "Avoid content from this site" command 36 from the context menu 34, an embodiment of the present invention substitutes an alternate IP address for the hostname of the website that provided the undesirable content. For instance, as shown in FIG. 4, a browser module/plug-in 38 substitutes in a local DNS server 42 (or hosts file) an alternate IP address 40 (e.g., xxx.xxx.x.x) for the hostname (e.g., adsitel.com) of the website that provided the undesirable content. The substitution is based on a profile 44. In this example, the alternate IP address 40 points to a website (e.g., desirable-contentsite.com) that provides more desirable content for display in the banner advertisement 14. One or more profiles 44 can be associated with each user and selectively accessed.

In step S5, the user loads or reloads the web page 10 at a later time. In step S6, content from the website associated with the alternate IP address 40 is displayed in the area selected by the user in step S1.

In the above example, as shown in FIG. 5, when a request for content from the website adsitel.com is received by the local DNS server 42 (or hosts file), the local DNS server 42 (or hosts file) now points to the website (desirable-contentsite.com) corresponding to the alternate IP address (xxx.xxx.x.x) provided by the browser module/plugin 38. As a result, desirable content from the website desirable-contentsite.com, in this example stock quotes, is now displayed in the banner advertisement 14 instead of the undesirable content previously provided by the website adsitel.com.

The profile 44 (FIG. 4) is used to control the content that is loaded in a selected area (e.g., banner advertisement, popup window, etc.) of a web page in place of undesirable content. The profile 44 can be created by a user to drive the behavior of the content loading. Preset profiles 44 are also possible. Virtually any type of profile 44 can be used in the practice of embodiments of the present invention. For example, the profile 44 could be configured by a user 46 via a user interface (UI) 48 (FIG. to:

- Display content (e.g., images, graphics, text, content from a portlet, etc.) from one or more selected websites in place of undesirable content.

- Display content pertaining to one or more types of selected subject matter in place of undesirable content.

- Display content (advertisements, product information, etc.) from the website of one or more selected entities (e.g., company, organization, retailer, etc.) in place of undesirable content.

- Replace undesirable content in popup windows, but not banner advertisements, or vice versa.

- Replace undesirable content originating from specific websites with more desirable content.

- Replace undesirable content associated with a specific entity (e.g., company, organization, retailer, etc.) or containing a specific type of subject matter (e.g., pornography) with other more desirable content.

- When used within a corporate intranet or within a service provider's domain, replace undesirable content with more desirable content for the entire set of users for which service is provided.

A computer system 100 for preventing a web browser from loading content from undesirable sources in accordance with an embodiment of the present invention is depicted in FIG. 6. Computer system 100 is provided

in a computer infrastructure 102. Computer system 100 is intended to represent any type of computer system suitable for use with embodiments of the present invention. For example, computer system 100 can be a laptop computer, a desktop computer, a workstation, a handheld device, a server, a cluster of computers, etc. In addition, as will be further described below, computer system 100 can be deployed and/or operated by a service provider that provides a service for preventing a web browser from loading content from undesirable sources in accordance with embodiments of the present invention. It should be appreciated that a user 46 can access computer system 100 directly, or can operate a computer system that communicates with computer system 100 over a network 106 (e.g., the Internet, a wide area network (WAN), a local area network (LAN), a virtual private network (VPN), etc). In the case of the latter, communications between computer system 100 and a user-operated computer system can occur via any combination of various types of communications links. For example, the communication links can comprise addressable connections that can utilize any combination of wired and/or wireless transmission methods. Where communications occur via the Internet, connectivity can be provided by conventional TCP/IP sockets-based protocol, and an Internet service provider can be used to establish connectivity to the Internet.

Computer system 100 is shown including a processing unit 108, a memory 110, a bus 112, and input/output (I/O) interfaces 114. Further, computer system 100 is shown in communication with external devices/resources 116 and one or more storage units 118. In general, processing unit 108 executes computer program code, such as content control system 130, that is stored in memory 110 and/or storage units(s) 118. While executing computer program code, processing unit 108 can read and/or write data, to/from memory 110, storage unit(s) 118, and/or I/O interfaces 114. Bus 112 provides a communication link between each of the components in computer system 100. External devices/resources 116 can comprise any devices (e.g., keyboard, pointing device, display (e.g., display 120, printer, etc.) that enable a user to interact with computer system 100 and/or any devices (e.g., network card, modem, etc.) that enable computer system 100 to communicate with one or more other computing devices.

