Web Hacking

KSAJ Inc.

www.PENETRATIONTEST.com

HaX0rz Toolkit

- Complicated ‘sploits that need a Bachelor’s degree to understand and use
- Scripts in various languages and syntaxes like C, PERL, gtk and bash
- Automated scanning tools like nmap and nessus
- A web browser

A Web Browser?

- Web surfing:
  - Is easy to do,
  - Is Operating System independent,
  - Doesn’t require intimate knowledge of “the system”,
  - Provides access to vast amounts of data and information,
  - and topped off with all kinds of data mining tools

Web Features

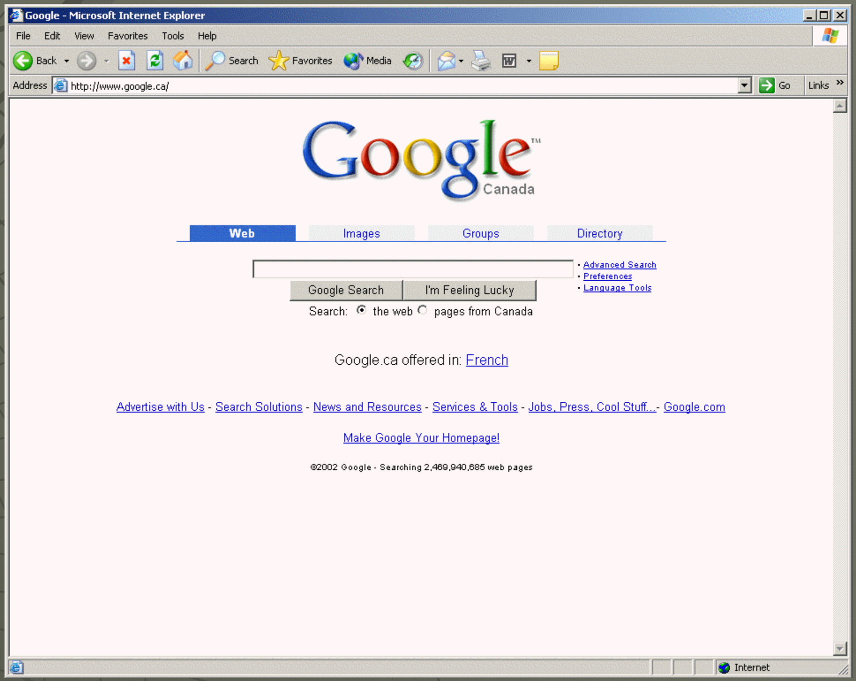
- Reverse phone number searches
- Detailed address topological maps
- Satellite photography of target area
- Resumes
- Phone and Email lists
- Likely targets described in detail
- Exploit information easy to obtain
- Data aggregation makes it more serious

What We’ll Learn

- Methods of Reconnaissance
- The level of sensitive detail companies and organizations leave exposed to the Internet
- The level of detail about specific people on the Internet
- The effect of data aggregation on privacy

Where to start?

- Search Engines are one of the first things people learn to use on the Internet
- Most use highly effective search algorithms to mine the Internet
- Most provide equally advanced search abilities to the user



Address http://www.google.ca/

Search: ● the web ○ pages from Canada

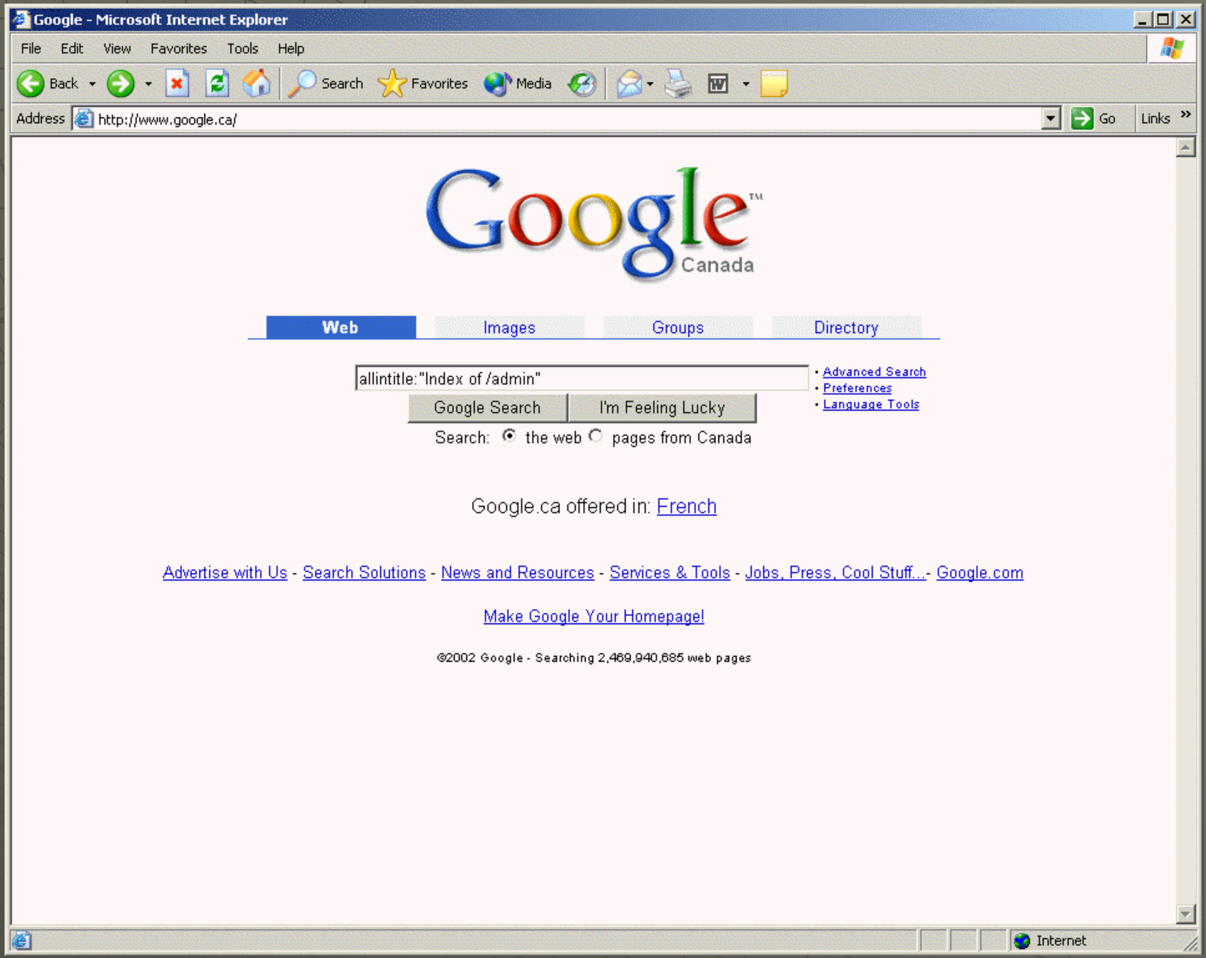
Google.ca offered in: French

Advertise with Us - Search Solutions - News and Resources - Services & Tools - Jobs, Press, Cool Stuff...- Google.com

Make Google Your Homepage!

©2002 Google - Searching 2,469,940,685 web pages

allintitle:”Index of /admin”



Address: http://www.google.ca/

allintitle:"Index of /admin"

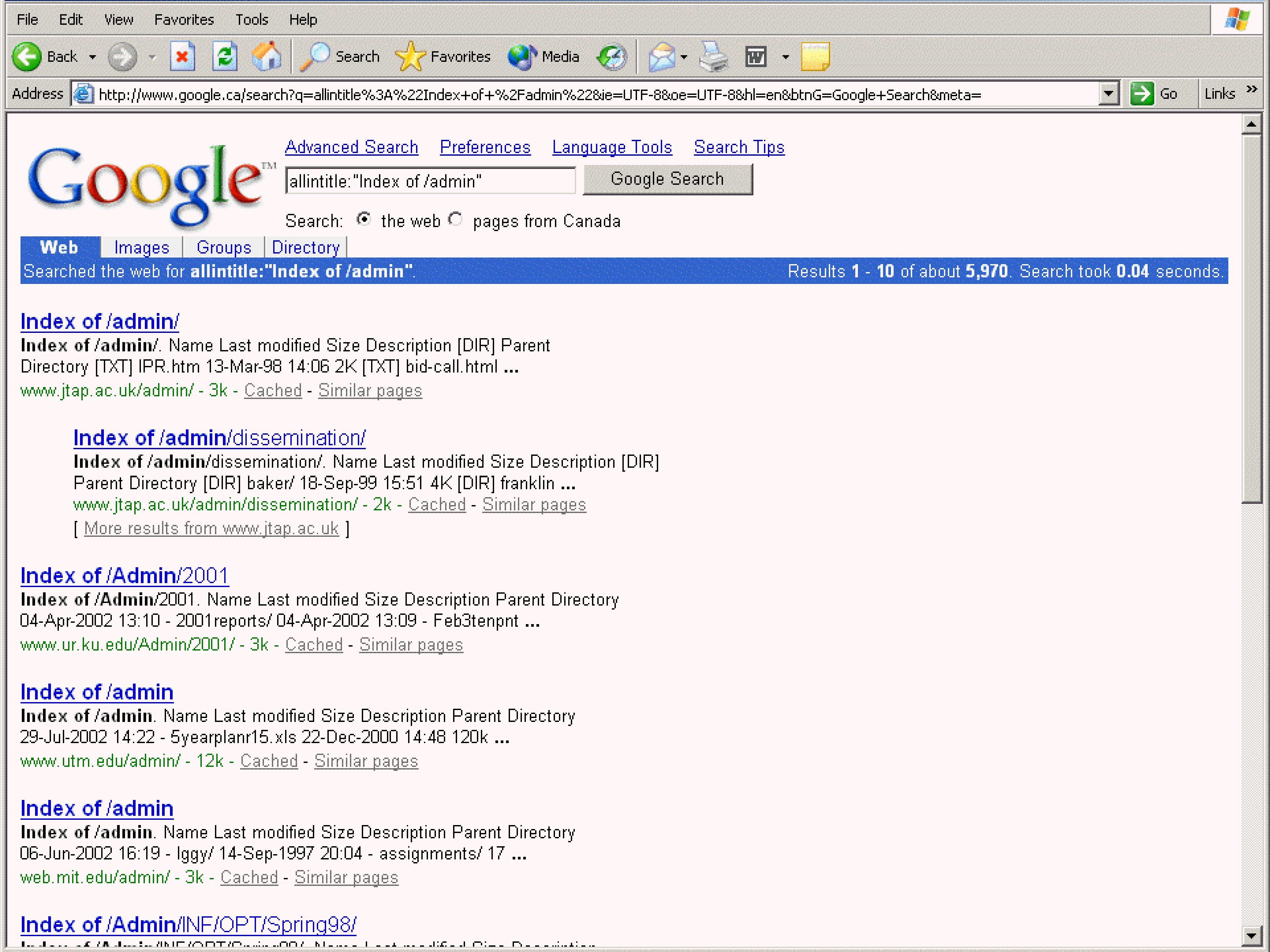
Search: ● the web ○ pages from Canada

Google.ca offered in: French

Advertise with Us - Search Solutions - News and Resources - Services & Tools - Jobs, Press, Cool Stuff...- Google.com

Make Google Your Homepage!

©2002 Google - Searching 2,469,940,685 web pages



http://www.google.ca/search?q=allintitle%3A%22Index+of+%2Fadmin%22&ie=UTF-8&oe=UTF-8&hl=en&btnG=Google+Search&meta=

allintitle:"Index of /admin"

Search: ● the web ○ pages from Canada

Searched the web for **allintitle:"Index of /admin"**. Results **1** - **10** of about **5,970**. Search took **0.04** seconds.

Index of /admin/
Index of /admin/. Name Last modified Size Description [DIR] Parent Directory [TXT] IPR.htm 13-Mar-98 14:06 2K [TXT] bid-call.html **...**
www.jtap.ac.uk/admin/ - 3k - Cached - Similar pages

Index of /admin/dissemination/
Index of /admin/dissemination/. Name Last modified Size Description [DIR] Parent Directory [DIR] baker/ 18-Sep-99 15:51 4K [DIR] franklin **...**
www.jtap.ac.uk/admin/dissemination/ - 2k - Cached - Similar pages
[More results from www.jtap.ac.uk]

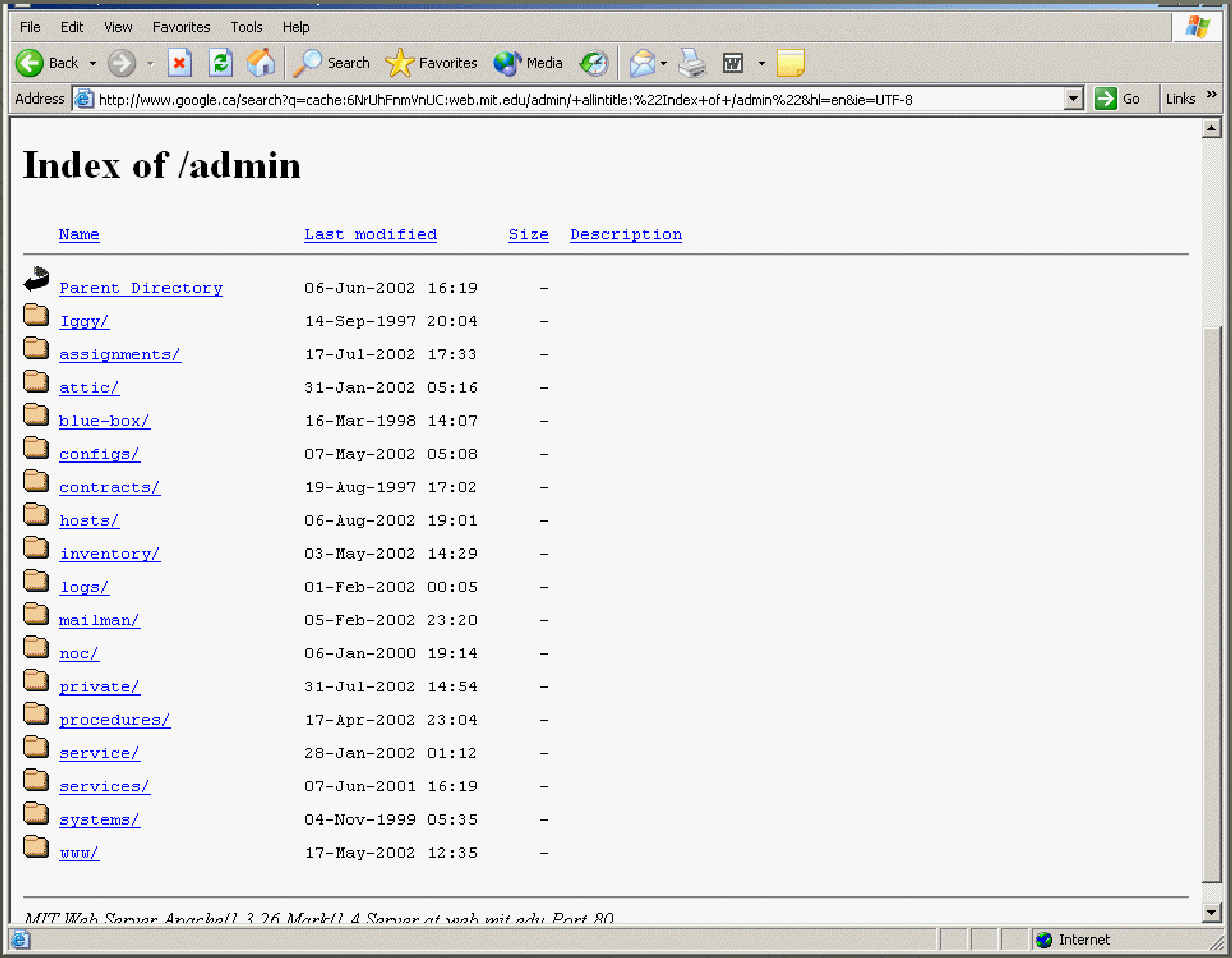
Index of /Admin/2001
Index of /Admin/2001. Name Last modified Size Description Parent Directory 04-Apr-2002 13:10 - 2001reports/ 04-Apr-2002 13:09 - Feb3tenpnt **...**
www.ur.ku.edu/Admin/2001/ - 3k - Cached - Similar pages

Index of /admin
Index of /admin. Name Last modified Size Description Parent Directory 29-Jul-2002 14:22 - 5yearplanr15.xls 22-Dec-2000 14:48 120k **...**
www.utm.edu/admin/ - 12k - Cached - Similar pages

Index of /admin
Index of /admin. Name Last modified Size Description Parent Directory 06-Jun-2002 16:19 - Iggy/ 14-Sep-1997 20:04 - assignments/ 17 **...**
web.mit.edu/admin/ - 3k - Cached - Similar pages

Index of /Admin/INF/OPT/Spring98/

- Here is a Google hit from MIT, pulled from the cache



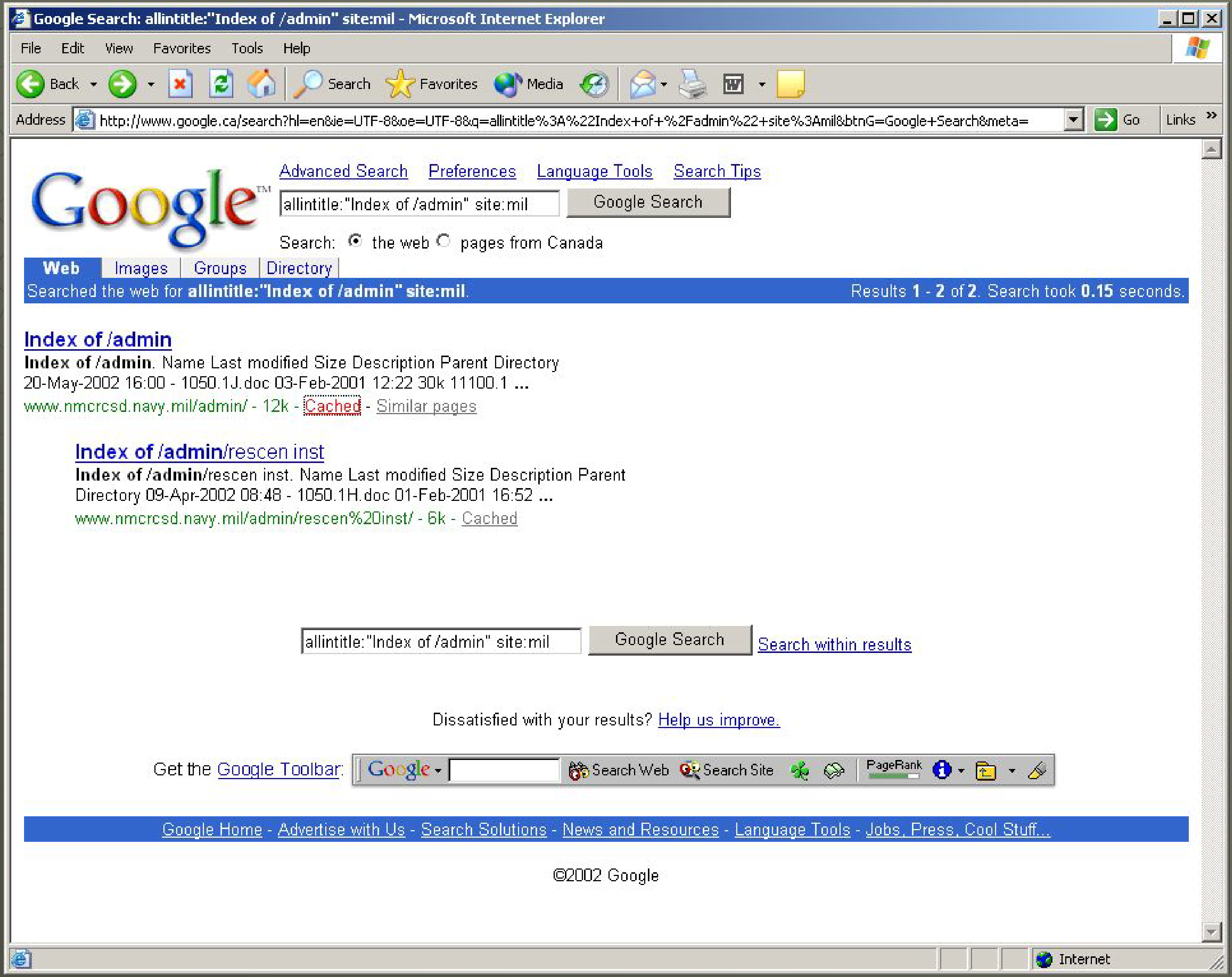
http://www.google.ca/search?q=cache:6NrUhFnmVnUC:web.mit.edu/admin/+allintitle:%22Index+of+/admin%22&hl=en&ie=UTF-8

Index of /admin

```
    Name                    Last modified       Size  Description
---------------------------------------------------------------------
    Parent Directory        06-Jun-2002 16:19      -
    Iggy/                   14-Sep-1997 20:04      -
    assignments/            17-Jul-2002 17:33      -
    attic/                  31-Jan-2002 05:16      -
    blue-box/               16-Mar-1998 14:07      -
    configs/                07-May-2002 05:08      -
    contracts/              19-Aug-1997 17:02      -
    hosts/                  06-Aug-2002 19:01      -
    inventory/              03-May-2002 14:29      -
    logs/                   01-Feb-2002 00:05      -
    mailman/                05-Feb-2002 23:20      -
    noc/                    06-Jan-2000 19:14      -
    private/                31-Jul-2002 14:54      -
    procedures/             17-Apr-2002 23:04      -
    service/                28-Jan-2002 01:12      -
    services/               07-Jun-2001 16:19      -
    systems/                04-Nov-1999 05:35      -
    www/                    17-May-2002 12:35      -
---------------------------------------------------------------------
```

MIT Web Server Apache/1.3.26 Mark/1.4 Server at web.mit.edu Port 80

- allintitle:”Index of /” site:mil



Google Search: allintitle:"Index of /admin" site:mil - Microsoft Internet Explorer

Address http://www.google.ca/search?hl=en&ie=UTF-8&oe=UTF-8&q=allintitle%3A%22Index+of+%2Fadmin%22+site%3Amil&btnG=Google+Search&meta=

Advanced Search Preferences Language Tools Search Tips

allintitle:"Index of /admin" site:mil [Google Search]

Search: ● the web ○ pages from Canada

Web Images Groups Directory

Searched the web for **allintitle:"Index of /admin" site:mil**. Results **1** - **2** of **2**. Search took **0.15** seconds.