Computer infrastructure 102 is only illustrative of various types of computer infrastructures that can be used to implement embodiments of the present invention. For example, in one embodiment, computer infrastructure 102 can comprise two or more computing devices (e.g., a server cluster)



that communicate over a network (e.g., network 106) to perform the various process steps of a preferred embodiment of the present invention.

Moreover, computer system 100 is only representative of the many types of computer systems that can be used in the practice of embodiments of the present invention, each of which can include numerous combinations of hardware/software. For example, processing unit 108 can comprise a single processing unit, or can be distributed across one or more processing units in one or more locations, e.g., on a client and server. Similarly, memory 110 and/or storage unit(s) 118 can comprise any combination of various types of data storage and/or transmission media that reside at one or more physical locations. Further, I/O interfaces 114 can comprise any system for exchanging information with one or more external devices/resources 116. Still further, it is understood that one or more additional components (e.g., system software, communication systems, cache memory, etc.) not shown in FIG. 6 can be included in computer system 100.

However, if computer system 100 comprises a handheld device or the like, it is understood that one or more external devices/resources 116 (e.g., a display) and/or one or more storage unit(s) 118 can be contained within computer system 100, and not externally as shown.

Storage unit(s) 118 can be any type of system (e.g., a database) capable of providing storage for information in embodiments of the present invention. To this extent, storage unit(s) 118 can include one or more storage devices, such as a magnetic disk drive or an optical disk drive. In another embodiment, storage unit(s) 118 can include data distributed across, for example, a local area network (LAN), wide area network (WAN) or a storage area network (SAN) (not shown). Moreover, although not shown, computer systems operated by user 46 can contain computerized components similar to those described above with regard to computer system 100.

Shown in memory 110 (e.g., as a computer program product) is a content control system 130 for preventing a web browser 132 from loading content from undesirable sources in accordance with embodiment(s) of the present invention. The content control system 130 includes a selection system 134 for selecting (by the user) an area of a web page 10 containing undesirable content. In response to the selection of an area of the web page 10 containing undesirable content, a context menu 34 (FIG. 3) is displayed that includes a command such as "Avoid content from this site." Upon selection of this command, a browser module/plug-in 38 substitutes in a local DNS server 42 (or hosts file) an alternate IP address for the

hostname of the website that provided the undesirable content. The provision of the alternate IP address is based on profile information provided in a profile 44. When the web page 10 is subsequently loaded/reloaded, content from the website associated with the alternate IP address is displayed in the selected area of the web page 10, as described above.

Embodiments of the present invention can be offered as a business method on a subscription or fee basis. For example, one or more components can be created, maintained, supported, and/or deployed by a service provider that offers the functions described herein for customers. That is, a service provider can be used to provide a service for preventing a web browser from loading content from undesirable sources, as described above.

It should also be understood that embodiments of the present invention can be realized in hardware, software, a propagated signal, or any combination thereof. Any kind of computer/server system(s) - or other apparatus adapted for carrying out the methods described herein - is suitable. A typical combination of hardware and software can include a general purpose computer system with a computer program that, when loaded and executed, carries out the respective methods described herein. Alternatively, a specific use computer, containing specialized hardware for carrying out one or more of the functional tasks of embodiments of the invention, can be utilized. Embodiments of the present invention can also be embedded in a computer program product or a propagated signal, which comprises all the respective features enabling the implementation of the methods described herein, and which - when loaded in a computer system - is able to carry out these methods.

Embodiments of the present invention can take an entirely hardware form, an entirely software form, or an embodiment containing both hardware and software elements.

Embodiments of the present invention can take the form of a computer program product accessible from a computer-usable or computer-readable medium providing program code for use by or in connection with a computer or any instruction execution system. For the purposes of this description, a computer-usable or computer-readable medium can be any apparatus that can contain, store, communicate, propagate, or transport

the program for use by or in connection with the instruction execution system, apparatus, or device.

5 The medium can be an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device), or a propagation medium. Examples of a computer-readable medium include a semiconductor or solid state memory, magnetic tape, removable computer  
10 diskette, random access memory (RAM), read-only memory (ROM), rigid magnetic disk and optical disk. Current examples of optical disks include a compact disk - read only disk (CD-ROM), a compact disk - read/write disk (CD-R/W), and a digital versatile disk (DVD).

15 Computer program, propagated signal, software program, program, or software, in the present context mean any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following:

- (a) conversion to another language, code or notation; and/or
- (b) reproduction in a different material form.

20 The foregoing description of the preferred embodiments of this invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed, and obviously, many modifications and variations  
25 are possible.