Index of /admin
Index of /admin. Name Last modified Size Description Parent Directory 20-May-2002 16:00 - 1050.1J.doc 03-Feb-2001 12:22 30k 11100.1 **...**
www.nmcrcsd.navy.mil/admin/ - 12k - Cached - Similar pages

Index of /admin/rescen inst
Index of /admin/rescen inst. Name Last modified Size Description Parent Directory 09-Apr-2002 08:48 - 1050.1H.doc 01-Feb-2001 16:52 **...**
www.nmcrcsd.navy.mil/admin/rescen%20inst/ - 6k - Cached

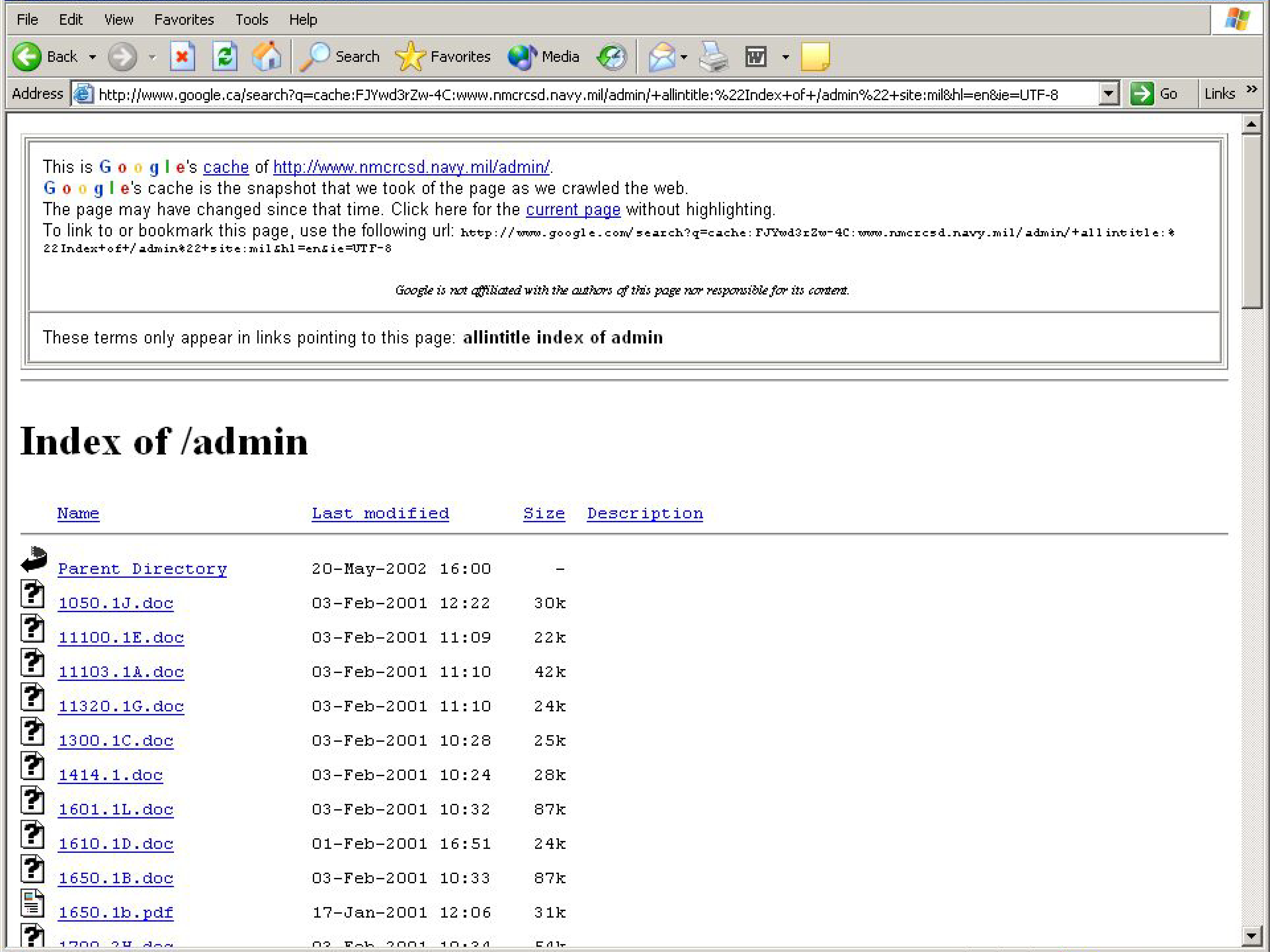
allintitle:"Index of /admin" site:mil [Google Search] Search within results

Dissatisfied with your results? Help us improve.

Get the Google Toolbar:

Google Home - Advertise with Us - Search Solutions - News and Resources - Language Tools - Jobs, Press, Cool Stuff...

©2002 Google



http://www.google.ca/search?q=cache:FJYwd3rZw-4C:www.nmcrcsd.navy.mil/admin/+allintitle:%22Index+of+/admin%22+site:mil&hl=en&ie=UTF-8

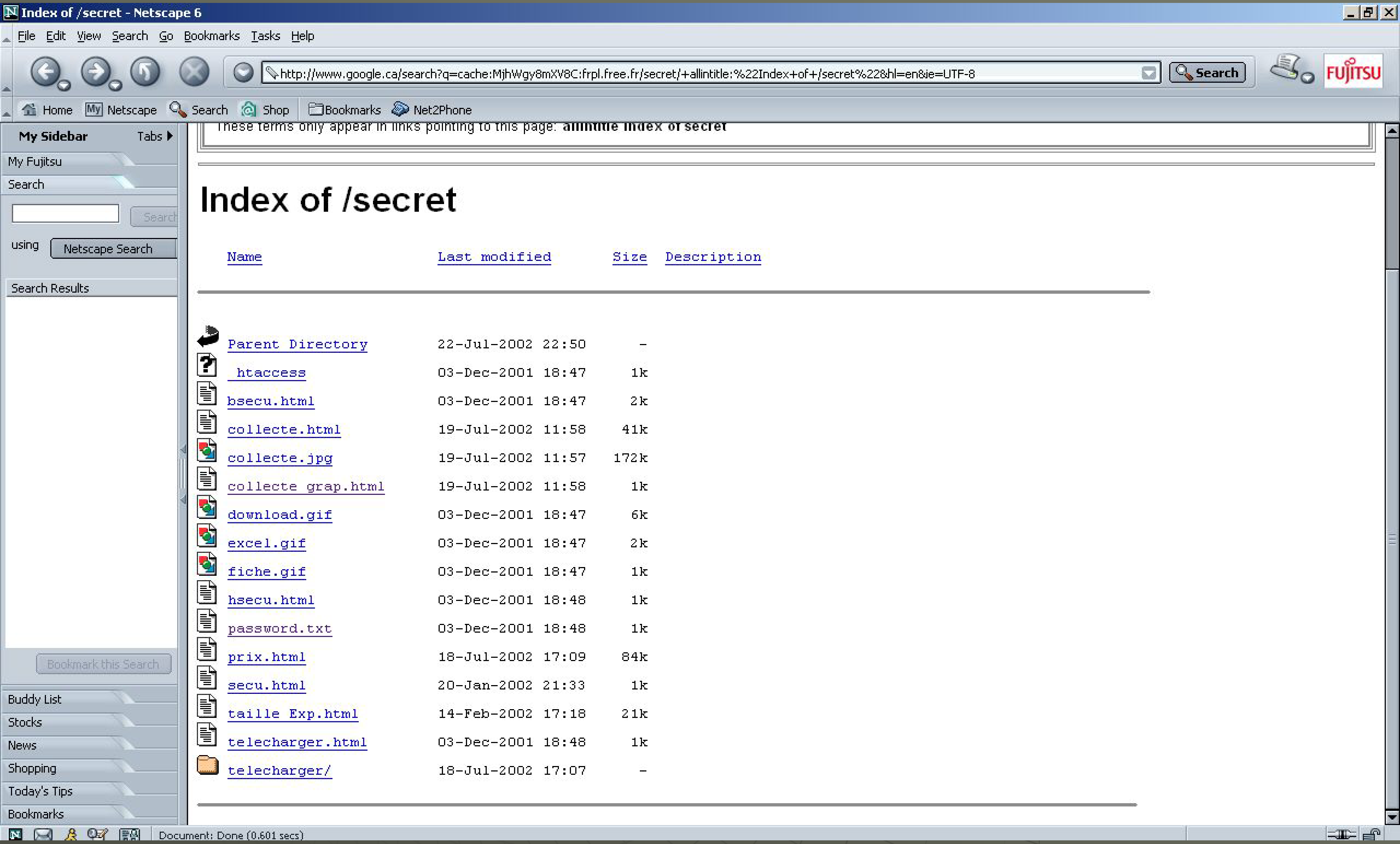
This is Google's cache of http://www.nmcrcsd.navy.mil/admin/.
Google's cache is the snapshot that we took of the page as we crawled the web.
The page may have changed since that time. Click here for the current page without highlighting.
To link to or bookmark this page, use the following url: `http://www.google.com/search?q=cache:FJYwd3rZw-4C:www.nmcrcsd.navy.mil/admin/+allintitle:%22Index+of+/admin%22+site:mil&hl=en&ie=UTF-8`

Google is not affiliated with the authors of this page nor responsible for its content.

These terms only appear in links pointing to this page: **allintitle index of admin**

Index of /admin

```
   Name                    Last modified      Size  Description

   Parent Directory        20-May-2002 16:00     -
   1050.1J.doc             03-Feb-2001 12:22   30k
   11100.1E.doc            03-Feb-2001 11:09   22k
   11103.1A.doc            03-Feb-2001 11:10   42k
   11320.1G.doc            03-Feb-2001 11:10   24k
   1300.1C.doc             03-Feb-2001 10:28   25k
   1414.1.doc              03-Feb-2001 10:24   28k
   1601.1L.doc             03-Feb-2001 10:32   87k
   1610.1D.doc             01-Feb-2001 16:51   24k
   1650.1B.doc             03-Feb-2001 10:33   87k
   1650.1b.pdf             17-Jan-2001 12:06   31k
   1700.2H.doc             03-Feb-2001 10:34   54k
```

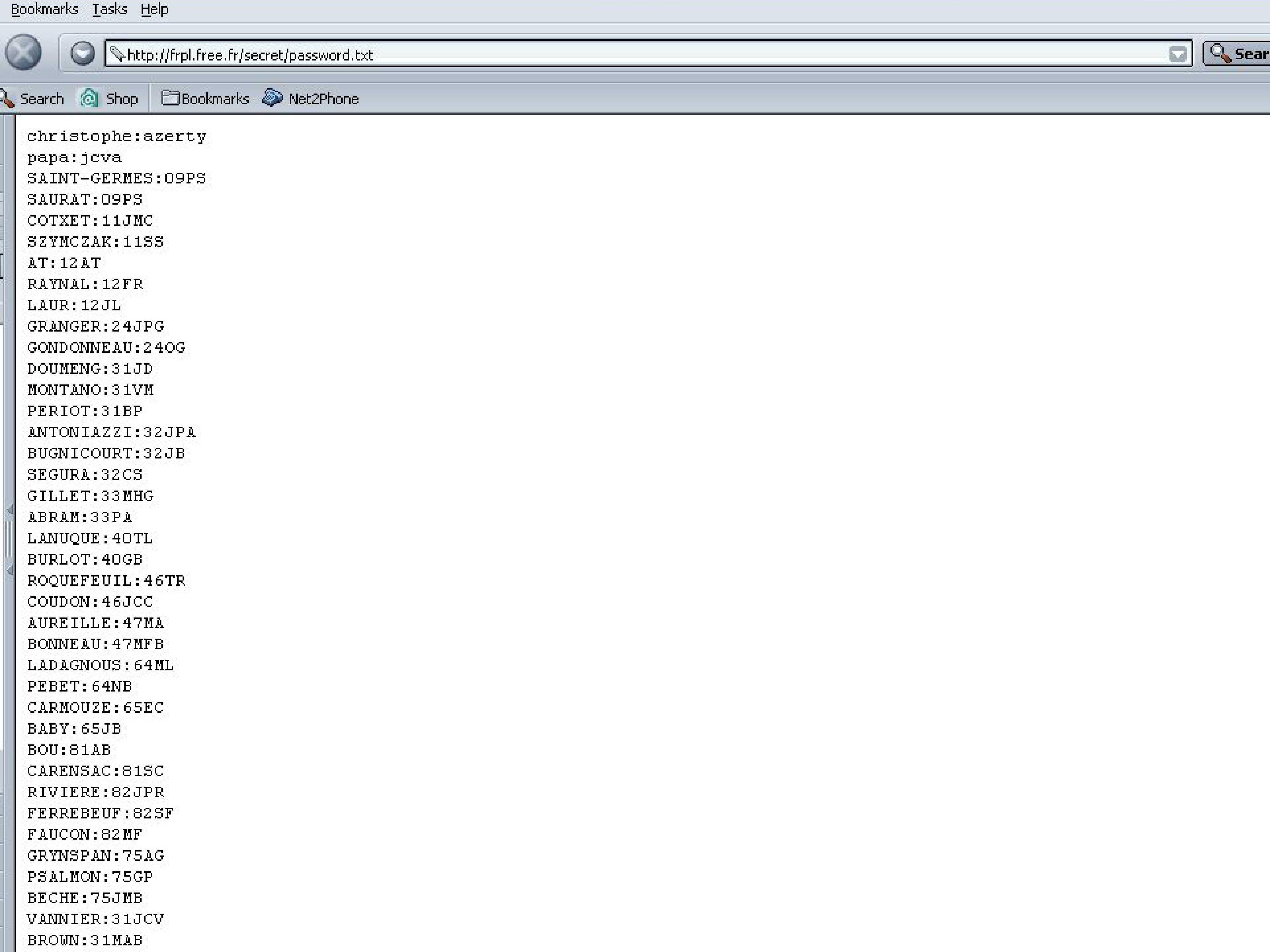


Index of /secret - Netscape 6
File Edit View Search Go Bookmarks Tasks Help
http://www.google.ca/search?q=cache:MjhWgy8mXV8C:frpl.free.fr/secret/+allintitle:%22Index+of+/secret%22&hl=en&ie=UTF-8
Search
FUJITSU
Home
My Netscape
Search
Shop
Bookmarks
Net2Phone
My Sidebar
Tabs
My Fujitsu
Search
Search
using
Netscape Search
Search Results
Bookmark this Search
Buddy List
Stocks
News
Shopping
Today's Tips
Bookmarks
Document: Done (0.601 secs)

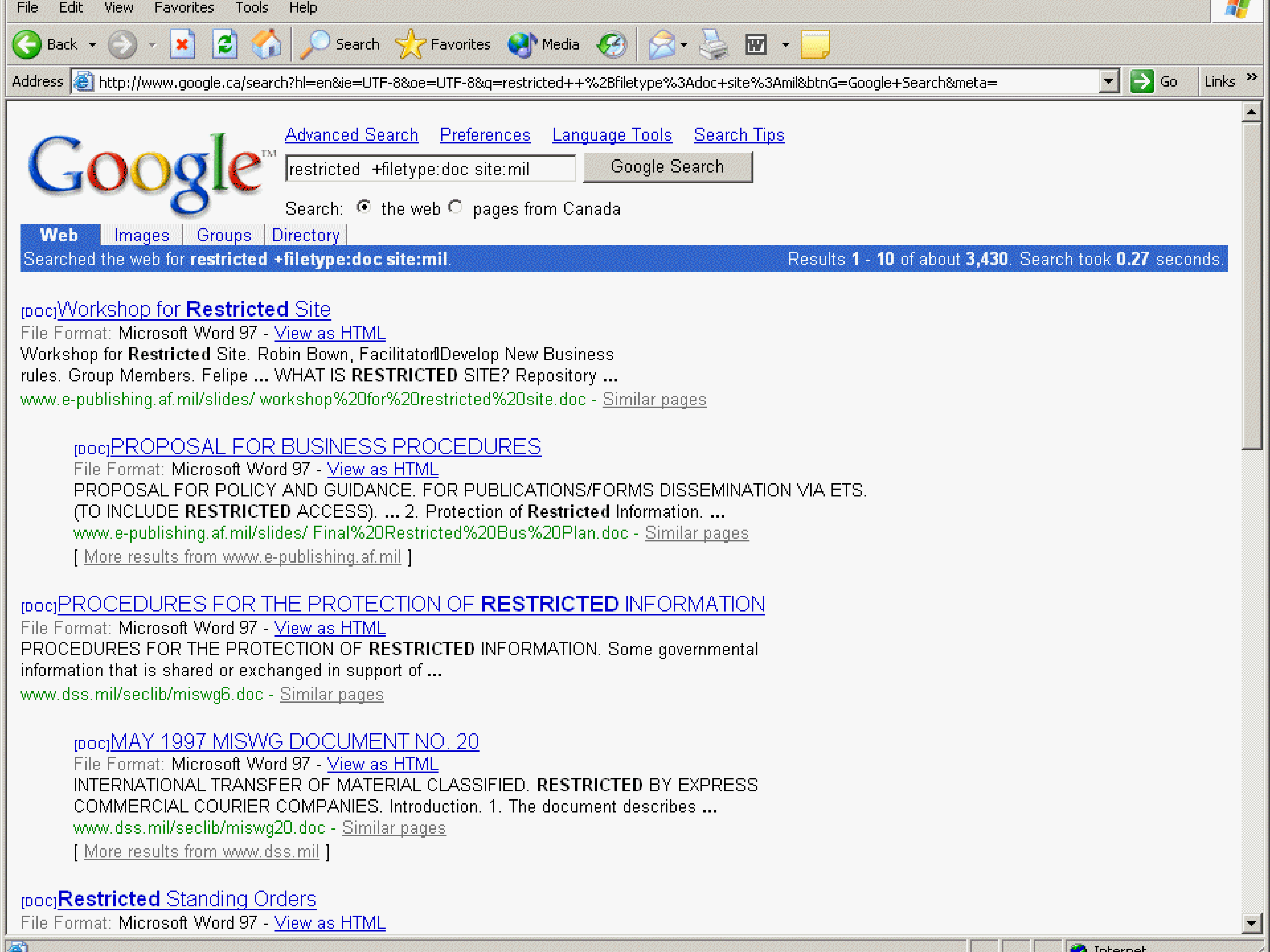
These terms only appear in links pointing to this page: **allintitle index of secret**

Index of /secret

```
Name                    Last modified       Size  Description

Parent Directory        22-Jul-2002 22:50      -
.htaccess               03-Dec-2001 18:47     1k
bsecu.html              03-Dec-2001 18:47     2k
collecte.html           19-Jul-2002 11:58    41k
collecte.jpg            19-Jul-2002 11:57   172k
collecte_grap.html      19-Jul-2002 11:58     1k
download.gif            03-Dec-2001 18:47     6k
excel.gif               03-Dec-2001 18:47     2k
fiche.gif               03-Dec-2001 18:47     1k
hsecu.html              03-Dec-2001 18:48     1k
password.txt            03-Dec-2001 18:48     1k
prix.html               18-Jul-2002 17:09    84k
secu.html               20-Jan-2002 21:33     1k
taille_Exp.html         14-Feb-2002 17:18    21k
telecharger.html        03-Dec-2001 18:48     1k
telecharger/            18-Jul-2002 17:07      -
```



```
christophe:azerty
papa:jcva
SAINT-GERMES:09PS
SAURAT:09PS
COTXET:11JMC
SZYMCZAK:11SS
AT:12AT
RAYNAL:12FR
LAUR:12JL
GRANGER:24JPG
GONDONNEAU:24OG
DOUMENG:31JD
MONTANO:31VM
PERIOT:31BP
ANTONIAZZI:32JPA
BUGNICOURT:32JB
SEGURA:32CS
GILLET:33MHG
ABRAM:33PA
LANUQUE:40TL
BURLOT:40GB
ROQUEFEUIL:46TR
COUDON:46JCC
AUREILLE:47MA
BONNEAU:47MFB
LADAGNOUS:64ML
PEBET:64NB
CARMOUZE:65EC
BABY:65JB
BOU:81AB
CARENSAC:81SC
RIVIERE:82JPR
FERREBEUF:82SF
FAUCON:82MF
GRYNSPAN:75AG
PSALMON:75GP
BECHE:75JMB
VANNIER:31JCV
BROWN:31MAB
```



http://www.google.ca/search?hl=en&ie=UTF-8&oe=UTF-8&q=restricted++%2Bfiletype%3Adoc+site%3Amil&btnG=Google+Search&meta=

restricted +filetype:doc site:mil

Search: ● the web ○ pages from Canada

Searched the web for **restricted +filetype:doc site:mil**. Results **1** - **10** of about **3,430**. Search took **0.27** seconds.

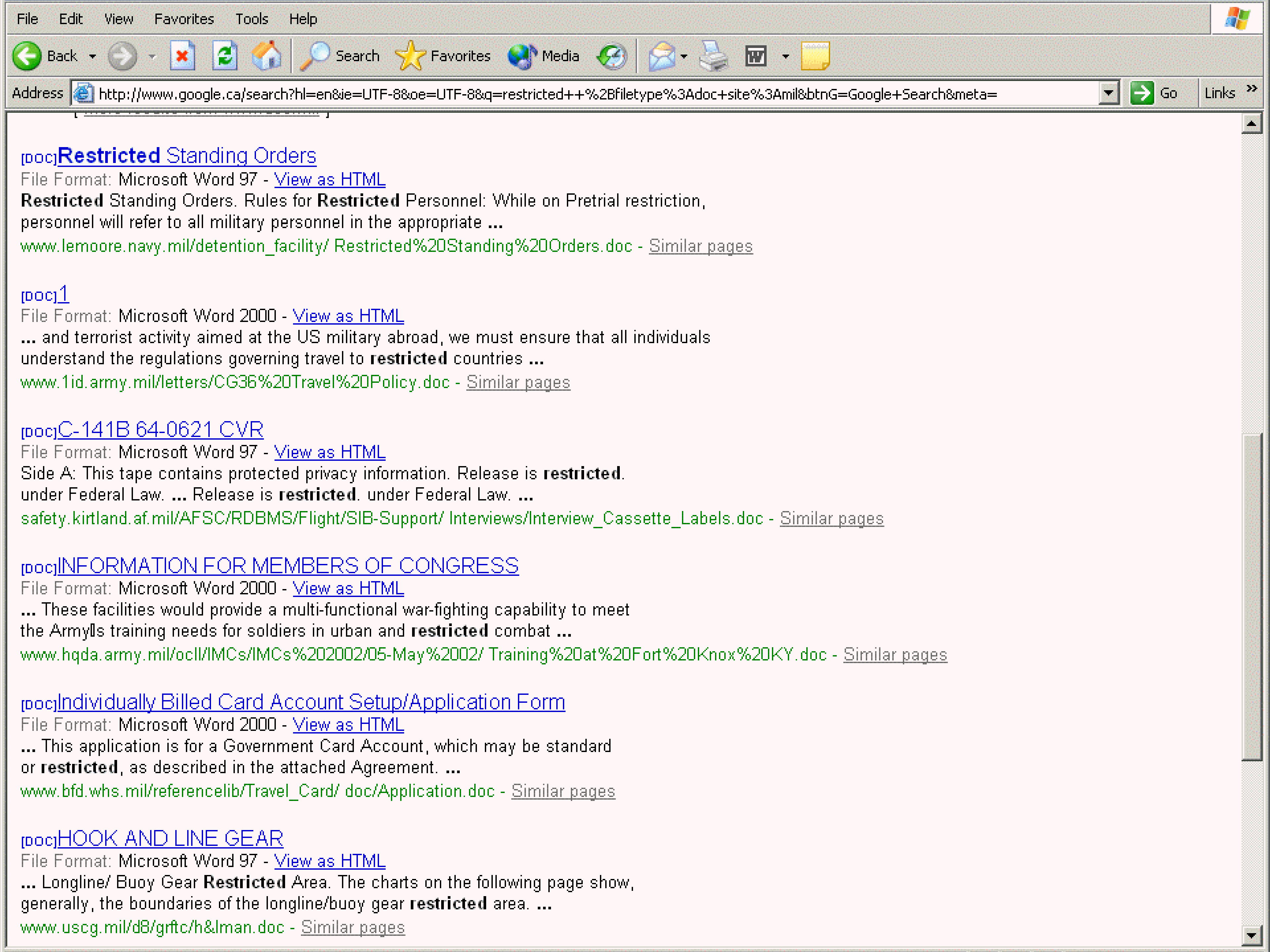
[DOC]Workshop for **Restricted** Site
File Format: Microsoft Word 97 - View as HTML
Workshop for **Restricted** Site. Robin Bown, Facilitator Develop New Business rules. Group Members. Felipe **...** WHAT IS **RESTRICTED** SITE? Repository **...**
www.e-publishing.af.mil/slides/ workshop%20for%20restricted%20site.doc - Similar pages

[DOC]PROPOSAL FOR BUSINESS PROCEDURES
File Format: Microsoft Word 97 - View as HTML
PROPOSAL FOR POLICY AND GUIDANCE. FOR PUBLICATIONS/FORMS DISSEMINATION VIA ETS. (TO INCLUDE **RESTRICTED** ACCESS). **...** 2. Protection of **Restricted** Information. **...**
www.e-publishing.af.mil/slides/ Final%20Restricted%20Bus%20Plan.doc - Similar pages
[More results from www.e-publishing.af.mil]

[DOC]PROCEDURES FOR THE PROTECTION OF **RESTRICTED** INFORMATION
File Format: Microsoft Word 97 - View as HTML
PROCEDURES FOR THE PROTECTION OF **RESTRICTED** INFORMATION. Some governmental information that is shared or exchanged in support of **...**
www.dss.mil/seclib/miswg6.doc - Similar pages

[DOC]MAY 1997 MISWG DOCUMENT NO. 20
File Format: Microsoft Word 97 - View as HTML
INTERNATIONAL TRANSFER OF MATERIAL CLASSIFIED. **RESTRICTED** BY EXPRESS COMMERCIAL COURIER COMPANIES. Introduction. 1. The document describes **...**
www.dss.mil/seclib/miswg20.doc - Similar pages
[More results from www.dss.mil]

[DOC]**Restricted** Standing Orders
File Format: Microsoft Word 97 - View as HTML



http://www.google.ca/search?hl=en&ie=UTF-8&oe=UTF-8&q=restricted++%2Bfiletype%3Adoc+site%3Amil&btnG=Google+Search&meta=

[DOC] **Restricted** Standing Orders
File Format: Microsoft Word 97 - View as HTML
Restricted Standing Orders. Rules for **Restricted** Personnel: While on Pretrial restriction, personnel will refer to all military personnel in the appropriate **...**
www.lemoore.navy.mil/detention_facility/ Restricted%20Standing%20Orders.doc - Similar pages

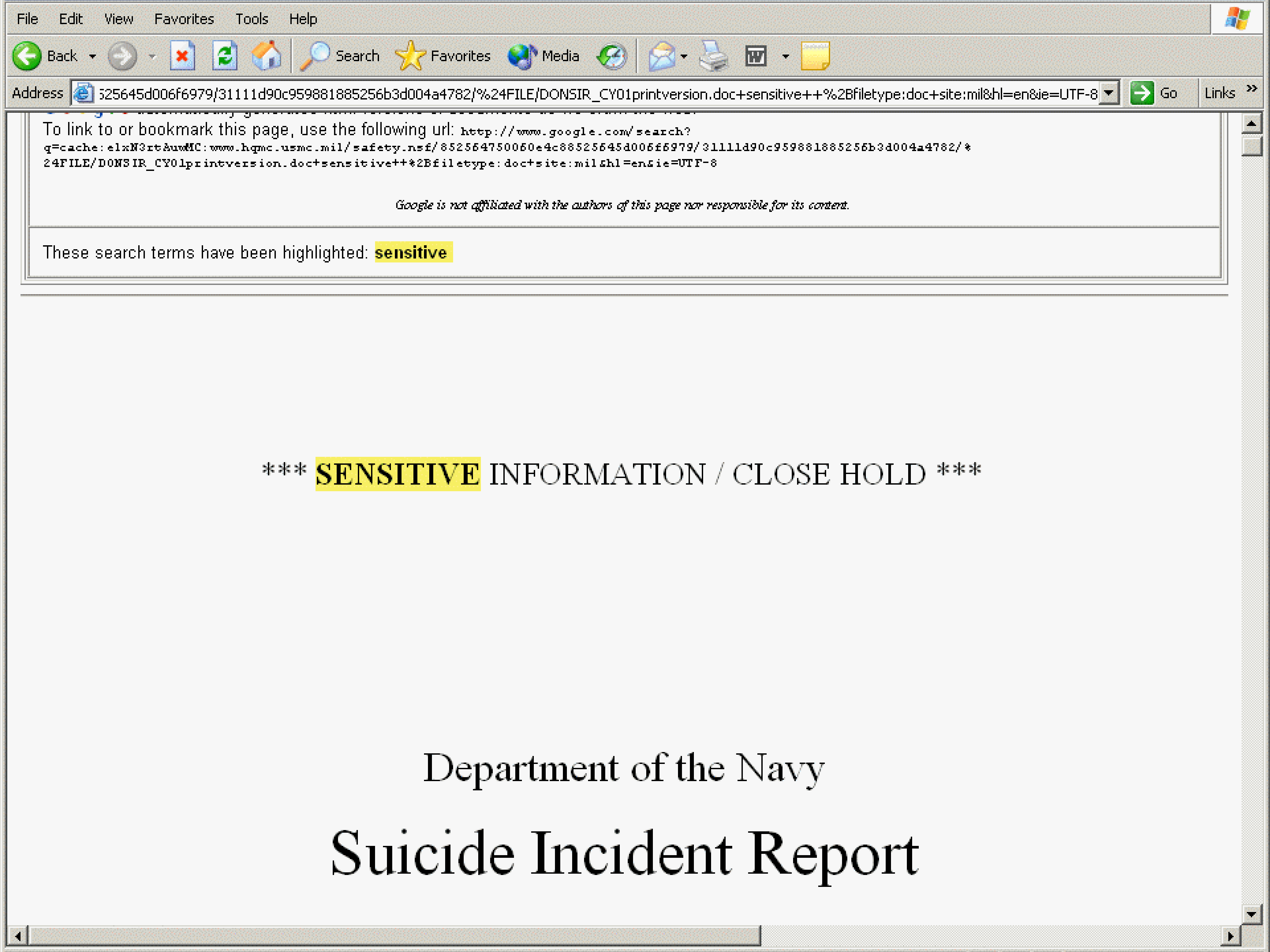
[DOC] 1
File Format: Microsoft Word 2000 - View as HTML
... and terrorist activity aimed at the US military abroad, we must ensure that all individuals understand the regulations governing travel to **restricted** countries **...**
www.1id.army.mil/letters/CG36%20Travel%20Policy.doc - Similar pages

[DOC] C-141B 64-0621 CVR
File Format: Microsoft Word 97 - View as HTML
Side A: This tape contains protected privacy information. Release is **restricted**. under Federal Law. **...** Release is **restricted**. under Federal Law. **...**
safety.kirtland.af.mil/AFSC/RDBMS/Flight/SIB-Support/ Interviews/Interview_Cassette_Labels.doc - Similar pages

[DOC] INFORMATION FOR MEMBERS OF CONGRESS
File Format: Microsoft Word 2000 - View as HTML
... These facilities would provide a multi-functional war-fighting capability to meet the Army▯s training needs for soldiers in urban and **restricted** combat **...**
www.hqda.army.mil/ocll/IMCs/IMCs%202002/05-May%2002/ Training%20at%20Fort%20Knox%20KY.doc - Similar pages

[DOC] Individually Billed Card Account Setup/Application Form
File Format: Microsoft Word 2000 - View as HTML
... This application is for a Government Card Account, which may be standard or **restricted**, as described in the attached Agreement. **...**
www.bfd.whs.mil/referencelib/Travel_Card/ doc/Application.doc - Similar pages

[DOC] HOOK AND LINE GEAR
File Format: Microsoft Word 97 - View as HTML
... Longline/ Buoy Gear **Restricted** Area. The charts on the following page show, generally, the boundaries of the longline/buoy gear **restricted** area. **...**
www.uscg.mil/d8/grftc/h&lman.doc - Similar pages



Address 525645d006f6979/31111d90c959881885256b3d004a4782/%24FILE/DONSIR_CY01printversion.doc+sensitive++%2Bfiletype:doc+site:mil&hl=en&ie=UTF-8

To link to or bookmark this page, use the following url: http://www.google.com/search?q=cache:elxN3rtAuwMC:www.hqmc.usmc.mil/safety.nsf/852564750060e4c88525645d006f6979/31111d90c959881885256b3d004a4782/%24FILE/DONSIR_CY01printversion.doc+sensitive++%2Bfiletype:doc+site:mil&hl=en&ie=UTF-8

Google is not affiliated with the authors of this page nor responsible for its content.

These search terms have been highlighted: **sensitive**

*** SENSITIVE INFORMATION / CLOSE HOLD ***

Department of the Navy

Suicide Incident Report

Sometimes it works when broken

- From an allintitle:"Index of /admin" search
- Admin account had been patched
- But the error information was pretty interesting, too…
  - Within the full page error report was:
    - Full paths to libraries /home/faraway/opt/cancat/lib
    - /usr/local/share/perl/5.6.1/Apache/ASP.pm
    - /usr/local/lib/perl/5.6.1/DBD/mysql.pm

Search Engines

- allintitle:”Index of /”
- site:gov   site:mil   site:ztarget.com
- filetype:doc   filetype:pdf   filetype:xls
- [cached]   [view as html]
- intitle:, inurl:, allinurl:
- Filetypes include: pdf, ps, wk[12345], wki, wks, wku, lwp, mw, xls, ppt, doc, wps, wdb, wri, rtf, ans and txt

Other Interesting Searches

- Far too many password files to bother counting anymore
- Access and error logs from a hotel chain
  - Included booking information and how long customers were staying
  - Some very well-known people had their full vacation schedules made available to the public
- Military “Procedures and Practices”

Other Interesting Searches

- allintitle:”Index of /” +confidential filetype:doc
  - A regulatory matters postal letter to an executive at a telecommunications commission, which contained competitor and specific revenue information, and made the following declaration:
    - The release of such information on the public record would allow current and potential competitors to develop more effective business and marketing strategies…

Other Interesting Searches

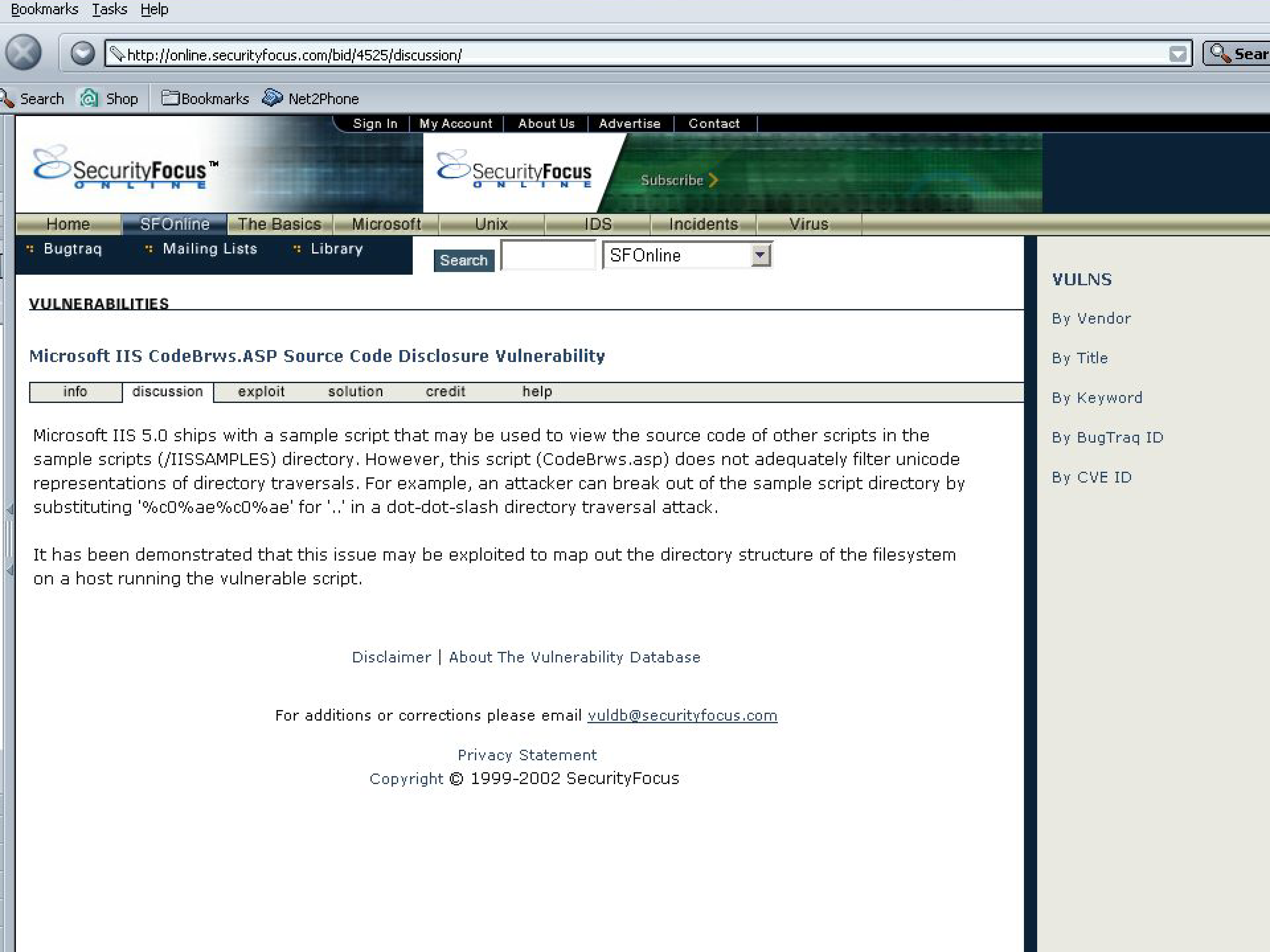
- Searches for WS_FTP.LOG give a rather detailed list of files that are updated regularly, and often provides internal network IP information normally hidden from the Internet
- Name, job title, phone number, and email address of mailroom staff at major military sites
- Inter-department electronic funds transfers

Other Interesting Searches

- robots.txt files tell search engines "don't look here"
- World-readable and in a known location so the search engines will find it easily, and ignore confidential or private directories
- What do you find when you *do* look in those directories?

Other Interesting Searches

- Passive scanning for vulnerable targets
- Where to find targets:
  - Search for phrases commonly found on web-based application interfaces (and especially their error messages)
  - Sites like http://www.securityfocus.com – provide information that can be used to create search criteria



VULNERABILITIES

Microsoft IIS CodeBrws.ASP Source Code Disclosure Vulnerability

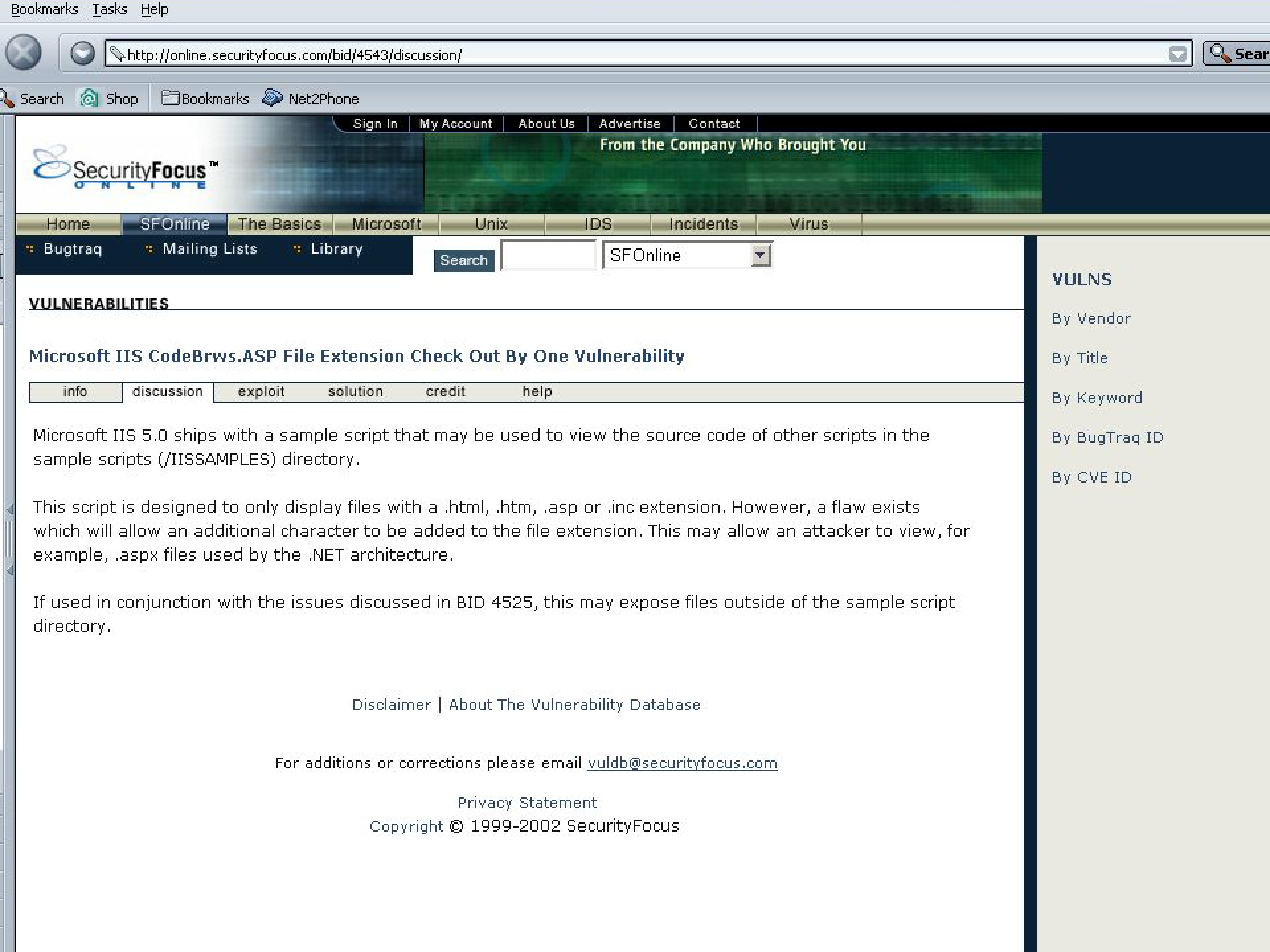
Microsoft IIS 5.0 ships with a sample script that may be used to view the source code of other scripts in the sample scripts (/IISSAMPLES) directory. However, this script (CodeBrws.asp) does not adequately filter unicode representations of directory traversals. For example, an attacker can break out of the sample script directory by substituting '%c0%ae%c0%ae' for '..' in a dot-dot-slash directory traversal attack.

It has been demonstrated that this issue may be exploited to map out the directory structure of the filesystem on a host running the vulnerable script.

Disclaimer | About The Vulnerability Database

For additions or corrections please email vuldb@securityfocus.com

Privacy Statement



VULNERABILITIES

Microsoft IIS CodeBrws.ASP File Extension Check Out By One Vulnerability

Microsoft IIS 5.0 ships with a sample script that may be used to view the source code of other scripts in the sample scripts (/IISSAMPLES) directory.

This script is designed to only display files with a .html, .htm, .asp or .inc extension. However, a flaw exists which will allow an additional character to be added to the file extension. This may allow an attacker to view, for example, .aspx files used by the .NET architecture.

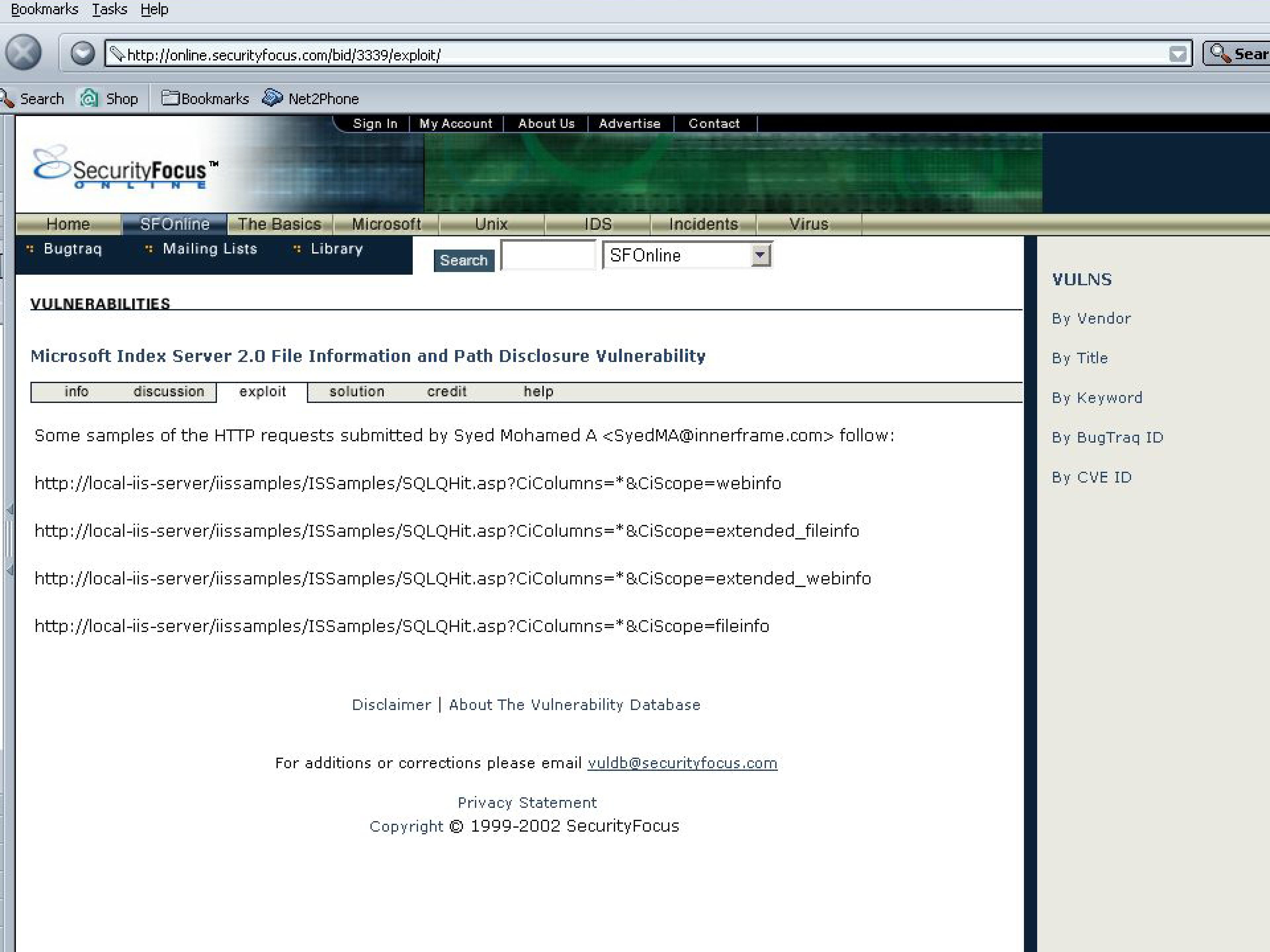
If used in conjunction with the issues discussed in BID 4525, this may expose files outside of the sample script directory.