**CLAIMS**

- 5 1. A method for preventing a web browser from loading content from an undesirable source, comprising:  
selecting an area of a web page containing undesirable content;  
substituting an alternate Internet Protocol (IP) address for a  
hostname of a website that provided the undesirable content based on a  
profile; and  
10 redisplaying the web page with content from the alternate IP address displayed in the selected area of the web page.
- 15 2. The method of claim 1, wherein the area of the web page is selected from the group consisting of a banner and a popup window.
- 20 3. The method of claim 1, wherein selecting the area of the web page further comprises:  
displaying a context menu; and  
selecting a command from the context window for avoiding content  
from the website that provided the undesirable content.
- 25 4. The method of claim 1, wherein substituting the alternate IP address further comprises:  
providing the alternate IP address to a domain name service (DNS).
- 30 5. The method of claim 1, wherein substituting the alternate IP address further comprises:  
providing the alternate IP address to a hosts file.
- 35 6. The method of claim 1, wherein the profile causes content from a selected website to be displayed in place of the undesirable content.
7. The method of claim 1, wherein the profile causes content pertaining to a particular subject matter to be displayed in place of the undesirable  
content.
- 40 8. The method of claim 1, wherein the profile causes content from a website of a selected entity to be displayed in place of the undesirable content.

9. The method of claim 1, wherein the profile causes undesirable content originating from a specific website to be replaced with the content from the alternate IP address.

5 10. The method of claim 1, wherein the profile causes undesirable content associated with a specific entity to be replaced with the content from the alternate IP address.

10 11. A system for preventing a web browser from loading content from an undesirable source, comprising:

a system for selecting an area of a web page containing undesirable content;

15 a system for substituting an alternate Internet Protocol (IP) address for a hostname of a website that provided the undesirable content based on a profile; and

a system for displaying the web page with content from the alternate IP address displayed in the selected area of the web page.

20 12. The system of claim 11, wherein the area of the web page is selected from the group consisting of a banner and a popup window.

13. The system of claim 11, wherein the system for selecting the area of the web page further comprises:

25 a system for displaying a context menu; and

a system for selecting a command from the context window for avoiding content from the website that provided the undesirable content.

14. The system of claim 11, wherein the system for substituting the alternate IP address further comprises:

30 a system for providing the alternate IP address to a domain name service (DNS).

15. The system of claim 11, wherein the system for substituting the alternate IP address further comprises:

35 a system for providing the alternate IP address to a hosts file.

16. The system of claim 11, wherein the profile causes content from a selected website to be displayed in place of the undesirable content.

17. The system of claim 11, wherein the profile causes content pertaining to a particular subject matter to be displayed in place of the undesirable content.

5 18. The system of claim 11, wherein the profile causes content from a website of a selected entity to be displayed in place of the undesirable content.

10 19. The system of claim 11, wherein the profile causes undesirable content originating from a specific website to be replaced with the content from the alternate IP address.

15 20. The system of claim 11, wherein the profile causes undesirable content associated with a specific entity to be replaced with the content from the alternate IP address.

20 21. A program product stored on a computer readable medium for preventing a web browser from loading content from an undesirable source, the computer readable medium comprising program code for performing the steps of:

selecting an area of a web page containing undesirable content;  
substituting an alternate Internet Protocol (IP) address for a hostname of a website that provided the undesirable content based on a profile; and

25       redisplaying the web page with content from the alternate IP address displayed in the selected area of the web page.

22. A method for deploying an application for preventing a web browser from loading content from an undesirable source, comprising:

30       providing a computer infrastructure being operable to:  
select an area of a web page containing undesirable content;  
substitute an alternate Internet Protocol (IP) address for a hostname of a website that provided the undesirable content based on a profile; and

35       redisplay the web page with content from the alternate IP address displayed in the selected area of the web page.