Disclaimer | About The Vulnerability Database

For additions or corrections please email vuldb@securityfocus.com

Privacy Statement

Copyright © 1999-2002 SecurityFocus


Bookmarks Tasks Help
http://online.securityfocus.com/bid/3339/exploit/
Sear
Search Shop Bookmarks Net2Phone
Sign In | My Account | About Us | Advertise | Contact
SecurityFocus™ ONLINE
Home SFOnline The Basics Microsoft Unix IDS Incidents Virus
Bugtraq Mailing Lists Library
Search SFOnline
VULNS
By Vendor
By Title
By Keyword
By BugTraq ID
By CVE ID
info discussion exploit solution credit help

VULNERABILITIES

Microsoft Index Server 2.0 File Information and Path Disclosure Vulnerability

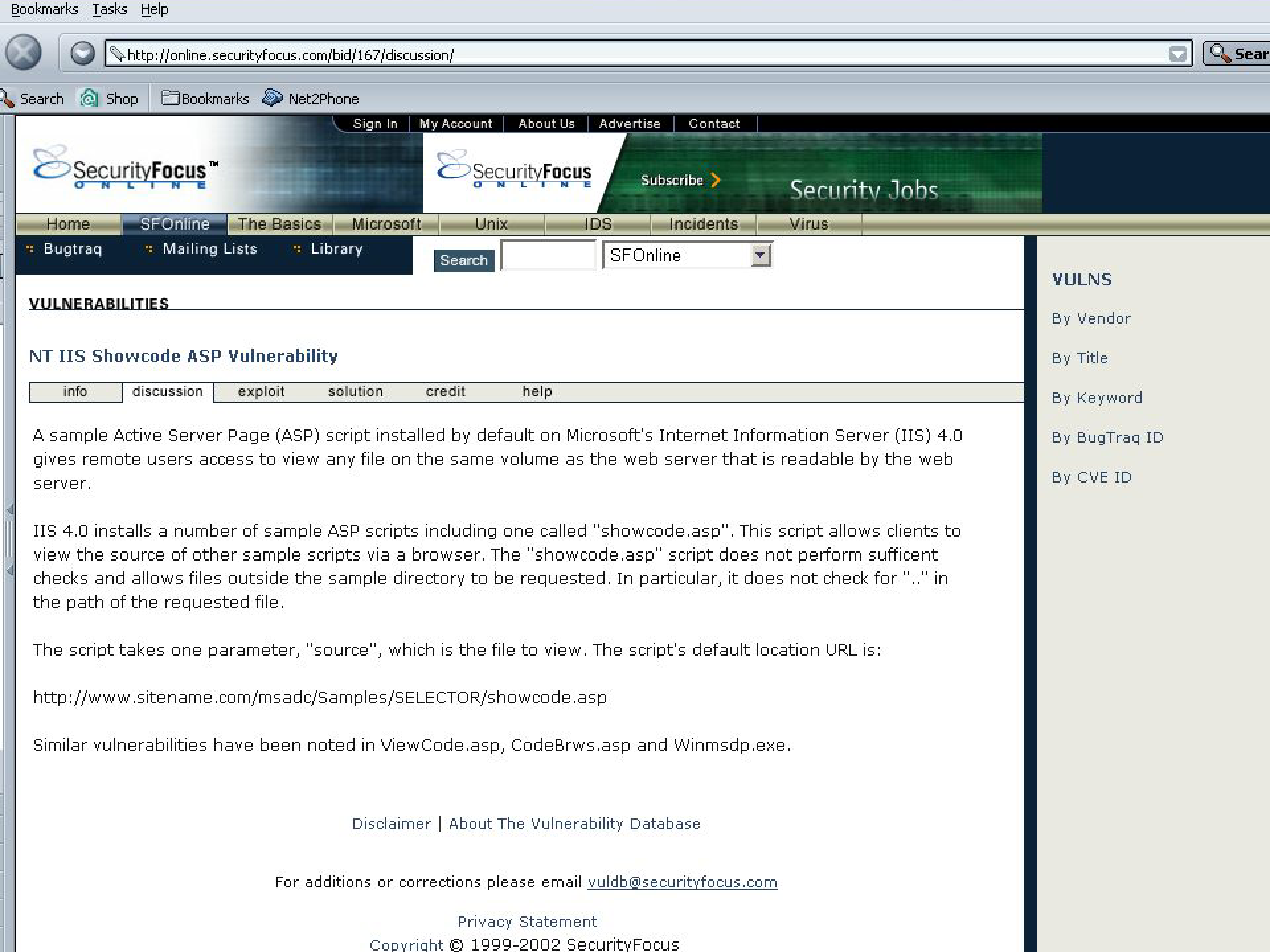
Some samples of the HTTP requests submitted by Syed Mohamed A <SyedMA@innerframe.com> follow:

```
http://local-iis-server/iissamples/ISSamples/SQLQHit.asp?CiColumns=*&CiScope=webinfo

http://local-iis-server/iissamples/ISSamples/SQLQHit.asp?CiColumns=*&CiScope=extended_fileinfo

http://local-iis-server/iissamples/ISSamples/SQLQHit.asp?CiColumns=*&CiScope=extended_webinfo

http://local-iis-server/iissamples/ISSamples/SQLQHit.asp?CiColumns=*&CiScope=fileinfo
```

Disclaimer | About The Vulnerability Database

For additions or corrections please email vuldb@securityfocus.com

Privacy Statement


Bookmarks Tasks Help
http://online.securityfocus.com/bid/167/discussion/
Sear
Search Shop Bookmarks Net2Phone
Sign In | My Account | About Us | Advertise | Contact
SecurityFocus ONLINE
Subscribe
Security Jobs
Home SFOnline The Basics Microsoft Unix IDS Incidents Virus
Bugtraq Mailing Lists Library
Search
SFOnline
VULNS
By Vendor
By Title
By Keyword
By BugTraq ID
By CVE ID
info discussion exploit solution credit help

VULNERABILITIES

NT IIS Showcode ASP Vulnerability

A sample Active Server Page (ASP) script installed by default on Microsoft's Internet Information Server (IIS) 4.0 gives remote users access to view any file on the same volume as the web server that is readable by the web server.

IIS 4.0 installs a number of sample ASP scripts including one called "showcode.asp". This script allows clients to view the source of other sample scripts via a browser. The "showcode.asp" script does not perform sufficent checks and allows files outside the sample directory to be requested. In particular, it does not check for ".." in the path of the requested file.

The script takes one parameter, "source", which is the file to view. The script's default location URL is:

http://www.sitename.com/msadc/Samples/SELECTOR/showcode.asp

Similar vulnerabilities have been noted in ViewCode.asp, CodeBrws.asp and Winmsdp.exe.

Disclaimer | About The Vulnerability Database

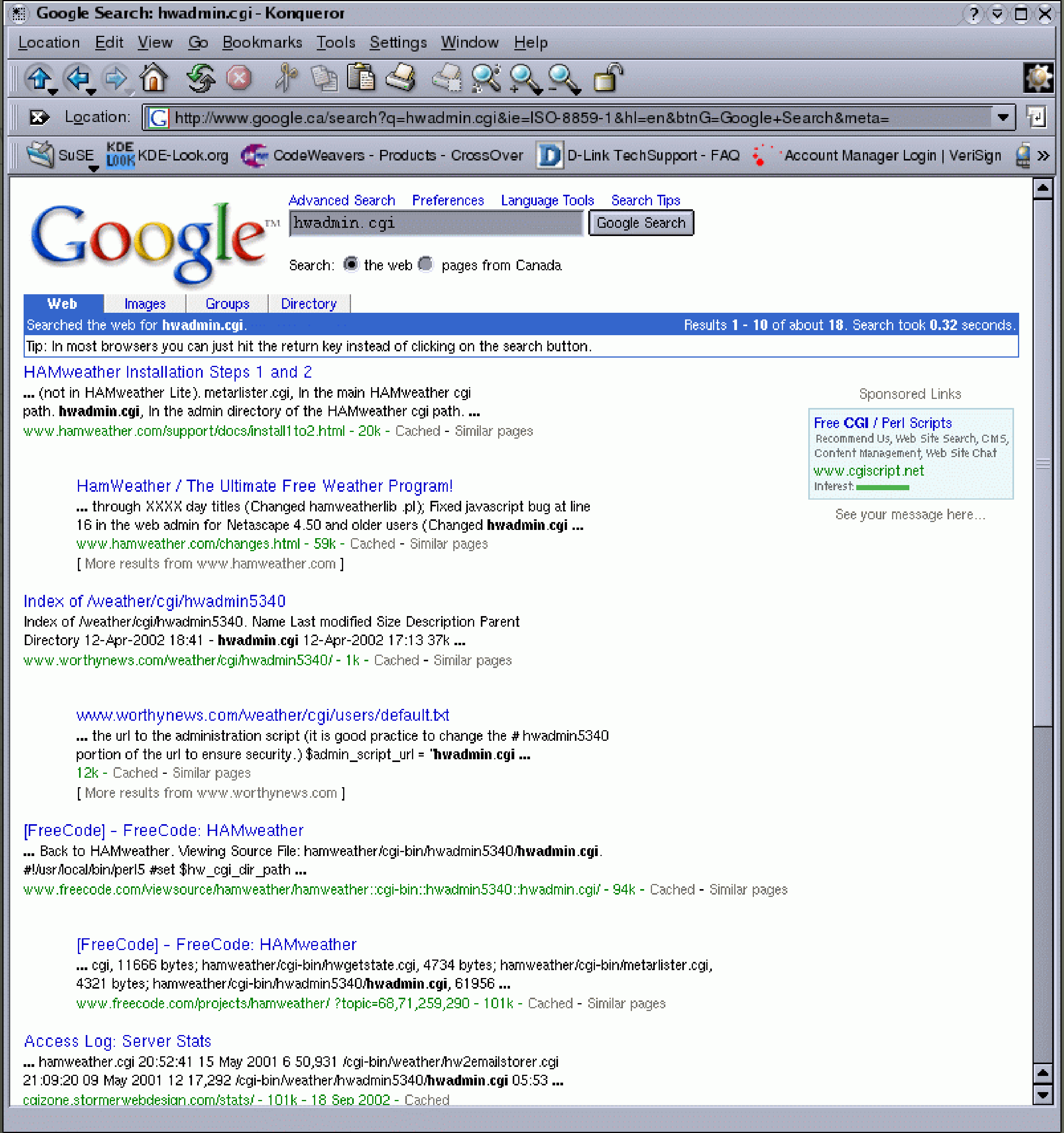
For additions or corrections please email vuldb@securityfocus.com

Privacy Statement

Copyright © 1999-2002 SecurityFocus

Unreported Vulnerabilities

- Many vulnerabilities go unreported and unfixed, despite how obvious they are
- Example:
  - HAMWeather is a weather software package that allows websites to provide accurate weather information. Geared towards news sites.
  - Does not require authentication for any of its administrative processes
  - Lets search for that administrative program…



Location: http://www.google.ca/search?q=hwadmin.cgi&ie=ISO-8859-1&hl=en&btnG=Google+Search&meta=

hwadmin.cgi

Search: ● the web ○ pages from Canada

Searched the web for **hwadmin.cgi**. Results **1** - **10** of about **18**. Search took **0.32** seconds.

Tip: In most browsers you can just hit the return key instead of clicking on the search button.

HAMweather Installation Steps 1 and 2
... (not in HAMweather Lite). metarlister.cgi, In the main HAMweather cgi path. **hwadmin.cgi**, In the admin directory of the HAMweather cgi path. ...
www.hamweather.com/support/docs/install1to2.html - 20k - Cached - Similar pages

HamWeather / The Ultimate Free Weather Program!
... through XXXX day titles (Changed hamweatherlib .pl); Fixed javascript bug at line 16 in the web admin for Netascape 4.50 and older users (Changed **hwadmin.cgi** ...
www.hamweather.com/changes.html - 59k - Cached - Similar pages
[More results from www.hamweather.com]

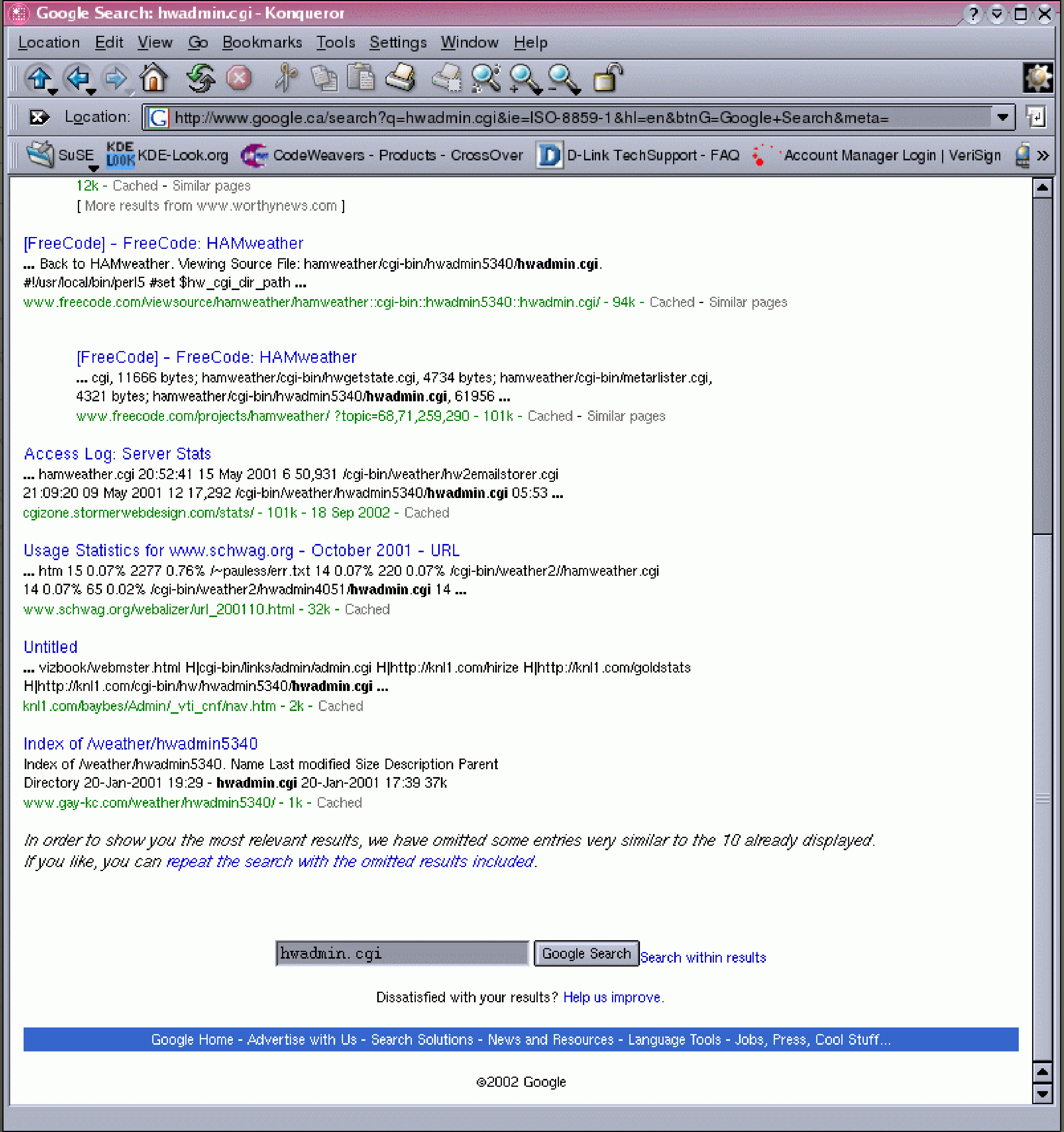
Index of /weather/cgi/hwadmin5340
Index of /weather/cgi/hwadmin5340. Name Last modified Size Description Parent Directory 12-Apr-2002 18:41 - **hwadmin.cgi** 12-Apr-2002 17:13 37k ...
www.worthynews.com/weather/cgi/hwadmin5340/ - 1k - Cached - Similar pages

www.worthynews.com/weather/cgi/users/default.txt
... the url to the administration script (it is good practice to change the # hwadmin5340 portion of the url to ensure security.) $admin_script_url = '**hwadmin.cgi** ...
12k - Cached - Similar pages
[More results from www.worthynews.com]

[FreeCode] - FreeCode: HAMweather
... Back to HAMweather. Viewing Source File: hamweather/cgi-bin/hwadmin5340/**hwadmin.cgi**. #!/usr/local/bin/perl5 #set $hw_cgi_dir_path ...
www.freecode.com/viewsource/hamweather/hamweather::cgi-bin::hwadmin5340::hwadmin.cgi/ - 94k - Cached - Similar pages

[FreeCode] - FreeCode: HAMweather
... cgi, 11666 bytes; hamweather/cgi-bin/hwgetstate.cgi, 4734 bytes; hamweather/cgi-bin/metarlister.cgi, 4321 bytes; hamweather/cgi-bin/hwadmin5340/**hwadmin.cgi**, 61956 ...
www.freecode.com/projects/hamweather/ ?topic=68,71,259,290 - 101k - Cached - Similar pages

Access Log: Server Stats
... hamweather.cgi 20:52:41 15 May 2001 6 50,931 /cgi-bin/weather/hw2emailstorer.cgi 21:09:20 09 May 2001 12 17,292 /cgi-bin/weather/hwadmin5340/**hwadmin.cgi** 05:53 ...
cgizone.stormerwebdesign.com/stats/ - 101k - 18 Sep 2002 - Cached


Google Search: hwadmin.cgi - Konqueror
Location
Edit
View
Go
Bookmarks
Tools
Settings
Window
Help
Location:
SuSE
KDE-Look.org
CodeWeavers - Products - CrossOver
D-Link TechSupport - FAQ
Account Manager Login | VeriSign

Location: http://www.google.ca/search?q=hwadmin.cgi&ie=ISO-8859-1&hl=en&btnG=Google+Search&meta=

12k - Cached - Similar pages
[More results from www.worthynews.com]

[FreeCode] - FreeCode: HAMweather
... Back to HAMweather. Viewing Source File: hamweather/cgi-bin/hwadmin5340/**hwadmin.cgi**.
#!/usr/local/bin/perl5 #set $hw_cgi_dir_path ...
www.freecode.com/viewsource/hamweather/hamweather::cgi-bin::hwadmin5340::hwadmin.cgi/ - 94k - Cached - Similar pages

[FreeCode] - FreeCode: HAMweather
... cgi, 11666 bytes; hamweather/cgi-bin/hwgetstate.cgi, 4734 bytes; hamweather/cgi-bin/metarlister.cgi,
4321 bytes; hamweather/cgi-bin/hwadmin5340/**hwadmin.cgi**, 61956 ...
www.freecode.com/projects/hamweather/ ?topic=68,71,259,290 - 101k - Cached - Similar pages

Access Log: Server Stats
... hamweather.cgi 20:52:41 15 May 2001 6 50,931 /cgi-bin/weather/hw2emailstorer.cgi
21:09:20 09 May 2001 12 17,292 /cgi-bin/weather/hwadmin5340/**hwadmin.cgi** 05:53 ...
cgizone.stormerwebdesign.com/stats/ - 101k - 18 Sep 2002 - Cached

Usage Statistics for www.schwag.org - October 2001 - URL
... htm 15 0.07% 2277 0.76% /~pauless/err.txt 14 0.07% 220 0.07% /cgi-bin/weather2//hamweather.cgi
14 0.07% 65 0.02% /cgi-bin/weather2/hwadmin4051/**hwadmin.cgi** 14 ...
www.schwag.org/webalizer/url_200110.html - 32k - Cached

Untitled
... vizbook/webmster.html H|cgi-bin/links/admin/admin.cgi H|http://knl1.com/hirize H|http://knl1.com/goldstats
H|http://knl1.com/cgi-bin/hw/hwadmin5340/**hwadmin.cgi** ...
knl1.com/baybes/Admin/_vti_cnf/nav.htm - 2k - Cached

Index of /weather/hwadmin5340
Index of /weather/hwadmin5340. Name Last modified Size Description Parent
Directory 20-Jan-2001 19:29 - **hwadmin.cgi** 20-Jan-2001 17:39 37k
www.gay-kc.com/weather/hwadmin5340/ - 1k - Cached

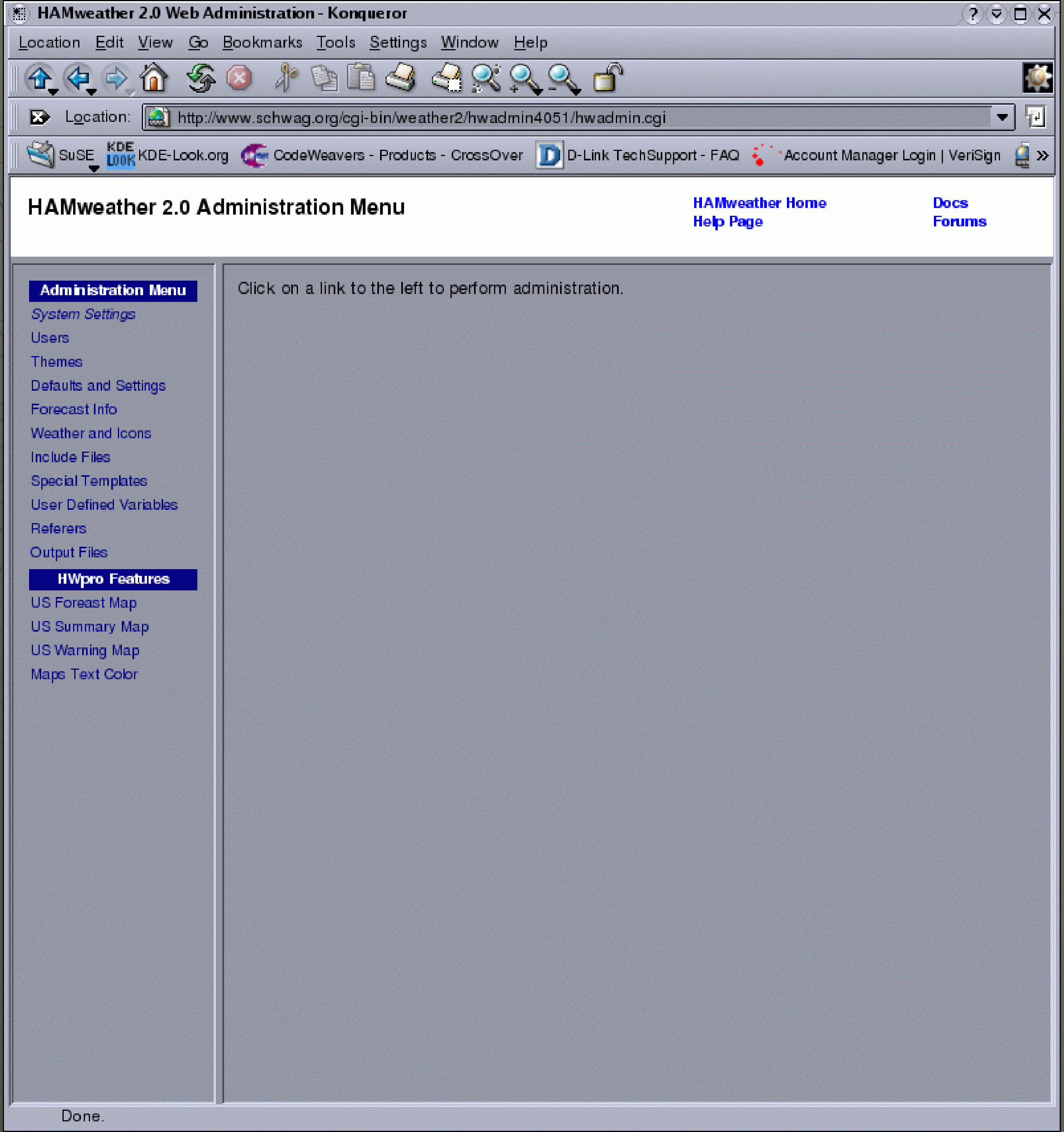
In order to show you the most relevant results, we have omitted some entries very similar to the 10 already displayed.
If you like, you can repeat the search with the omitted results included.

hwadmin.cgi

Dissatisfied with your results? Help us improve.

Google Home - Advertise with Us - Search Solutions - News and Resources - Language Tools - Jobs, Press, Cool Stuff...

©2002 Google


HAMweather 2.0 Web Administration - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location: http://www.schwag.org/cgi-bin/weather2/hwadmin4051/hwadmin.cgi
SuSE
KDE-Look.org
CodeWeavers - Products - CrossOver
D-Link TechSupport - FAQ
Account Manager Login | VeriSign

HAMweather 2.0 Administration Menu

HAMweather Home
Help Page
Docs
Forums

Administration Menu

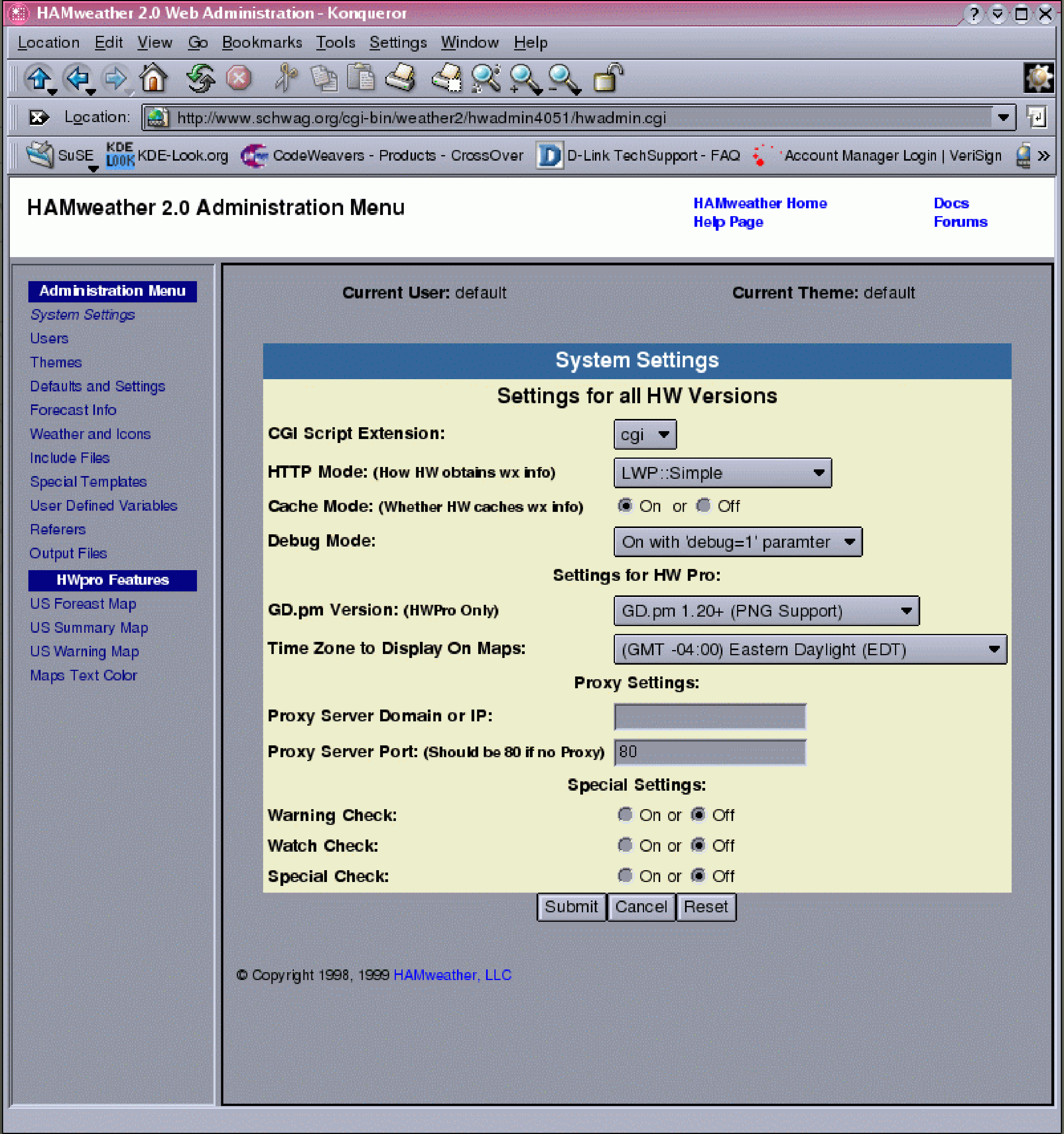
System Settings
Users
Themes
Defaults and Settings
Forecast Info
Weather and Icons
Include Files
Special Templates
User Defined Variables
Referers
Output Files

HWpro Features

US Foreast Map
US Summary Map
US Warning Map
Maps Text Color

Click on a link to the left to perform administration.

Done.


HAMweather 2.0 Web Administration - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:
SuSE
KDE-Look.org
CodeWeavers - Products - CrossOver
D-Link TechSupport - FAQ
Account Manager Login | VeriSign

Location: http://www.schwag.org/cgi-bin/weather2/hwadmin4051/hwadmin.cgi

HAMweather 2.0 Administration Menu

Current User: default **Current Theme:** default

System Settings

Settings for all HW Versions

CGI Script Extension:	cgi
HTTP Mode: **(How HW obtains wx info)**	LWP::Simple
Cache Mode: **(Whether HW caches wx info)**	● On or ○ Off
Debug Mode:	On with 'debug=1' paramter

Settings for HW Pro:

GD.pm Version: **(HWPro Only)**	GD.pm 1.20+ (PNG Support)
Time Zone to Display On Maps:	(GMT -04:00) Eastern Daylight (EDT)

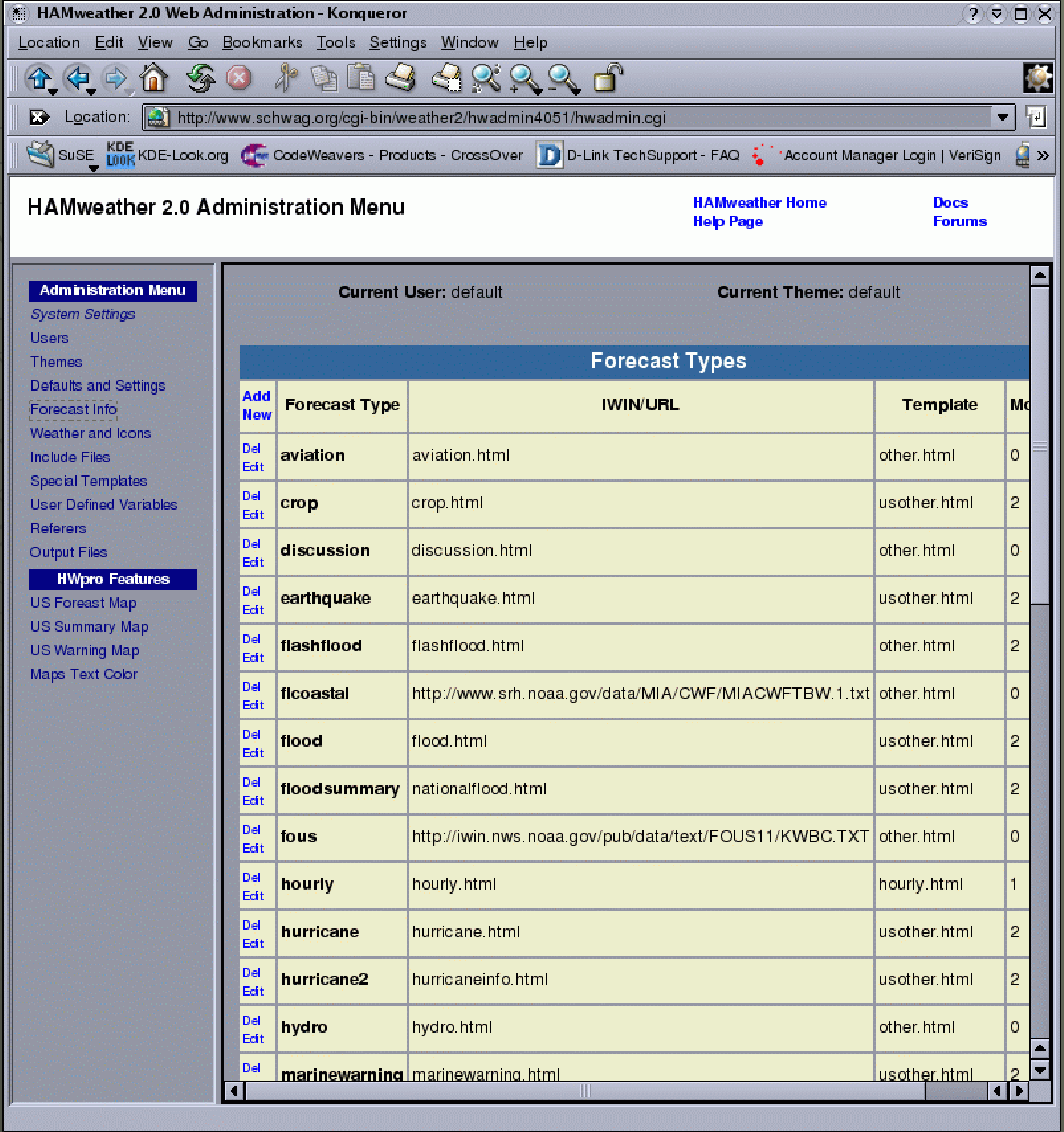
Proxy Settings:

Proxy Server Domain or IP:	
Proxy Server Port: **(Should be 80 if no Proxy)**	80

Special Settings:

Warning Check:	○ On or ● Off
Watch Check:	○ On or ● Off
Special Check:	○ On or ● Off

© Copyright 1998, 1999 HAMweather, LLC


HAMweather 2.0 Web Administration - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location: http://www.schwag.org/cgi-bin/weather2/hwadmin4051/hwadmin.cgi
SuSE
KDE-Look.org
CodeWeavers - Products - CrossOver
D-Link TechSupport - FAQ
Account Manager Login | VeriSign

HAMweather 2.0 Administration Menu

HAMweather Home
Help Page
Docs
Forums

Administration Menu

- *System Settings*
- Users
- Themes
- Defaults and Settings
- Forecast Info
- Weather and Icons
- Include Files
- Special Templates
- User Defined Variables
- Referers
- Output Files

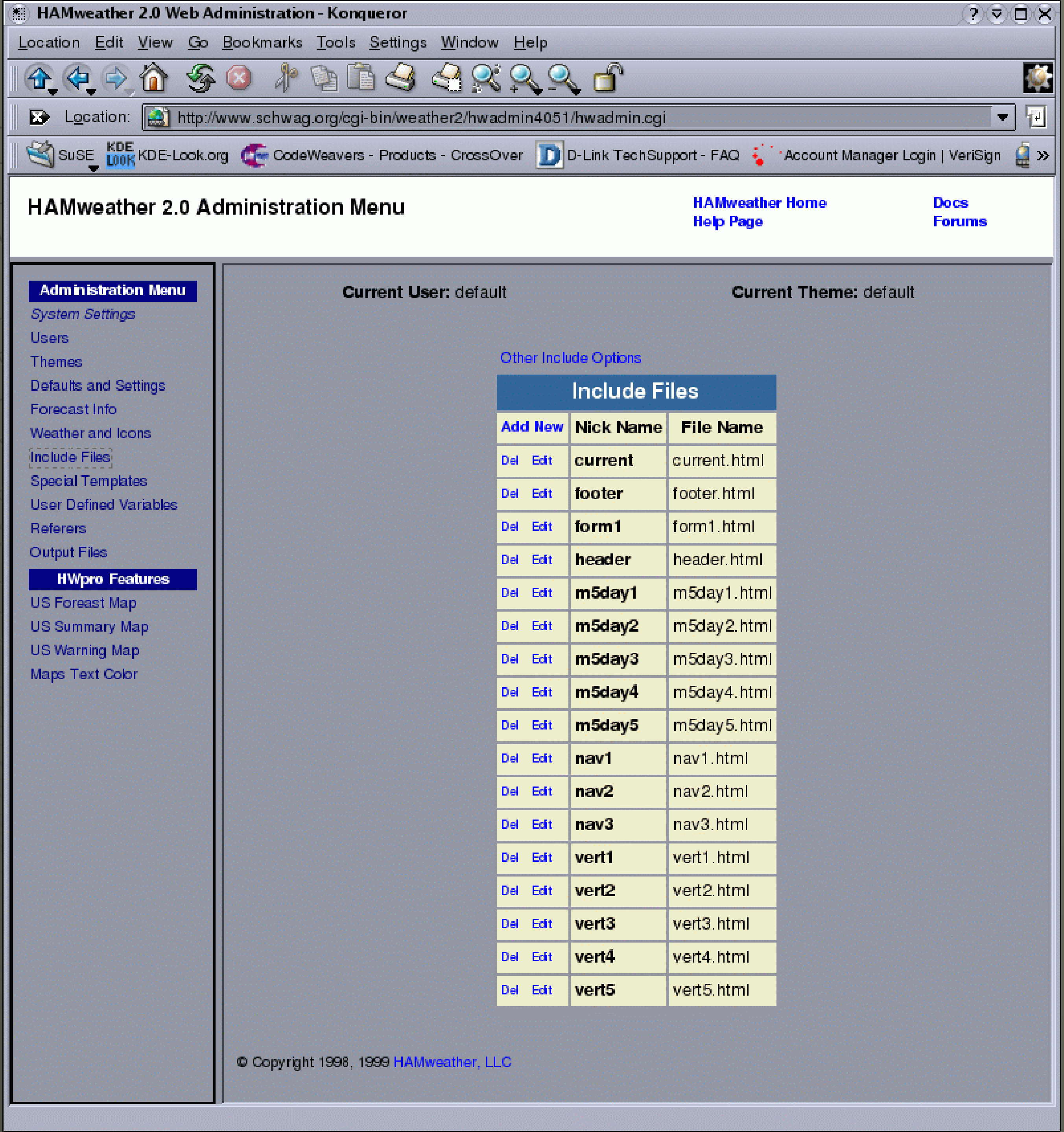
HWpro Features

- US Foreast Map
- US Summary Map
- US Warning Map
- Maps Text Color

Current User: default **Current Theme:** default

Forecast Types

Add New	Forecast Type	IWIN/URL	Template	Mo
Del Edit	**aviation**	aviation.html	other.html	0
Del Edit	**crop**	crop.html	usother.html	2
Del Edit	**discussion**	discussion.html	other.html	0
Del Edit	**earthquake**	earthquake.html	usother.html	2
Del Edit	**flashflood**	flashflood.html	other.html	2
Del Edit	**flcoastal**	http://www.srh.noaa.gov/data/MIA/CWF/MIACWFTBW.1.txt	other.html	0
Del Edit	**flood**	flood.html	usother.html	2
Del Edit	**floodsummary**	nationalflood.html	usother.html	2
Del Edit	**fous**	http://iwin.nws.noaa.gov/pub/data/text/FOUS11/KWBC.TXT	other.html	0
Del Edit	**hourly**	hourly.html	hourly.html	1
Del Edit	**hurricane**	hurricane.html	usother.html	2
Del Edit	**hurricane2**	hurricaneinfo.html	usother.html	2
Del Edit	**hydro**	hydro.html	other.html	0
Del	**marinewarning**	marinewarning.html	usother.html	2


HAMweather 2.0 Web Administration - Konqueror
Location
Edit
View
Go
Bookmarks
Tools
Settings
Window
Help
Location:
SuSE
KDE-Look.org
CodeWeavers - Products - CrossOver
D-Link TechSupport - FAQ
Account Manager Login | VeriSign

Location: http://www.schwag.org/cgi-bin/weather2/hwadmin4051/hwadmin.cgi

HAMweather 2.0 Administration Menu

HAMweather Home
Help Page
Docs
Forums

Administration Menu
- *System Settings*
- Users
- Themes
- Defaults and Settings
- Forecast Info
- Weather and Icons
- Include Files
- Special Templates
- User Defined Variables
- Referers
- Output Files

HWpro Features
- US Foreast Map
- US Summary Map
- US Warning Map
- Maps Text Color

Current User: default **Current Theme:** default

Other Include Options

Include Files

Add New		Nick Name	File Name
Del	Edit	**current**	current.html
Del	Edit	**footer**	footer.html
Del	Edit	**form1**	form1.html
Del	Edit	**header**	header.html
Del	Edit	**m5day1**	m5day1.html
Del	Edit	**m5day2**	m5day2.html
Del	Edit	**m5day3**	m5day3.html
Del	Edit	**m5day4**	m5day4.html
Del	Edit	**m5day5**	m5day5.html
Del	Edit	**nav1**	nav1.html
Del	Edit	**nav2**	nav2.html
Del	Edit	**nav3**	nav3.html
Del	Edit	**vert1**	vert1.html
Del	Edit	**vert2**	vert2.html
Del	Edit	**vert3**	vert3.html
Del	Edit	**vert4**	vert4.html
Del	Edit	**vert5**	vert5.html

© Copyright 1998, 1999 HAMweather, LLC

More Web Hacking

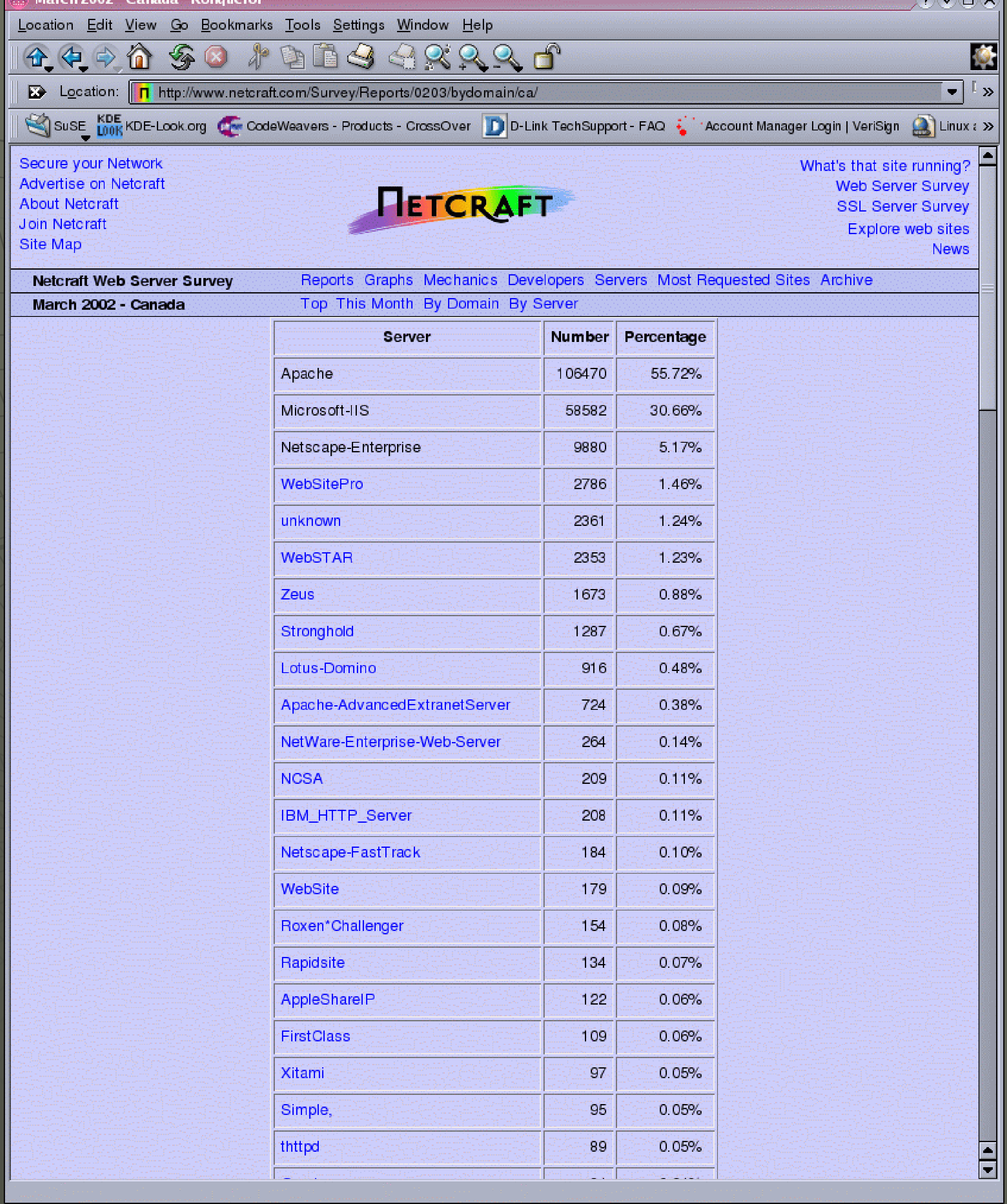
- Search engines are a treasure trove of information
- We’ve looked at general web search engines, but let’s now look at more information specific sites
  - Administrative web servers
  - Reconnaissance from the sky
  - Proxies

Administrative Web Servers

- Many devices come with web servers enabled by default:
  - Printers
  - Routers and Switches
  - Wireless Access Points

Printers on the Web?

- Netcraft provides an ongoing tally of web servers operating on the Internet.
- Can we find web based administration?