10

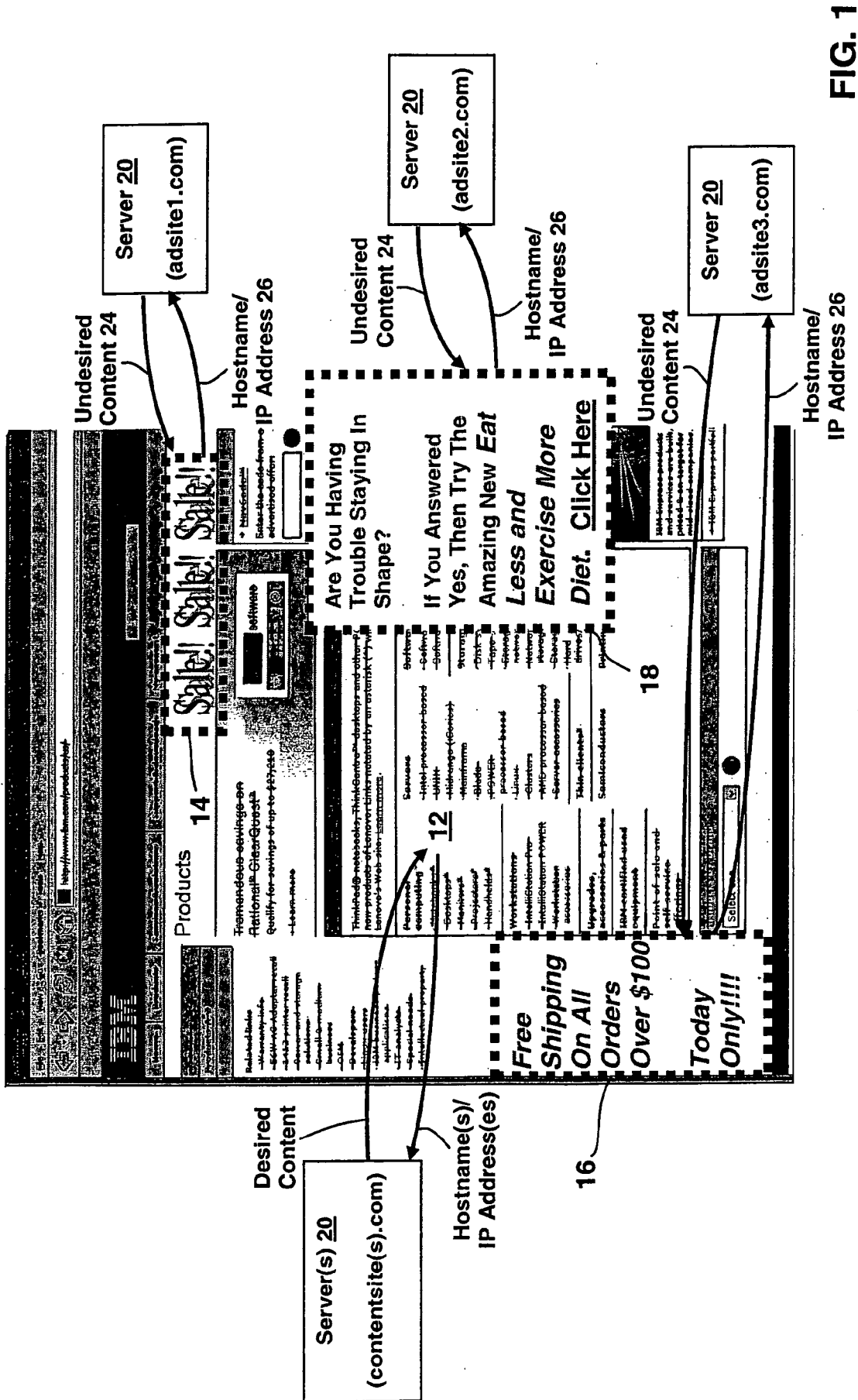


FIG. 1

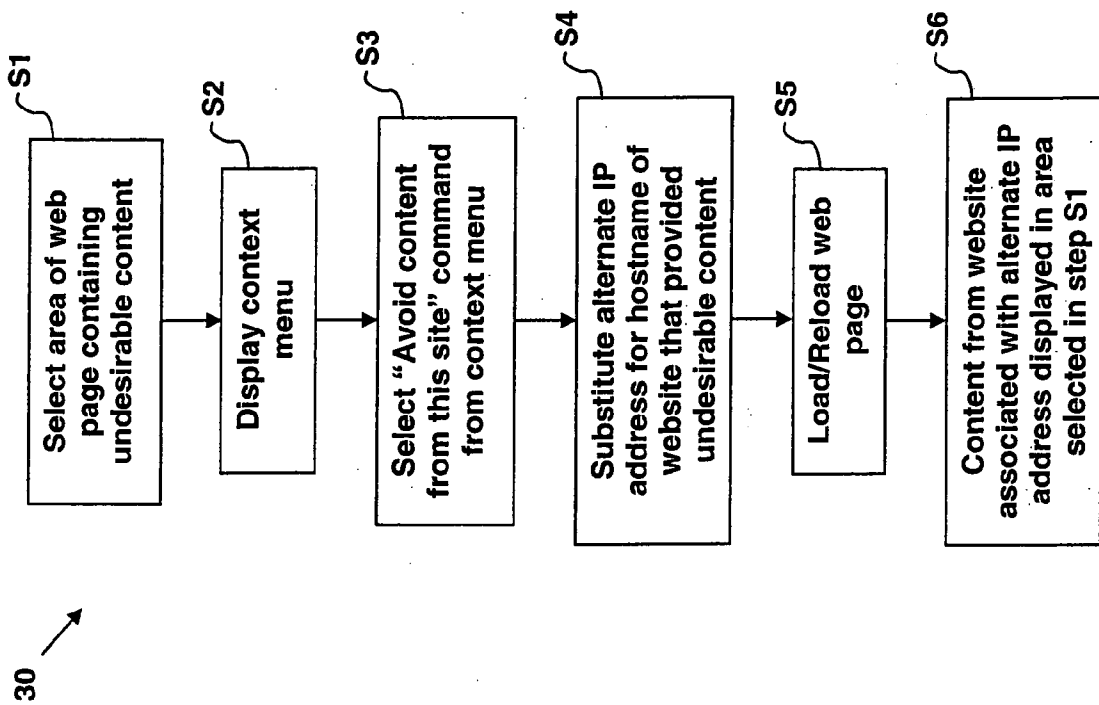


FIG. 2



10 ↗

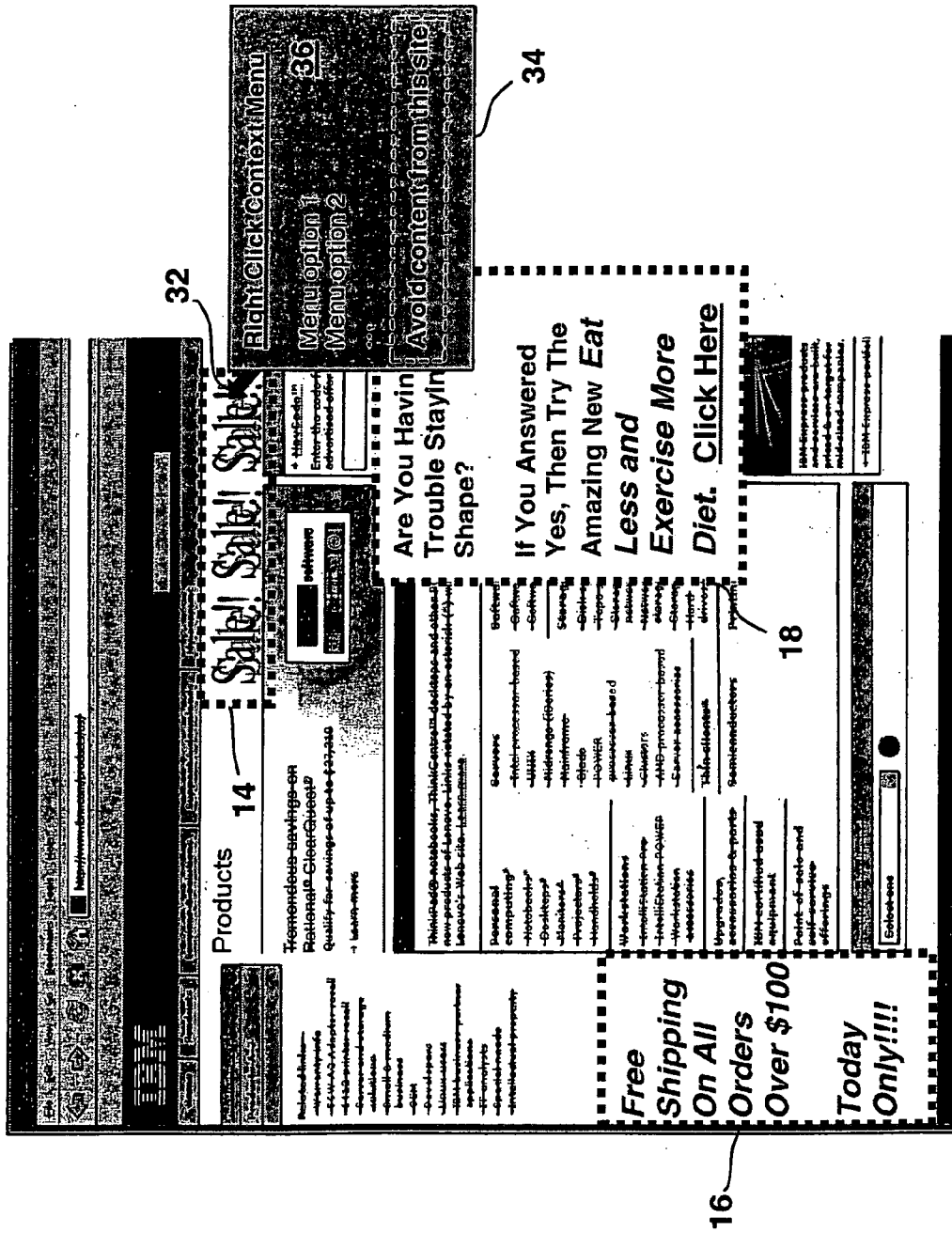


FIG. 3

10

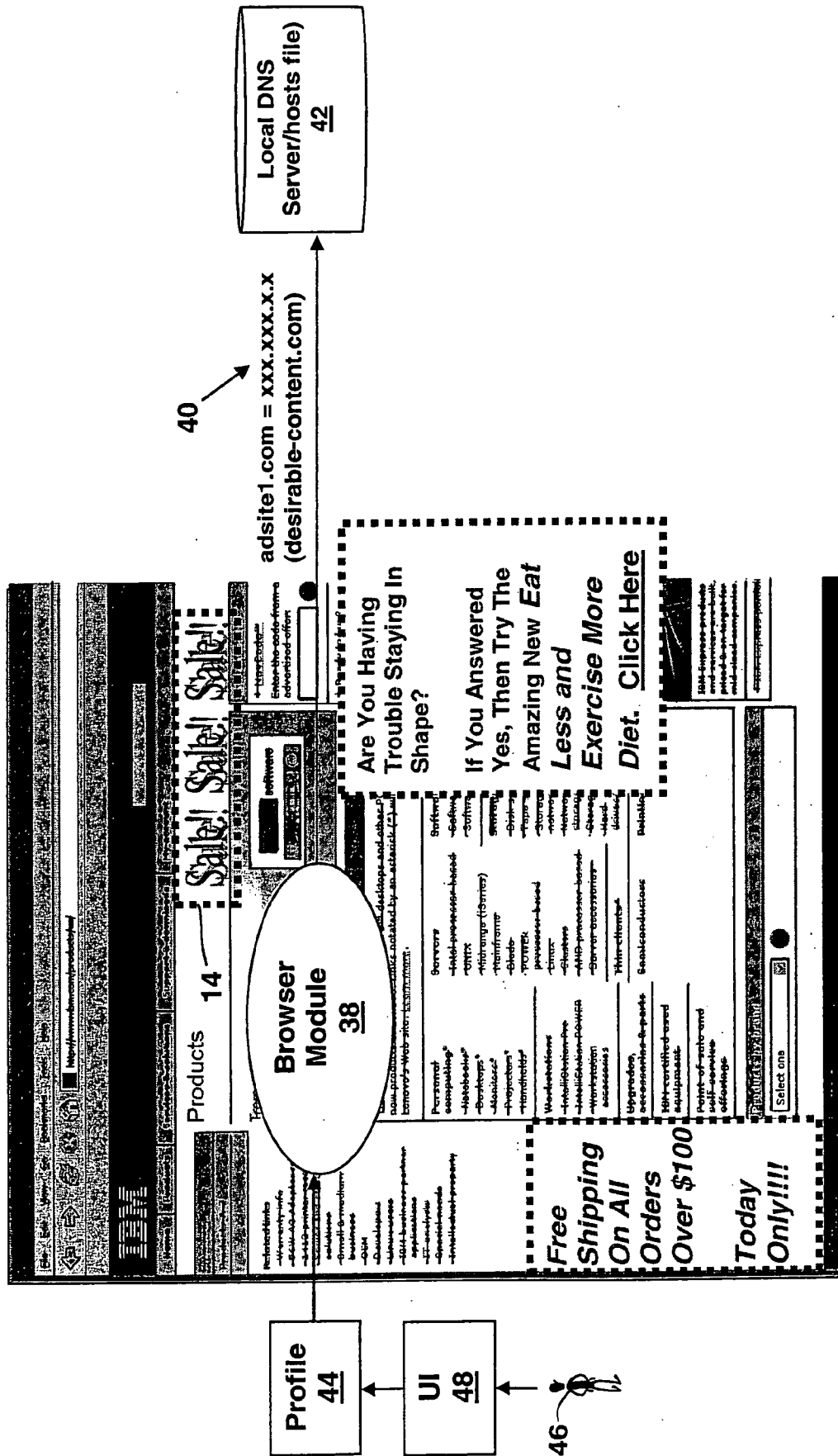


FIG. 4

10 ↗

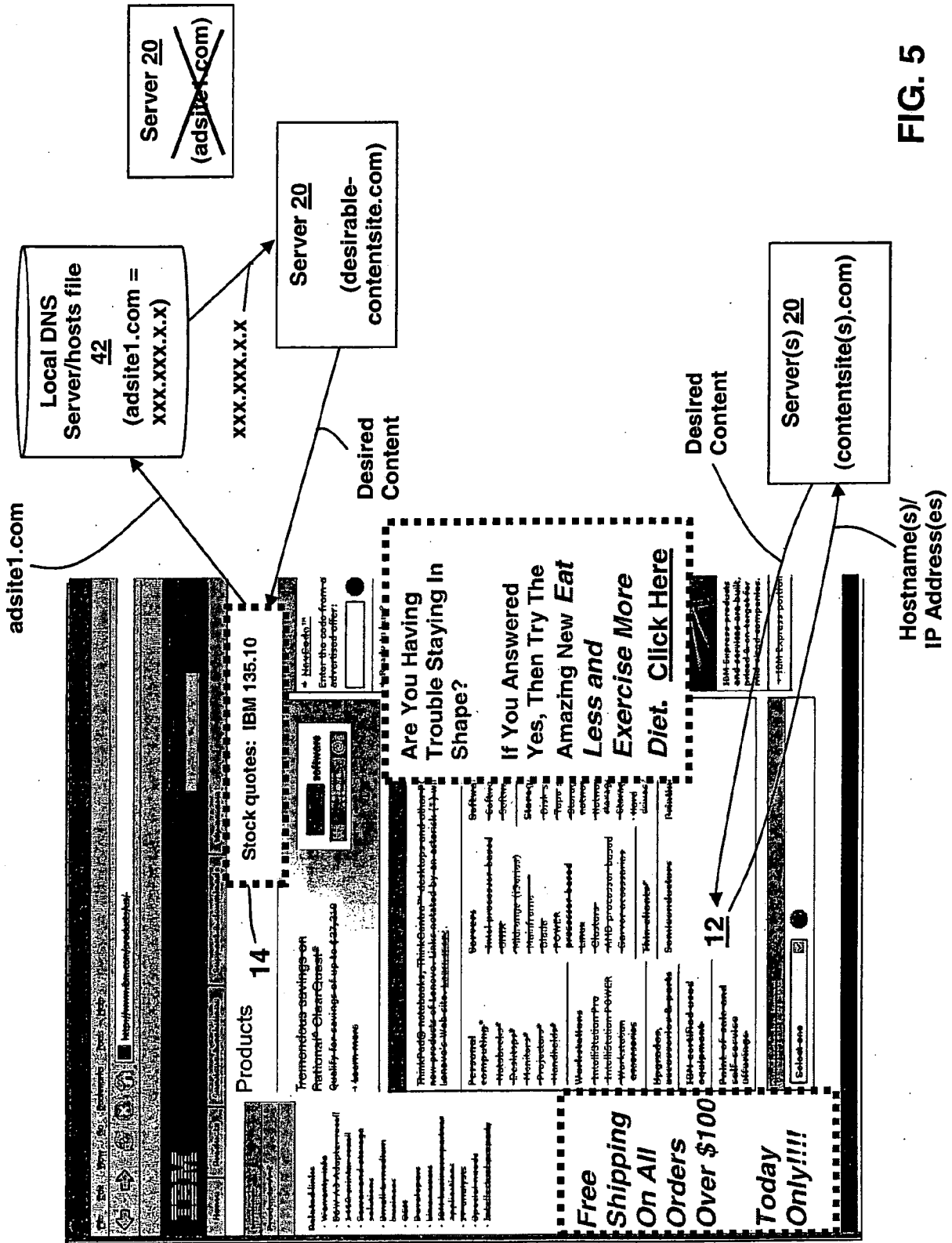


FIG. 5

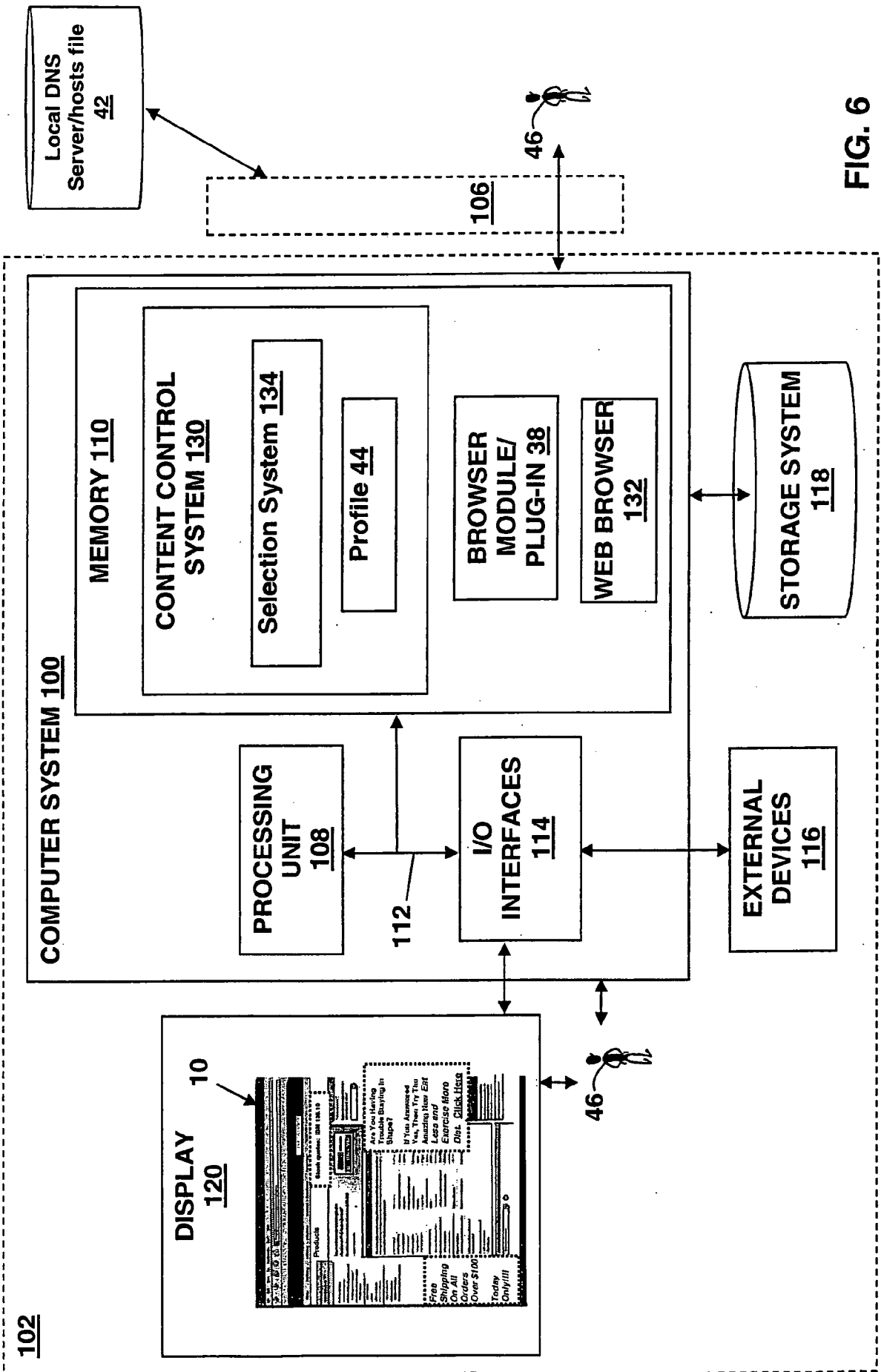


FIG. 6

**INTERNATIONAL SEARCH REPORT**

International application No  
PCT/EP2007/051208

**A. CLASSIFICATION OF SUBJECT MATTER**  
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/088570 A1 (ROBERTS GUY WILLIAM WELCH [GB] ET AL) 6 May 2004 (2004-05-06) paragraph [0032] - paragraph [0033] paragraph [0036]	1-22
A	US 6 904 569 B1 (ANDERSON GLEN J [US]) 7 June 2005 (2005-06-07) abstract column 2, line 25 - line 63 column 7, line 23 - column 8, line 31	3,13
A	US 2003/098882 A1 (COWDEN JAX B [US] ET AL) 29 May 2003 (2003-05-29) paragraph [0071] - paragraph [0072]	3,13

Further documents are listed in the continuation of Box C.

See patent family annex.

\* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \* & \* document member of the same patent family

Date of the actual completion of the international search

18 June 2007

Date of mailing of the international search report

29/06/2007

Name and mailing address of the ISA/  
European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Chabot, Pedro

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2007/051208

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004088570	A1	06-05-2004	NONE
US 6904569	B1	07-06-2005	NONE
US 2003098882	A1	29-05-2003	NONE