March 2002 - Canada - Konqueror
Location
Edit
View
Go
Bookmarks
Tools
Settings
Window
Help
SuSE
KDE-Look.org
CodeWeavers - Products - CrossOver
D-Link TechSupport - FAQ
Account Manager Login | VeriSign
Linux

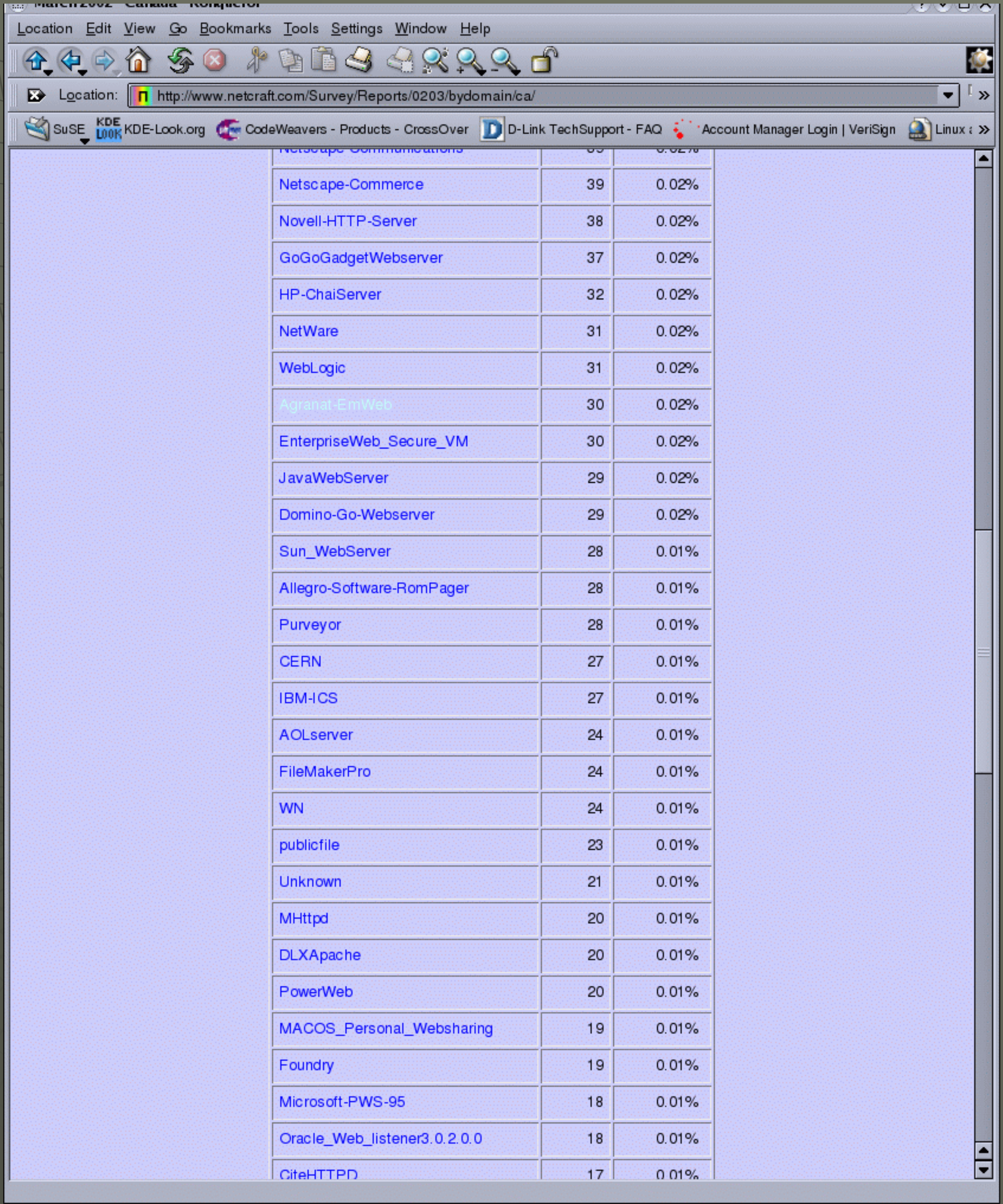
Location: http://www.netcraft.com/Survey/Reports/0203/bydomain/ca/

Netcraft Web Server Survey

March 2002 - Canada

Server	Number	Percentage
Apache	106470	55.72%
Microsoft-IIS	58582	30.66%
Netscape-Enterprise	9880	5.17%
WebSitePro	2786	1.46%
unknown	2361	1.24%
WebSTAR	2353	1.23%
Zeus	1673	0.88%
Stronghold	1287	0.67%
Lotus-Domino	916	0.48%
Apache-AdvancedExtranetServer	724	0.38%
NetWare-Enterprise-Web-Server	264	0.14%
NCSA	209	0.11%
IBM_HTTP_Server	208	0.11%
Netscape-FastTrack	184	0.10%
WebSite	179	0.09%
Roxen*Challenger	154	0.08%
Rapidsite	134	0.07%
AppleShareIP	122	0.06%
FirstClass	109	0.06%
Xitami	97	0.05%
Simple,	95	0.05%
thttpd	89	0.05%

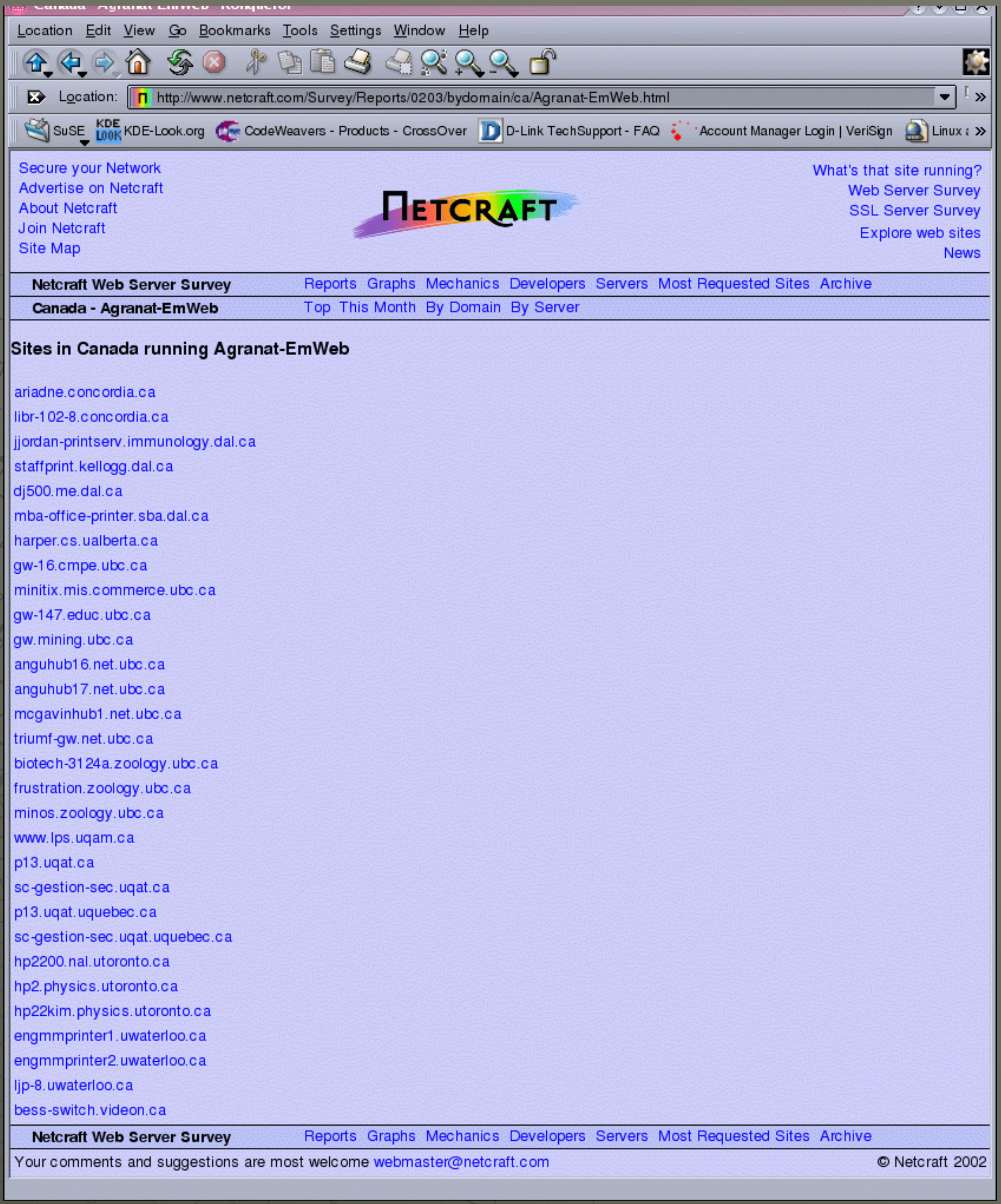
Agranat-EmWeb


March 2002 - Canada - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
SuSE
KDE-Look.org
CodeWeavers - Products - CrossOver
D-Link TechSupport - FAQ
Account Manager Login | VeriSign
Linux

Location: http://www.netcraft.com/Survey/Reports/0203/bydomain/ca/

Netscape-Communications	[illegible]	0.02%
Netscape-Commerce	39	0.02%
Novell-HTTP-Server	38	0.02%
GoGoGadgetWebserver	37	0.02%
HP-ChaiServer	32	0.02%
NetWare	31	0.02%
WebLogic	31	0.02%
Agranat-EmWeb	30	0.02%
EnterpriseWeb_Secure_VM	30	0.02%
JavaWebServer	29	0.02%
Domino-Go-Webserver	29	0.02%
Sun_WebServer	28	0.01%
Allegro-Software-RomPager	28	0.01%
Purveyor	28	0.01%
CERN	27	0.01%
IBM-ICS	27	0.01%
AOLserver	24	0.01%
FileMakerPro	24	0.01%
WN	24	0.01%
publicfile	23	0.01%
Unknown	21	0.01%
MHttpd	20	0.01%
DLXApache	20	0.01%
PowerWeb	20	0.01%
MACOS_Personal_Websharing	19	0.01%
Foundry	19	0.01%
Microsoft-PWS-95	18	0.01%
Oracle_Web_listener3.0.2.0.0	18	0.01%
CiteHTTPD	17	0.01%

Several sites seem to have left this particular printer wide open


Location Edit View Go Bookmarks Tools Settings Window Help
Location:
SuSE
KDE-Look.org
CodeWeavers - Products - CrossOver
D-Link TechSupport - FAQ
Account Manager Login | VeriSign
Linux

http://www.netcraft.com/Survey/Reports/0203/bydomain/ca/Agranat-EmWeb.html

Secure your Network
Advertise on Netcraft
About Netcraft
Join Netcraft
Site Map

NETCRAFT

What's that site running?
Web Server Survey
SSL Server Survey
Explore web sites
News

Netcraft Web Server Survey Reports Graphs Mechanics Developers Servers Most Requested Sites Archive

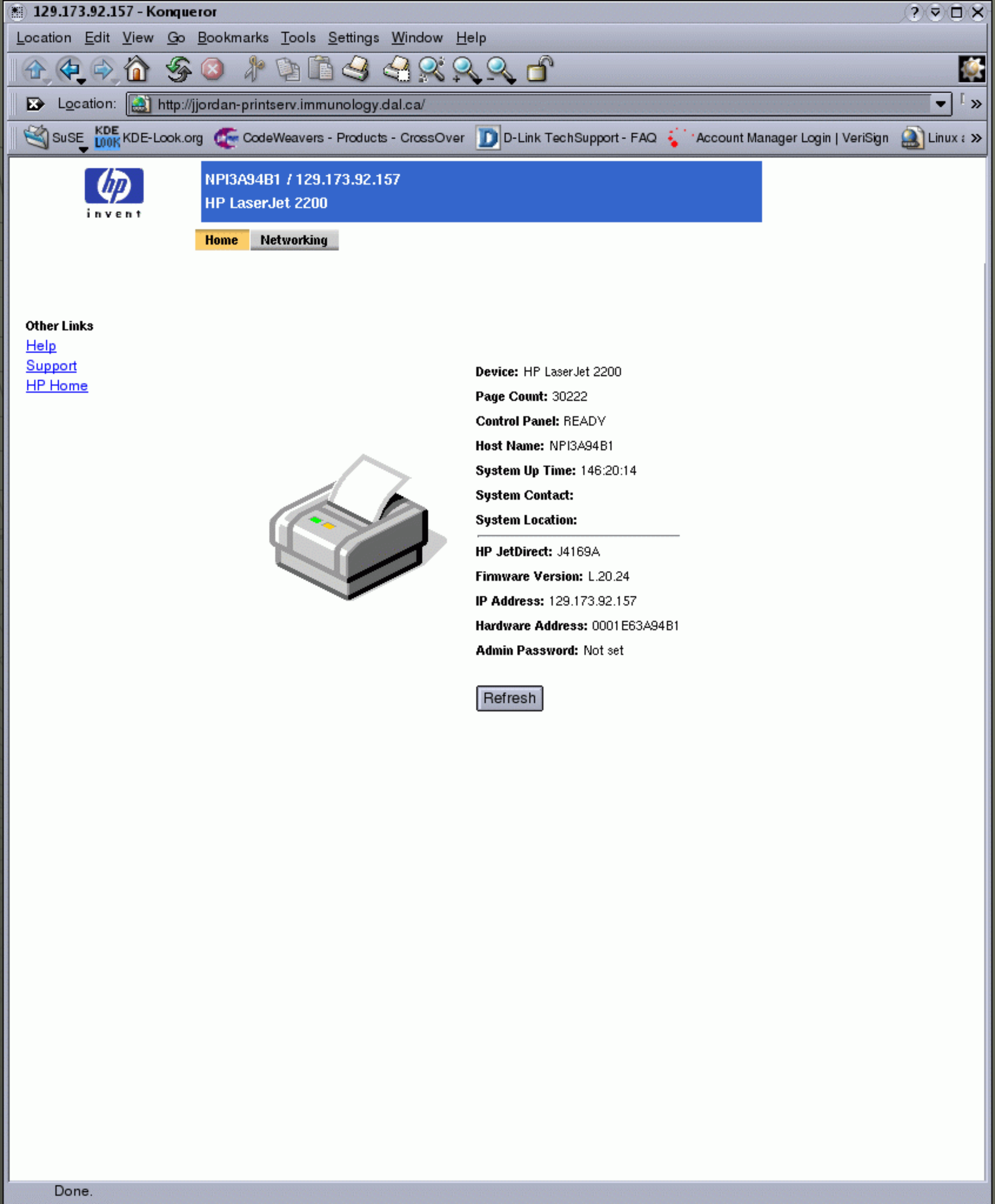
Canada - Agranat-EmWeb Top This Month By Domain By Server

Sites in Canada running Agranat-EmWeb

ariadne.concordia.ca
libr-102-8.concordia.ca
jjordan-printserv.immunology.dal.ca
staffprint.kellogg.dal.ca
dj500.me.dal.ca
mba-office-printer.sba.dal.ca
harper.cs.ualberta.ca
gw-16.cmpe.ubc.ca
minitix.mis.commerce.ubc.ca
gw-147.educ.ubc.ca
gw.mining.ubc.ca
anguhub16.net.ubc.ca
anguhub17.net.ubc.ca
mcgavinhub1.net.ubc.ca
triumf-gw.net.ubc.ca
biotech-3124a.zoology.ubc.ca
frustration.zoology.ubc.ca
minos.zoology.ubc.ca
www.lps.uqam.ca
p13.uqat.ca
sc-gestion-sec.uqat.ca
p13.uqat.uquebec.ca
sc-gestion-sec.uqat.uquebec.ca
hp2200.nal.utoronto.ca
hp2.physics.utoronto.ca
hp22kim.physics.utoronto.ca
engmmprinter1.uwaterloo.ca
engmmprinter2.uwaterloo.ca
ljp-8.uwaterloo.ca
bess-switch.videon.ca

Netcraft Web Server Survey Reports Graphs Mechanics Developers Servers Most Requested Sites Archive

Your comments and suggestions are most welcome webmaster@netcraft.com © Netcraft 2002

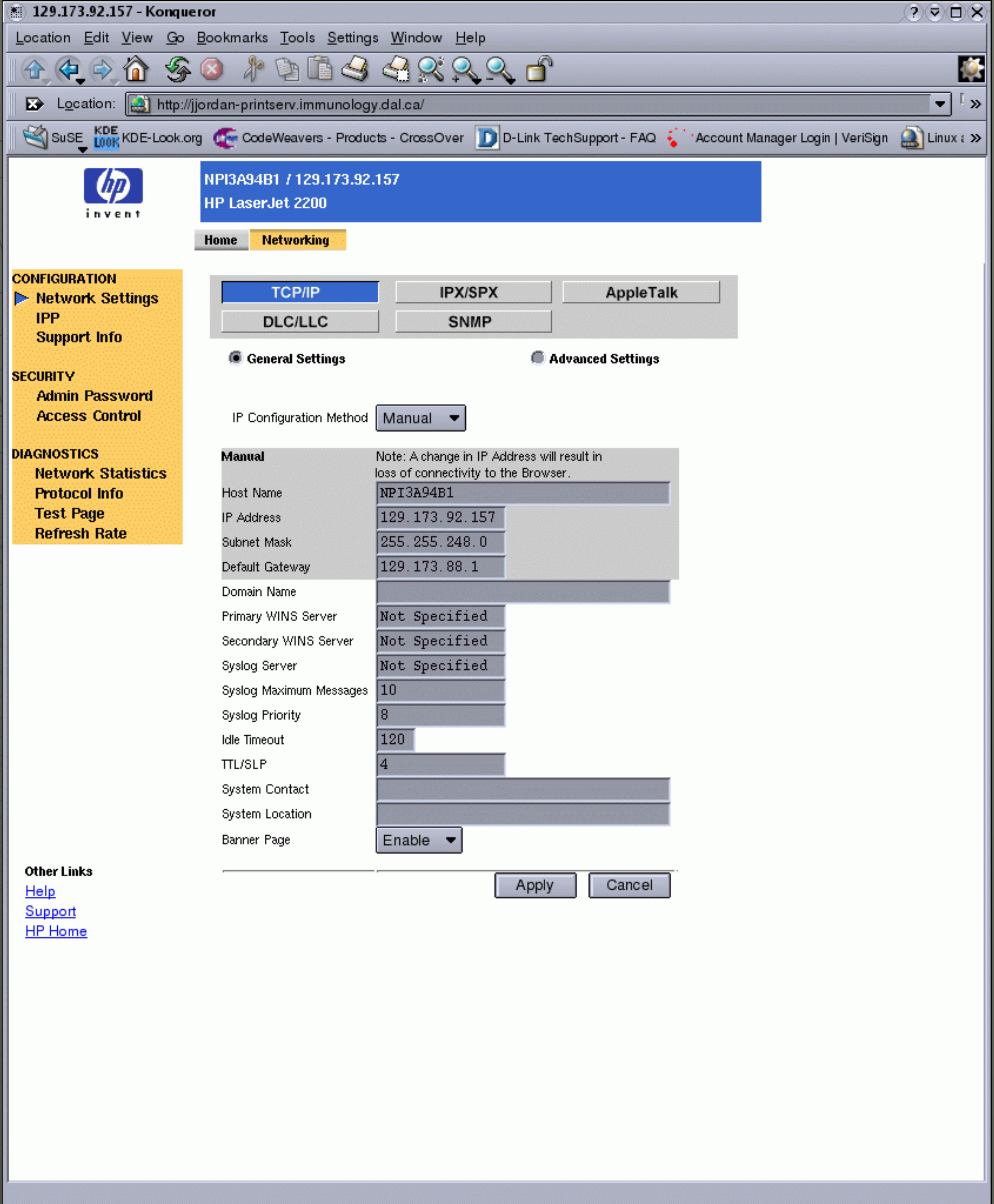

129.173.92.157 - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location: http://jjordan-printserv.immunology.dal.ca/
SuSE
KDE-Look.org
CodeWeavers - Products - CrossOver
D-Link TechSupport - FAQ
Account Manager Login | VeriSign
Linux
invent
Home
Networking
Refresh
Done.

NPI3A94B1 / 129.173.92.157
HP LaserJet 2200

Other Links
Help
Support
HP Home

Device: HP LaserJet 2200
Page Count: 30222
Control Panel: READY
Host Name: NPI3A94B1
System Up Time: 146:20:14
System Contact:
System Location:

HP JetDirect: J4169A
Firmware Version: L.20.24
IP Address: 129.173.92.157
Hardware Address: 0001E63A94B1
Admin Password: Not set



http://jjordan-printserv.immunology.dal.ca/

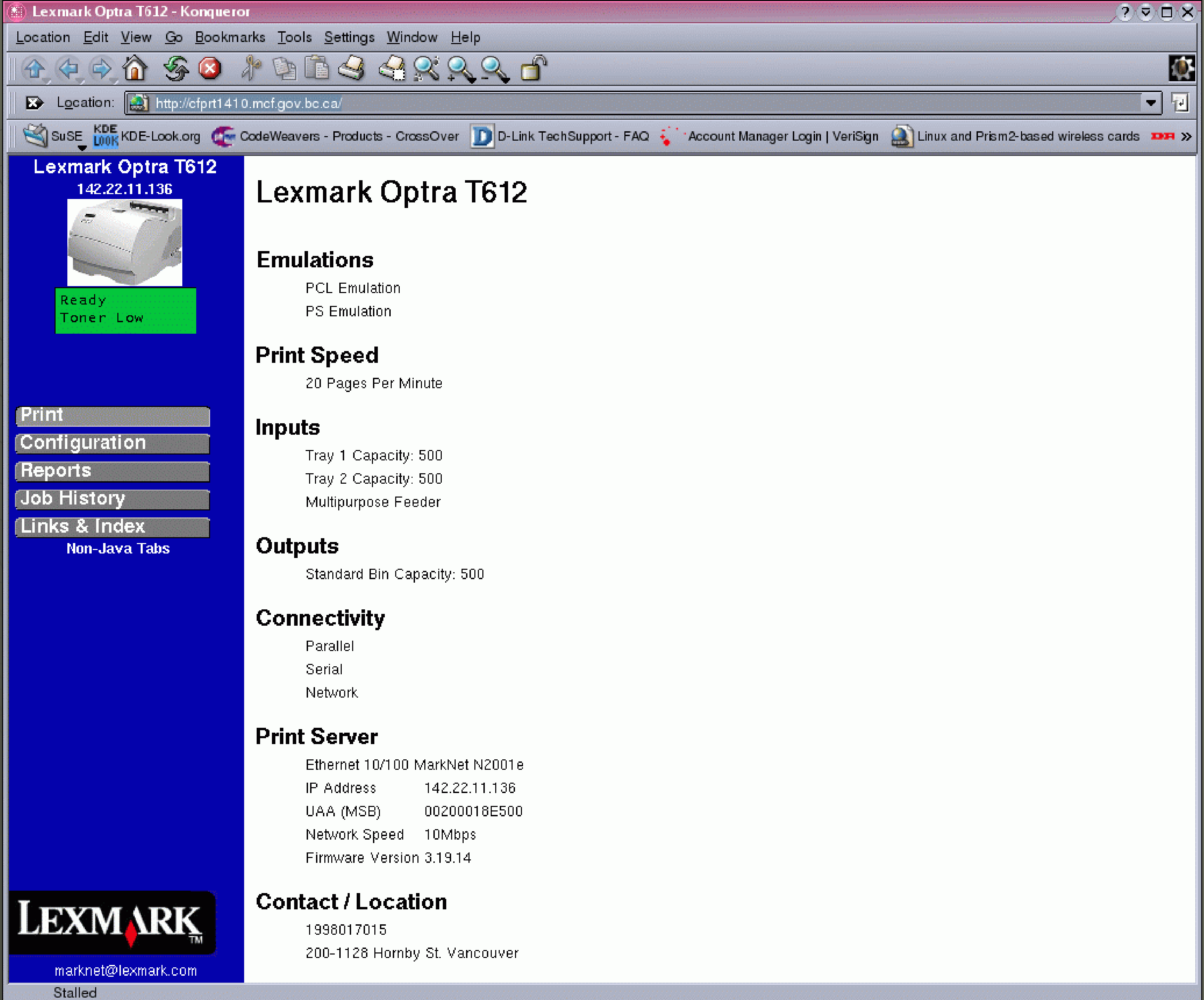
NPI3A94B1 / 129.173.92.157

HP LaserJet 2200

● General Settings ○ Advanced Settings

IP Configuration Method: Manual

Manual	Note: A change in IP Address will result in loss of connectivity to the Browser.
Host Name	NPI3A94B1
IP Address	129.173.92.157
Subnet Mask	255.255.248.0
Default Gateway	129.173.88.1
Domain Name	
Primary WINS Server	Not Specified
Secondary WINS Server	Not Specified
Syslog Server	Not Specified
Syslog Maximum Messages	10
Syslog Priority	8
Idle Timeout	120
TTL/SLP	4
System Contact	
System Location	
Banner Page	Enable


Lexmark Optra T612 - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location: http://cfprt1410.mcf.gov.bc.ca/
SuSE
KDE-Look.org
CodeWeavers - Products - CrossOver
D-Link TechSupport - FAQ
Account Manager Login | VeriSign
Linux and Prism2-based wireless cards
Print
Configuration
Reports
Job History
Links & Index
Non-Java Tabs
LEXMARK
Stalled

Lexmark Optra T612
142.22.11.136

Ready
Toner Low

marknet@lexmark.com

Lexmark Optra T612

Emulations

PCL Emulation

PS Emulation

Print Speed

20 Pages Per Minute

Inputs

Tray 1 Capacity: 500

Tray 2 Capacity: 500

Multipurpose Feeder

Outputs

Standard Bin Capacity: 500

Connectivity

Parallel

Serial

Network

Print Server

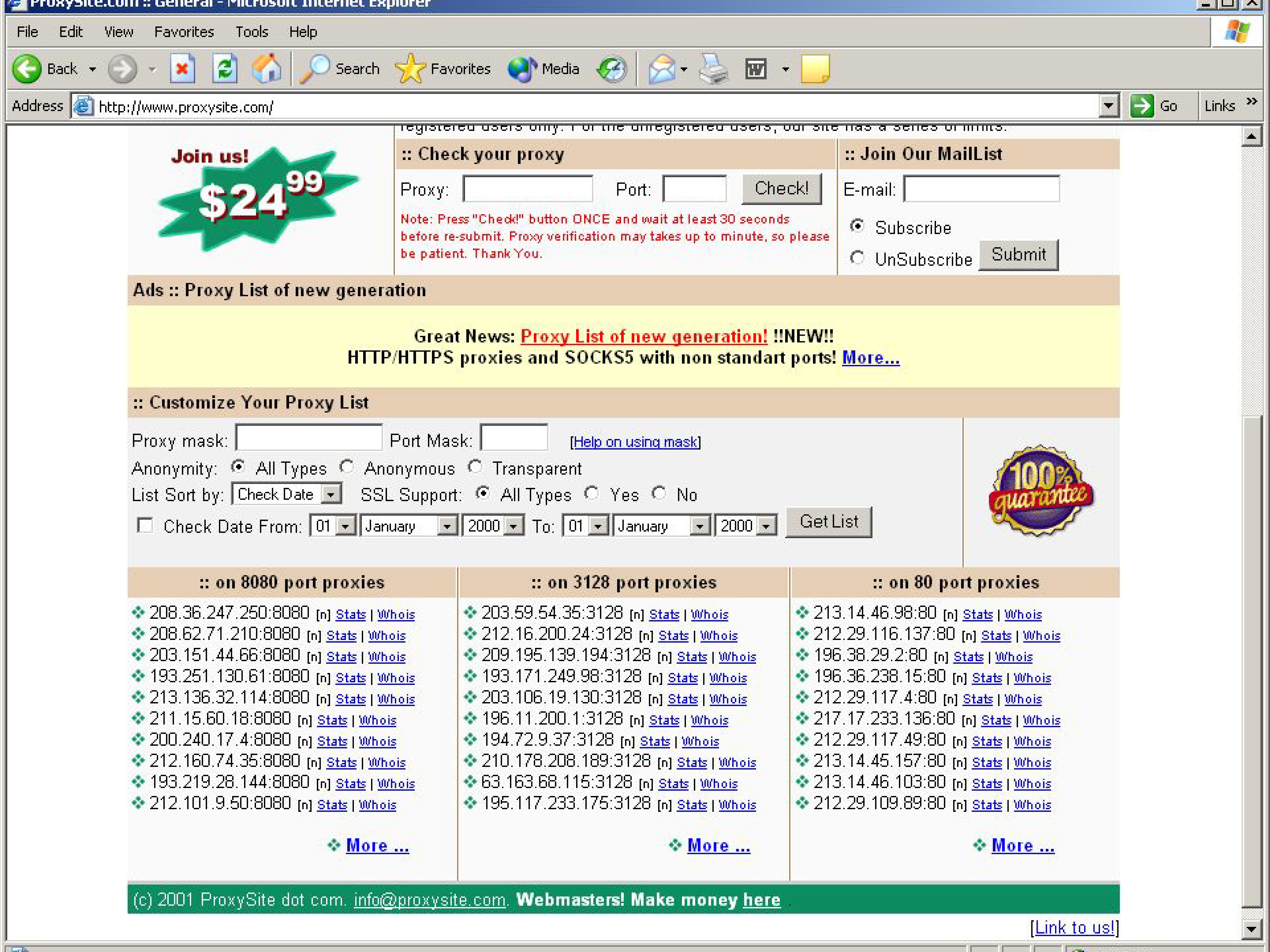
Ethernet 10/100 MarkNet N2001e

IP Address	142.22.11.136
UAA (MSB)	00200018E500
Network Speed	10Mbps
Firmware Version	3.19.14

Contact / Location

1998017015

200-1128 Hornby St. Vancouver


ProxySite.com :: General - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://www.proxysite.com/
Go
Links

registered users only. For the unregistered users, our site has a series of limits.

:: Check your proxy

Proxy: ______ Port: ______ Check!

Note: Press "Check!" button ONCE and wait at least 30 seconds before re-submit. Proxy verification may takes up to minute, so please be patient. Thank You.

:: Join Our MailList

E-mail: ______

● Subscribe

○ UnSubscribe Submit

:: Customize Your Proxy List

Proxy mask: ______ Port Mask: ______ [Help on using mask]

Anonymity: ● All Types ○ Anonymous ○ Transparent

List Sort by: Check Date SSL Support: ● All Types ○ Yes ○ No

□ Check Date From: 01 January 2000 To: 01 January 2000 Get List

:: on 8080 port proxies

- 208.36.247.250:8080 [n] Stats | Whois
- 208.62.71.210:8080 [n] Stats | Whois
- 203.151.44.66:8080 [n] Stats | Whois
- 193.251.130.61:8080 [n] Stats | Whois
- 213.136.32.114:8080 [n] Stats | Whois
- 211.15.60.18:8080 [n] Stats | Whois
- 200.240.17.4:8080 [n] Stats | Whois
- 212.160.74.35:8080 [n] Stats | Whois
- 193.219.28.144:8080 [n] Stats | Whois
- 212.101.9.50:8080 [n] Stats | Whois

More ...

:: on 3128 port proxies

- 203.59.54.35:3128 [n] Stats | Whois
- 212.16.200.24:3128 [n] Stats | Whois
- 209.195.139.194:3128 [n] Stats | Whois
- 193.171.249.98:3128 [n] Stats | Whois
- 203.106.19.130:3128 [n] Stats | Whois
- 196.11.200.1:3128 [n] Stats | Whois
- 194.72.9.37:3128 [n] Stats | Whois
- 210.178.208.189:3128 [n] Stats | Whois
- 63.163.68.115:3128 [n] Stats | Whois
- 195.117.233.175:3128 [n] Stats | Whois

More ...

:: on 80 port proxies

- 213.14.46.98:80 [n] Stats | Whois
- 212.29.116.137:80 [n] Stats | Whois
- 196.38.29.2:80 [n] Stats | Whois
- 196.36.238.15:80 [n] Stats | Whois
- 212.29.117.4:80 [n] Stats | Whois
- 217.17.233.136:80 [n] Stats | Whois
- 212.29.117.49:80 [n] Stats | Whois
- 213.14.45.157:80 [n] Stats | Whois
- 213.14.46.103:80 [n] Stats | Whois
- 212.29.109.89:80 [n] Stats | Whois

More ...

(c) 2001 ProxySite dot com. info@proxysite.com. Webmasters! Make money here .

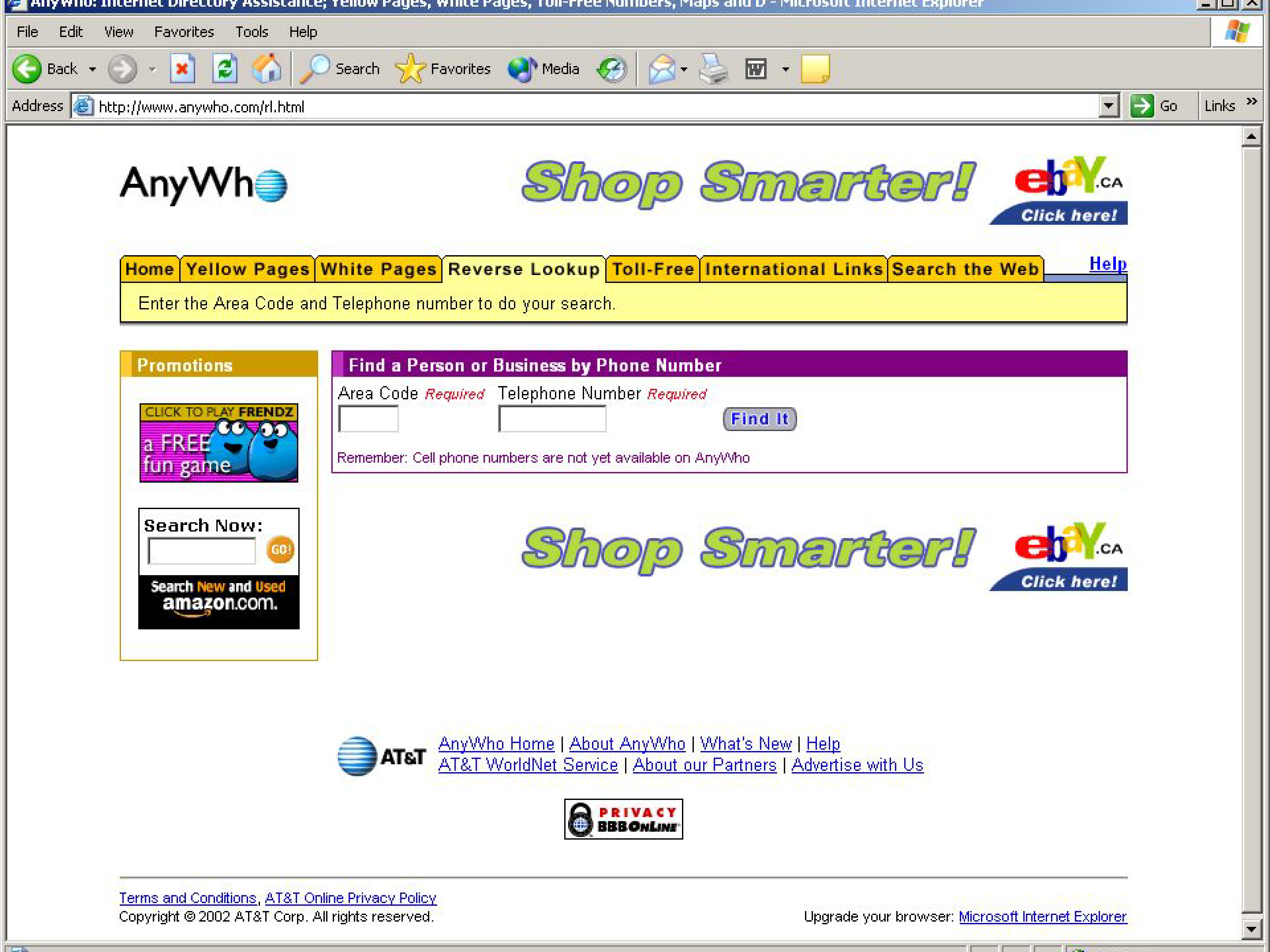
[Link to us!]

Reconnaissance

- We’ve seen a glimpse of various back doors available to web browsers
- Let’s turn the tables now, and talk much closer to home
- How much personal detail do we put online for all to see?

Reconaissance

- Web surfing habits
- Cookies
- Resumes
- Web site histories (www.archive.org)
- News group posts
- Friends
- Relatives
- School archives
- Maps



Address: http://www.anywho.com/rl.html

Enter the Area Code and Telephone number to do your search.

Promotions

Find a Person or Business by Phone Number

Area Code *Required* Telephone Number *Required*

Find It

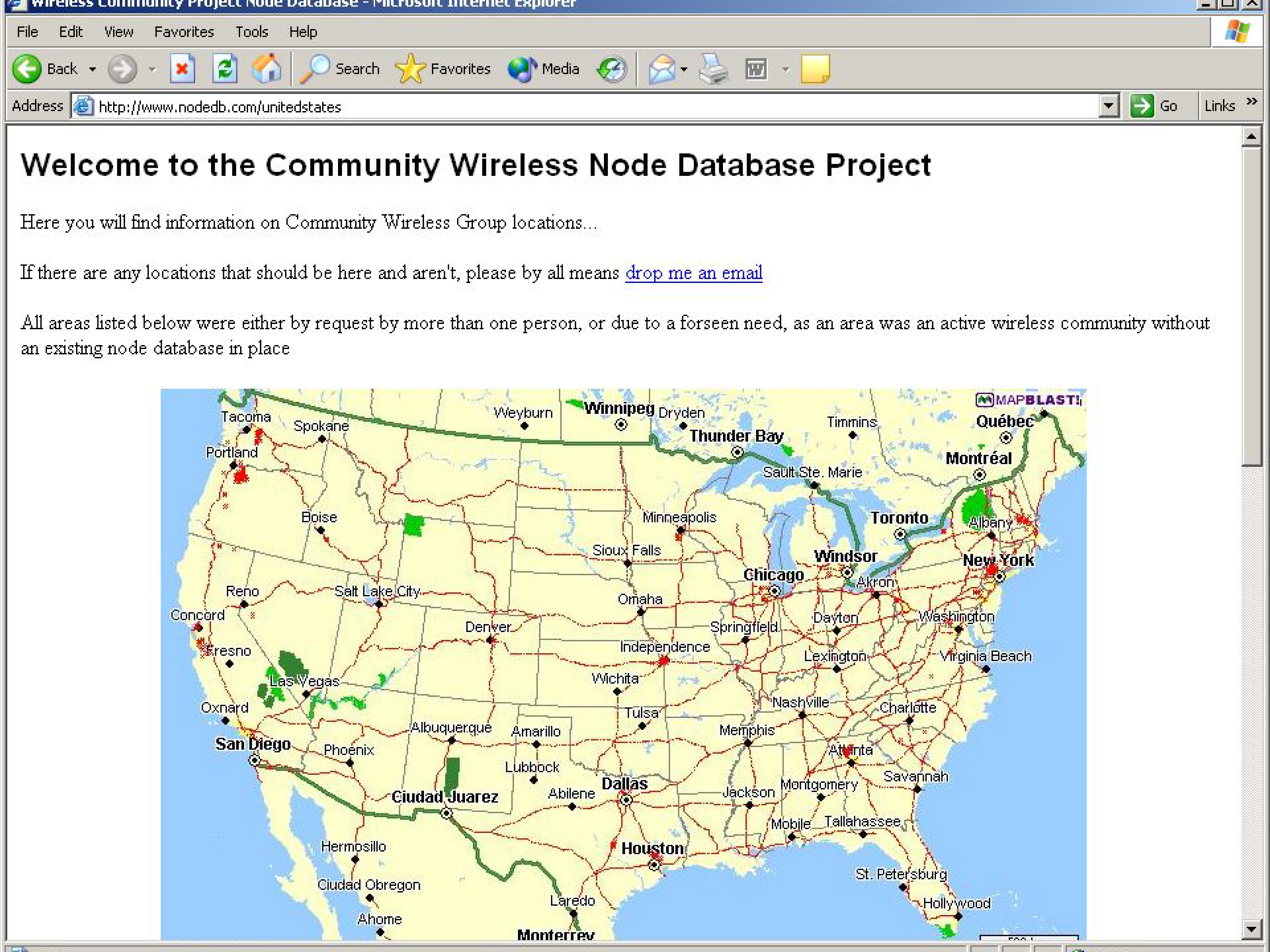
Remember: Cell phone numbers are not yet available on AnyWho

AT&T AnyWho Home | About AnyWho | What's New | Help
AT&T WorldNet Service | About our Partners | Advertise with Us

PRIVACY BBBOnLine

Terms and Conditions, AT&T Online Privacy Policy

Upgrade your browser: Microsoft Internet Explorer


Wireless Community Project Node Database - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Go
Links

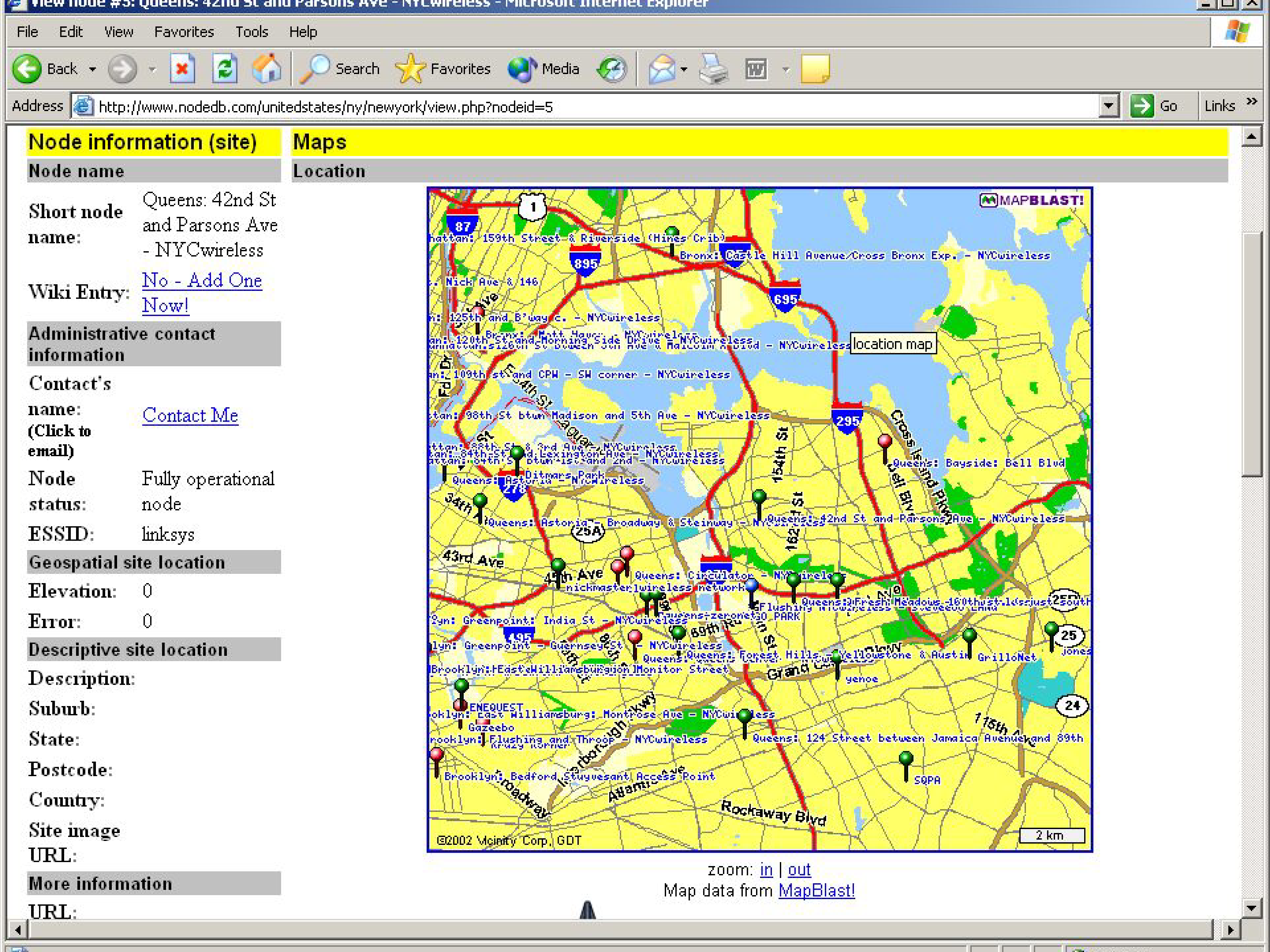
Address http://www.nodedb.com/unitedstates

Welcome to the Community Wireless Node Database Project

Here you will find information on Community Wireless Group locations...

If there are any locations that should be here and aren't, please by all means drop me an email

All areas listed below were either by request by more than one person, or due to a forseen need, as an area was an active wireless community without an existing node database in place



View node #5: Queens: 42nd St and Parsons Ave - NYCwireless - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://www.nodedb.com/unitedstates/ny/newyork/view.php?nodeid=5
Go
Links

Node information (site)

Node name

Short node name:	Queens: 42nd St and Parsons Ave - NYCwireless
Wiki Entry:	No - Add One Now!

Administrative contact information

Contact's name: **(Click to email)**	Contact Me
Node status:	Fully operational node
ESSID:	linksys

Geospatial site location

Elevation:	0
Error:	0

Descriptive site location

Description:	
Suburb:	
State:	
Postcode:	
Country:	
Site image URL:	

More information

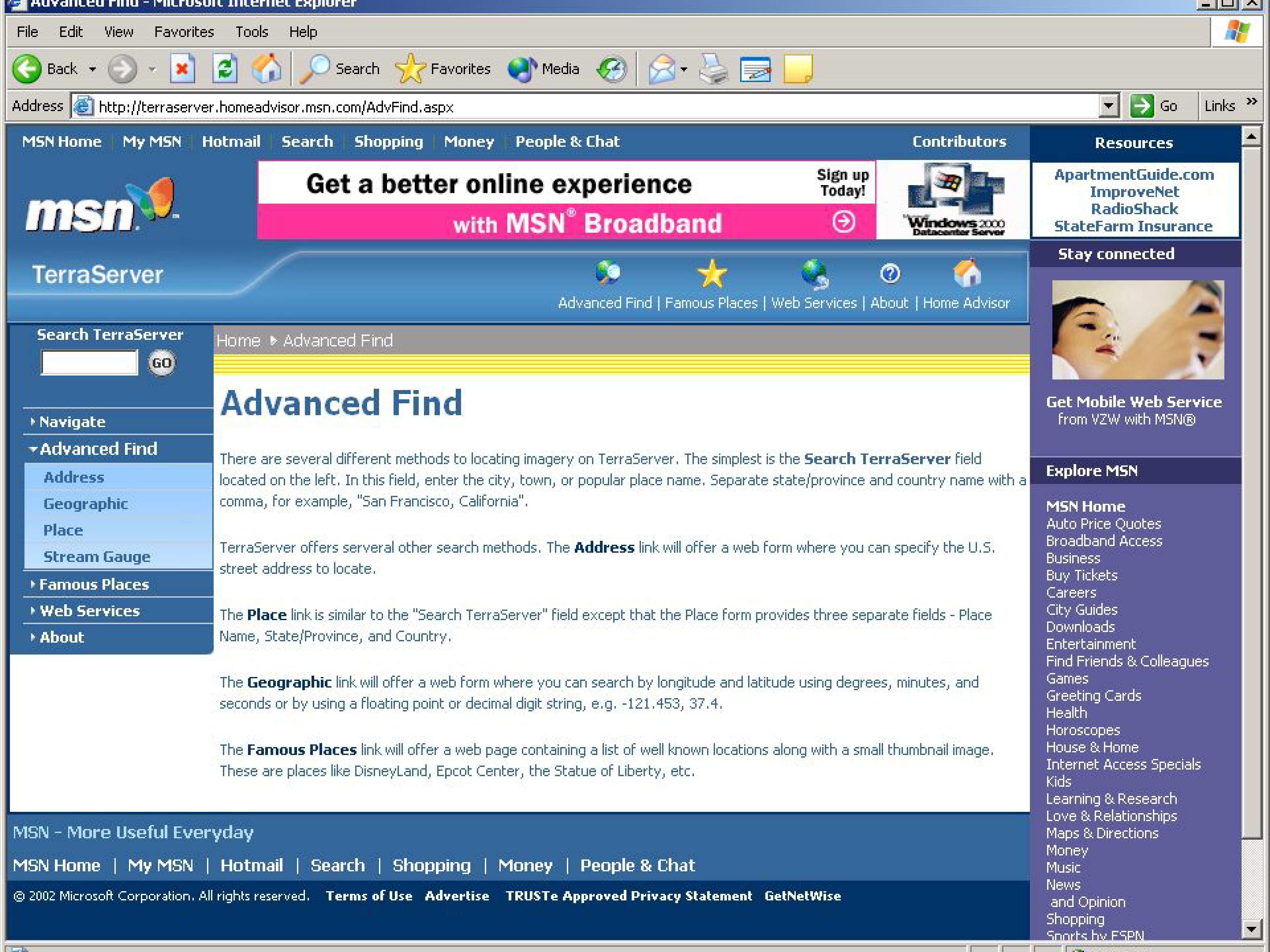
URL:

Maps

Location

MAPBLAST!
location map
87
895
695
295
1
278
25A
25
24
Manhattan: 159th Street & Riverside (Hines Crib)
Bronx: Castle Hill Avenue/Cross Bronx Exp. - NYCwireless
St. Nick Ave & 146
Manhattan: 125th and B'way c. - NYCwireless
Bronx: Mott Haven - NYCwireless
Manhattan: 120th St and Morningside Drive - NYCwireless
Manhattan: 120th St btween 5th Ave & Malcolm X Blvd - NYCwireless
Manhattan: 109th st and CPW - SW corner - NYCwireless
Manhattan: 98th St btwn Madison and 5th Ave - NYCwireless
Manhattan: 88th St & 3rd Ave - NYCwireless
Manhattan: 84th St and Lexington Ave - NYCwireless
Manhattan: 84th St btwn 1st and 2nd - NYCwireless
Queens: Astoria Ditmars Park - NYCwireless
Queens: Astoria - Broadway & Steinway - NYCwireless
Queens: 42nd St and Parsons Ave - NYCwireless
Queens: Bayside: Bell Blvd
Queens: Circulator - NYCwireless
nickmaster1wireless network
Flushing NYCwireless
Queens: Fresh Meadows 160th st.ldsjust2south
Brooklyn: Greenpoint: India St - NYCwireless
Brooklyn: Greenpoint - Guernsey St - NYCwireless
Queens-zeronet
Brooklyn: East Williamsburg: Monitor Street
Queens: Forest Hills - Yellowstone & Austin
GrilloNet
yenoe
ENEQUEST
Brooklyn: East Williamsburg: Montrose Ave - NYCwireless
Gazeebo
Brooklyn: Flushing and Throop - NYCwireless
Krazy Korner
Queens: 124 Street between Jamaica Avenue and 89th
Brooklyn: Bedford Stuyvesant Access Point
SQPA
jones
Cross Island Pkwy
Bell Blvd
154th St
162 St
34th St
43rd Ave
45th Ave
69th Rd
Grand Central
Jackie Robinson Pkwy
Broadway
Atlantic Ave
Rockaway Blvd
115th Ave
Union Tpke
©2002 Vicinity Corp., GDT
2 km

zoom: in | out
Map data from MapBlast!



Advanced Find

There are several different methods to locating imagery on TerraServer. The simplest is the **Search TerraServer** field located on the left. In this field, enter the city, town, or popular place name. Separate state/province and country name with a comma, for example, "San Francisco, California".

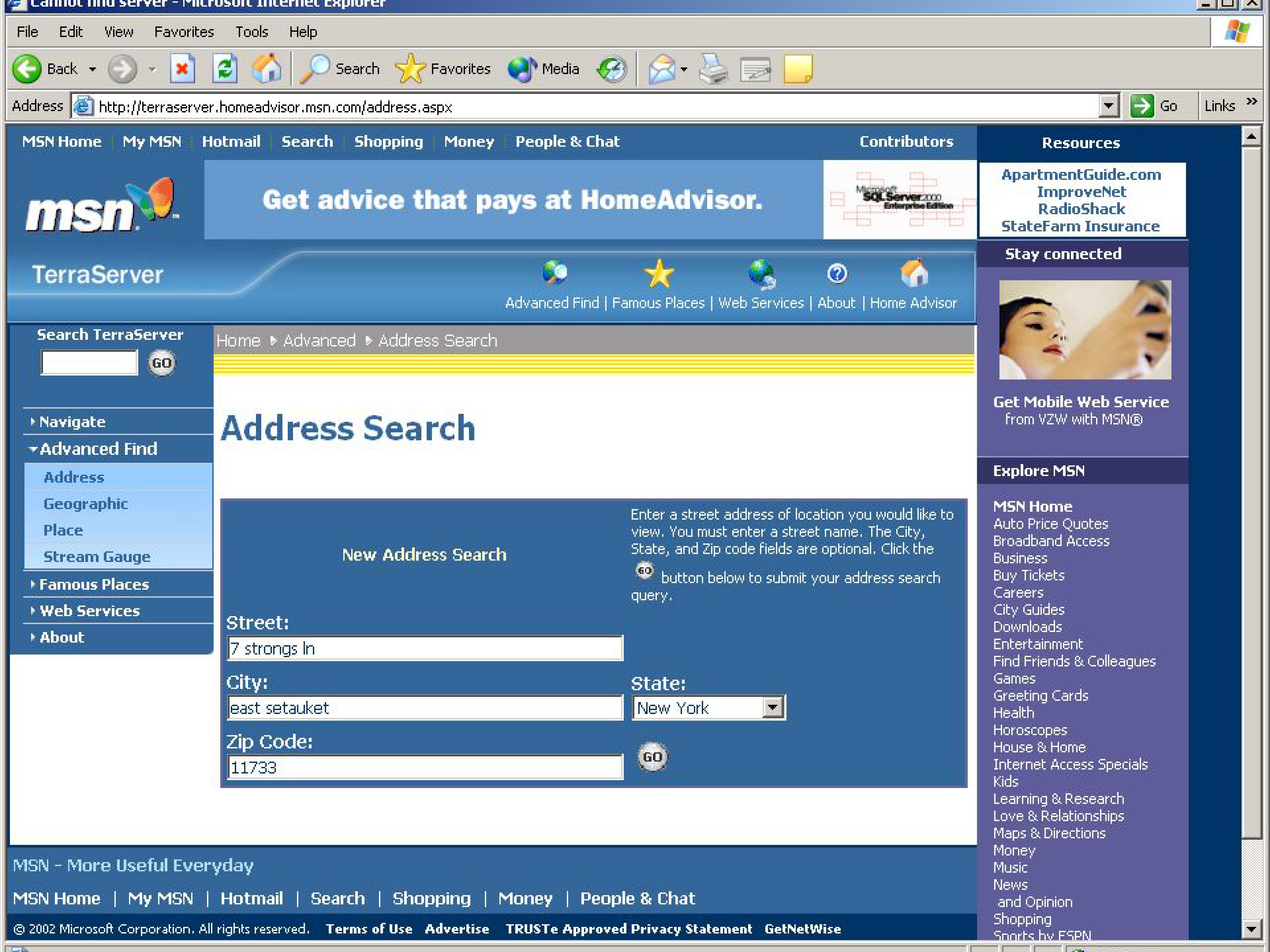
TerraServer offers serveral other search methods. The **Address** link will offer a web form where you can specify the U.S. street address to locate.

The **Place** link is similar to the "Search TerraServer" field except that the Place form provides three separate fields - Place Name, State/Province, and Country.

The **Geographic** link will offer a web form where you can search by longitude and latitude using degrees, minutes, and seconds or by using a floating point or decimal digit string, e.g. -121.453, 37.4.

The **Famous Places** link will offer a web page containing a list of well known locations along with a small thumbnail image. These are places like DisneyLand, Epcot Center, the Statue of Liberty, etc.

© 2002 Microsoft Corporation. All rights reserved.



Address Search

New Address Search

Enter a street address of location you would like to view. You must enter a street name. The City, State, and Zip code fields are optional. Click the GO button below to submit your address search query.

Street: 7 strongs ln

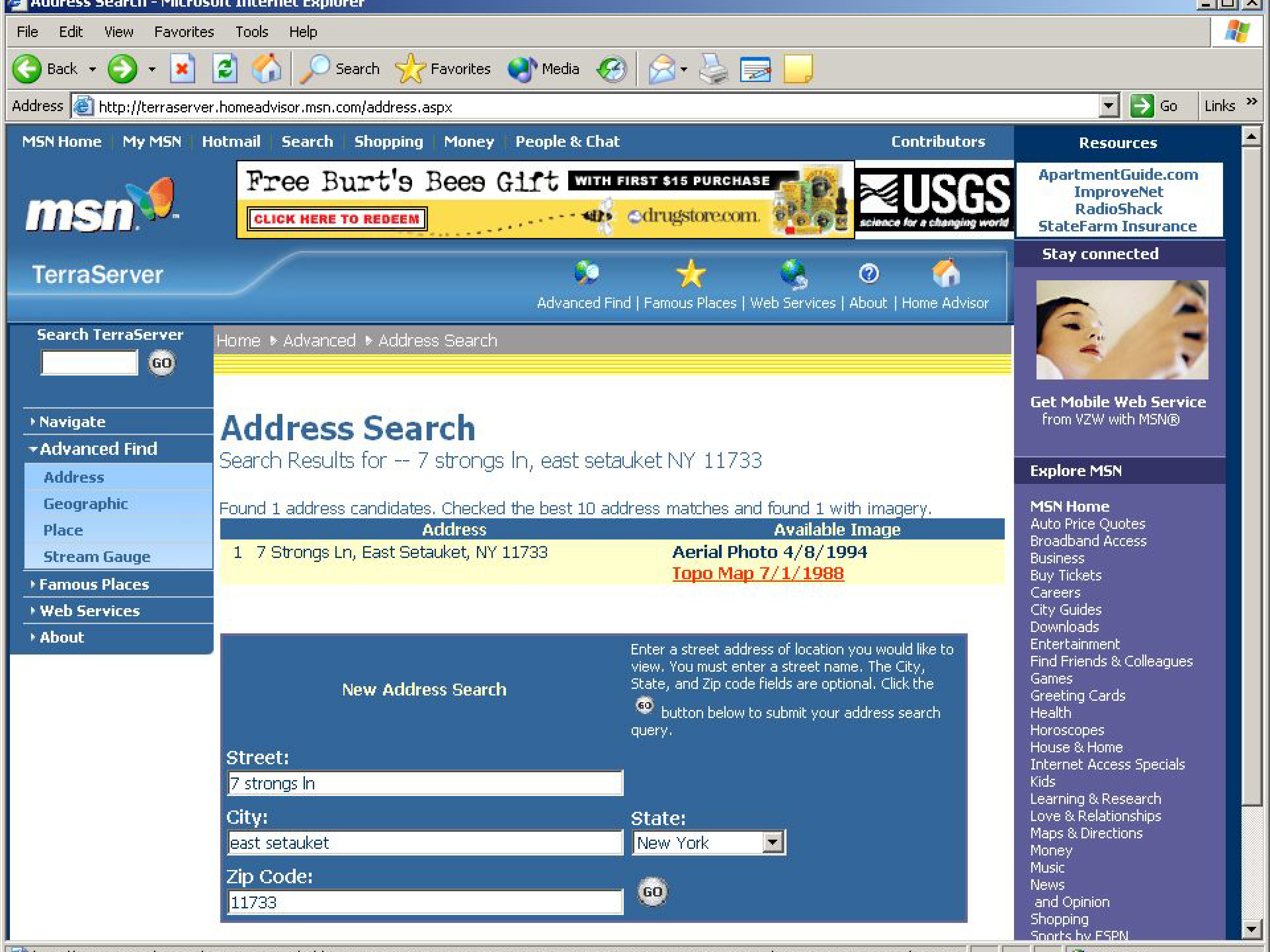
City: east setauket

State: New York

Zip Code: 11733

GO

MSN - More Useful Everyday
MSN Home | My MSN | Hotmail | Search | Shopping | Money | People & Chat



Address Search

Search Results for -- 7 strongs ln, east setauket NY 11733

Found 1 address candidates. Checked the best 10 address matches and found 1 with imagery.

	Address	Available Image
1	7 Strongs Ln, East Setauket, NY 11733	Aerial Photo 4/8/1994 Topo Map 7/1/1988

New Address Search

Enter a street address of location you would like to view. You must enter a street name. The City, State, and Zip code fields are optional. Click the GO button below to submit your address search query.

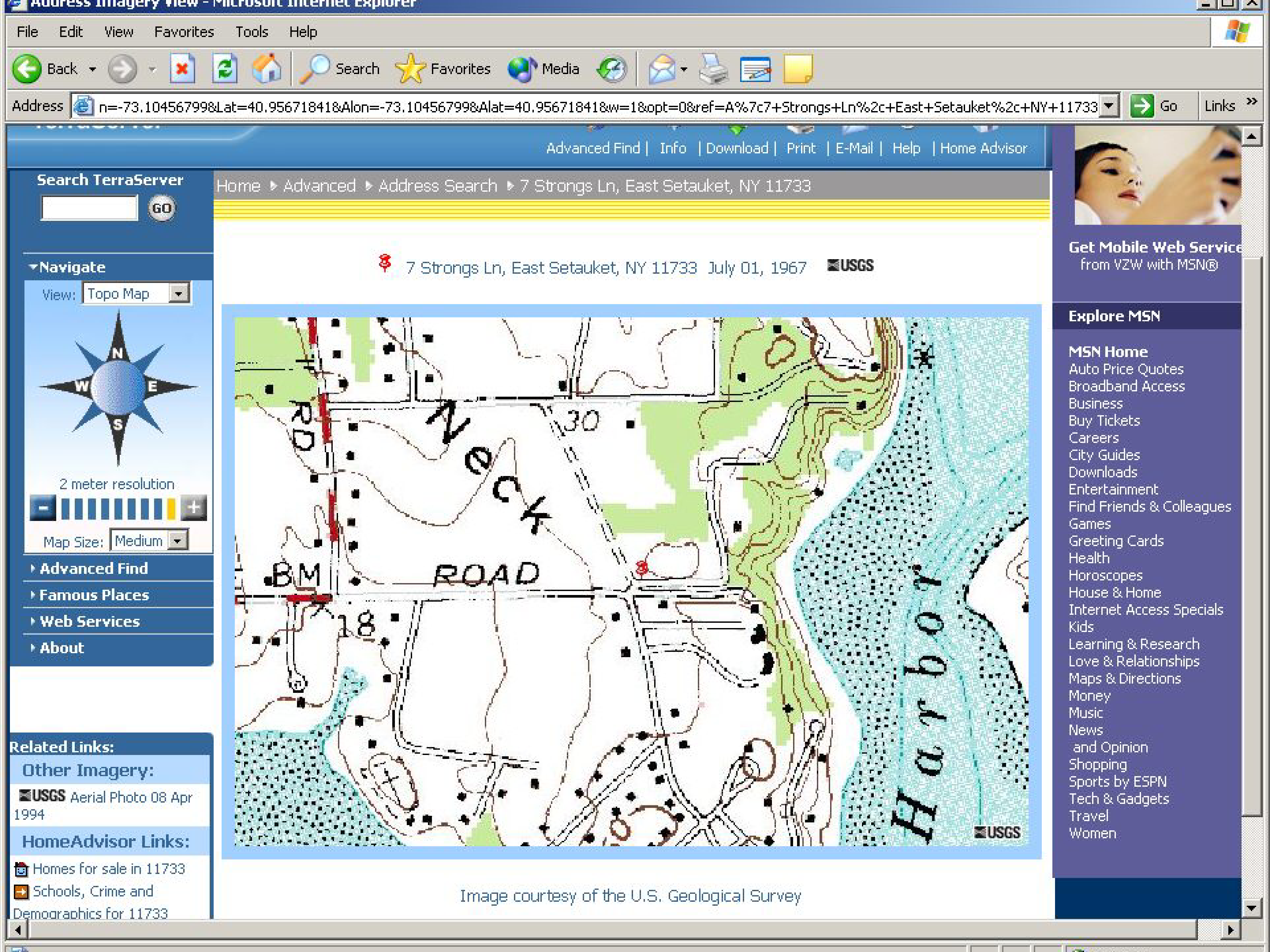
Street: 7 strongs ln

City: east setauket

State: New York

Zip Code: 11733

GO



Address Imagery View - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links

n=-73.10456799&Lat=40.95671841&Alon=-73.10456799&Alat=40.95671841&w=1&opt=0&ref=A%7c7+Strongs+Ln%2c+East+Setauket%2c+NY+11733

Advanced Find | Info | Download | Print | E-Mail | Help | Home Advisor
Search TerraServer
GO
Navigate
N
W
E
S
Advanced Find
Famous Places
Web Services
About

View: Topo Map

2 meter resolution

Map Size: Medium

Home ▸ Advanced ▸ Address Search ▸ 7 Strongs Ln, East Setauket, NY 11733

7 Strongs Ln, East Setauket, NY 11733 July 01, 1967 USGS

RD
Neck
ROAD
BM
30
18
Harbor
USGS

Image courtesy of the U.S. Geological Survey

Related Links:

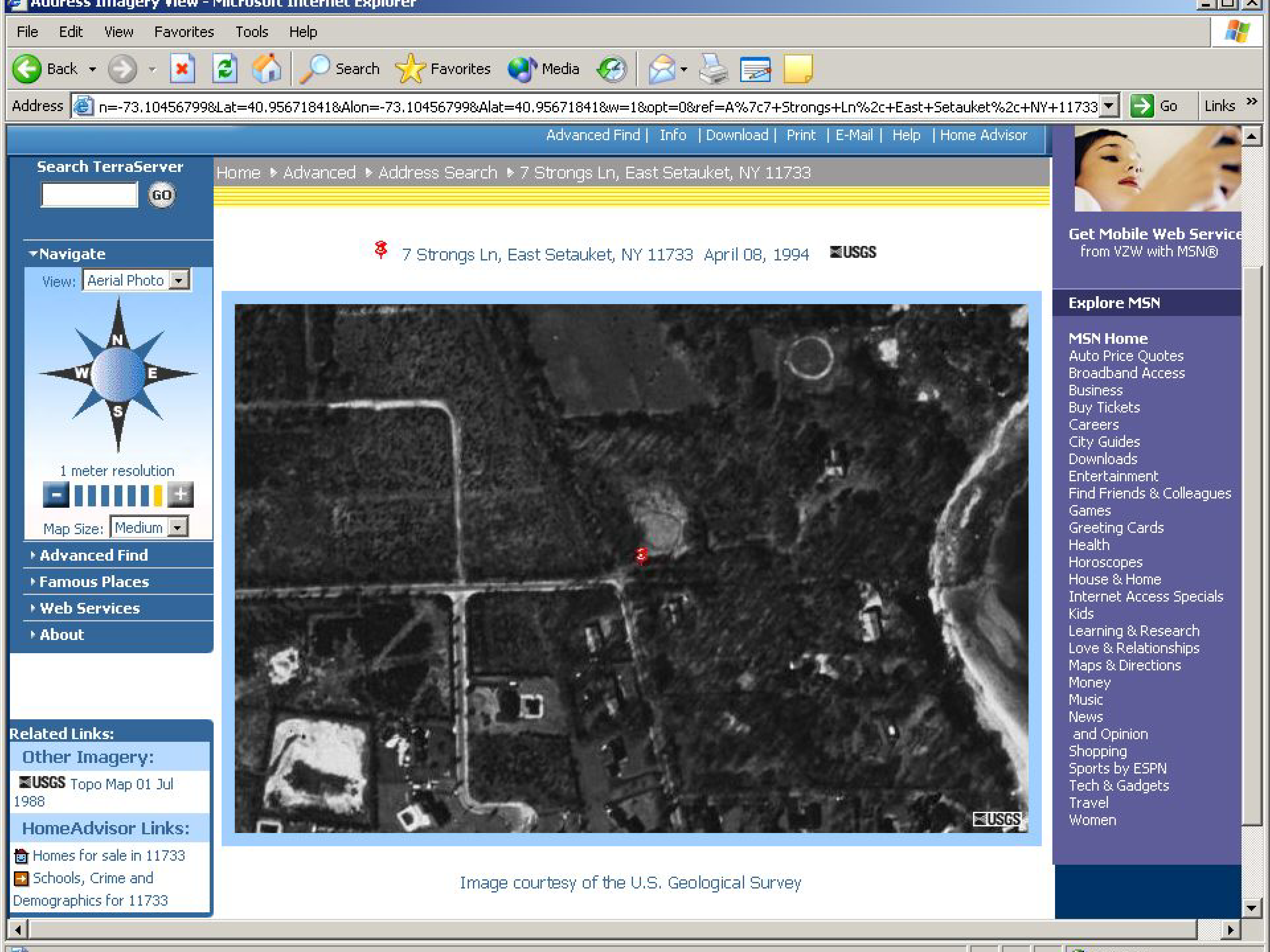
Other Imagery:

USGS Aerial Photo 08 Apr 1994

HomeAdvisor Links:

Homes for sale in 11733

Schools, Crime and Demographics for 11733



n=-73.10456799&Lat=40.95671841&Alon=-73.10456799&Alat=40.95671841&w=1&opt=0&ref=A%7c7+Strongs+Ln%2c+East+Setauket%2c+NY+11733

Home ▸ Advanced ▸ Address Search ▸ 7 Strongs Ln, East Setauket, NY 11733

7 Strongs Ln, East Setauket, NY 11733 April 08, 1994 USGS

Image courtesy of the U.S. Geological Survey

Related Links:

Other Imagery:

USGS Topo Map 01 Jul 1988

HomeAdvisor Links:

Homes for sale in 11733

Schools, Crime and Demographics for 11733

Final Thoughts

- We have shown a few ways that a web browser can be used to gather huge amounts of target information, and a few ways the web browser can be used to exploit trivial vulnerabilities
- There are many more online services like the ones pointed out in this presentation
- It is easy to collect and analyze this information to produce thorough profiles

Thank You

Karsten Johansson

KSAJ Inc.

www.PENETRATIONTEST.com