



Ethical Hacking and Countermeasures

Version 6



Module III

Footprinting

Mason is fuming with anger! The notebook which he had ordered online from *Xmachi Inc.*, did not have the configuration that he had requested.

When contacted, the customer care department gave a cold response. Vengeance crept into his mind. Finally he decided to teach the notebook manufacturer a lesson.

Being a Network Administrator of his firm, he knew exactly what he was supposed to do.

What will Mason do to defame the notebook manufacturer?

What information will Mason need to achieve his goal?

Reports Says FBI Misused Information-Gathering Power

BY DAN EGGEN - The Washington Post
March 14, 2008
URL: <http://www2.nysun.com/article/72916>

WASHINGTON — The FBI continued to improperly obtain private telephone, e-mail, and financial records five years after it was granted expanded powers under the USA Patriot Act, according to a report issued yesterday.

In a review focusing on FBI investigations in 2006, the Justice Department inspector general, Glenn Fine, found numerous privacy breaches by the bureau in its use of national security letters, which allowed the FBI to obtain personal information on Americans and foreigners without approval from a judge. The findings mirror a report issued by Mr. Fine's office last year, which concluded that the FBI had improperly used the letters to obtain telephone logs, banking records, and other personal data between 2003 and 2005.

The pattern persisted in 2006, Mr. Fine concluded in the report issued yesterday, in part because the FBI had not yet halted the shoddy record-keeping, poor oversight, and other practices that contributed to the problems.

"The FBI and Department of Justice have shown a commitment to addressing these problems," Mr. Fine said in a statement. "However, several of the FBI's and the Department's corrective measures are not yet fully implemented, and it is too early to determine whether these measures will eliminate the problems with the use of these authorities."

Source: <http://www2.nysun.com/>

Threat Chaos

March 20th, 2007

Competitive intelligence gathering

Posted by Richard Stiennon @ 2:12 pm

Categories: Data Security, Trade Shows

Tags:



The world of CI (competitive intelligence) spans the spectrum from analytical data gathering to seamy shoulder surfing and of course the use of custom Trojan horses. This article in *Forbes* describes how you can get insight into a company's future product plans by researching their job postings. In this case it turns out that Google is looking to hire the kinds of talent that would be needed to develop a GooglePhone (g-phone?).

The company's own job listings, for instance, have allowed Google watchers and followers to spot advance signs of everything from its online office suite to a possible foray into the travel business.

You certainly cannot fault someone for perusing publicly available information to glean tidbits like this. While the CI work of several Israeli companies who hired Private Investigators to install Trojan horses on competitors' computers to steal files is reprehensible.

I was reminded of the practices of at least one of the Big Four auditing firms when I overheard a conversation between three obvious consulting types getting on the plane to San Francisco last night. They mentioned their own firm, a client, and the size of a deal they just won

Source: <http://blogs.zdnet.com/>

Module Objective

This module will familiarize you with:

Overview of the Reconnaissance Phase

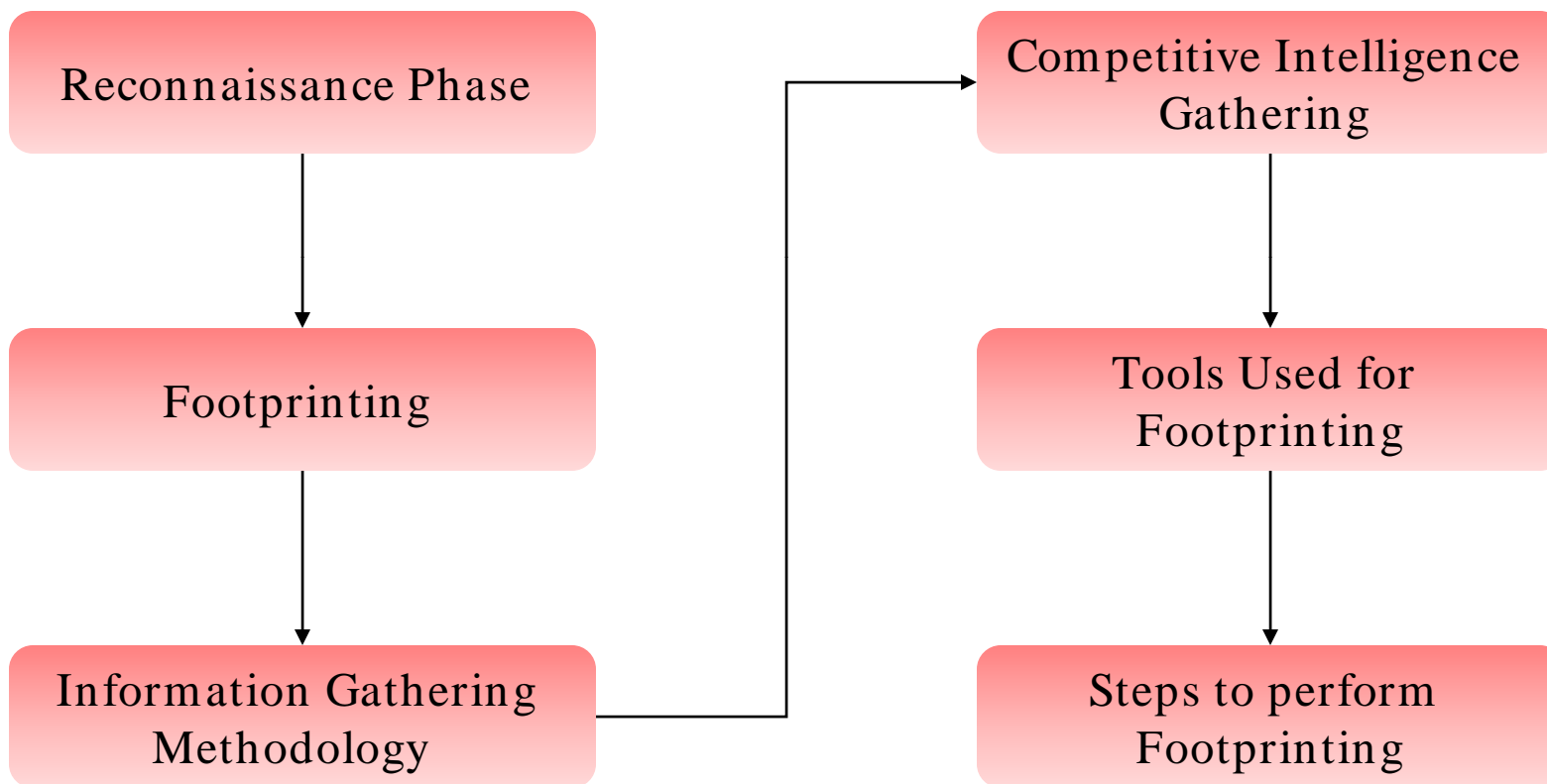
Footprinting: An Introduction

Information Gathering Methodology of Hackers

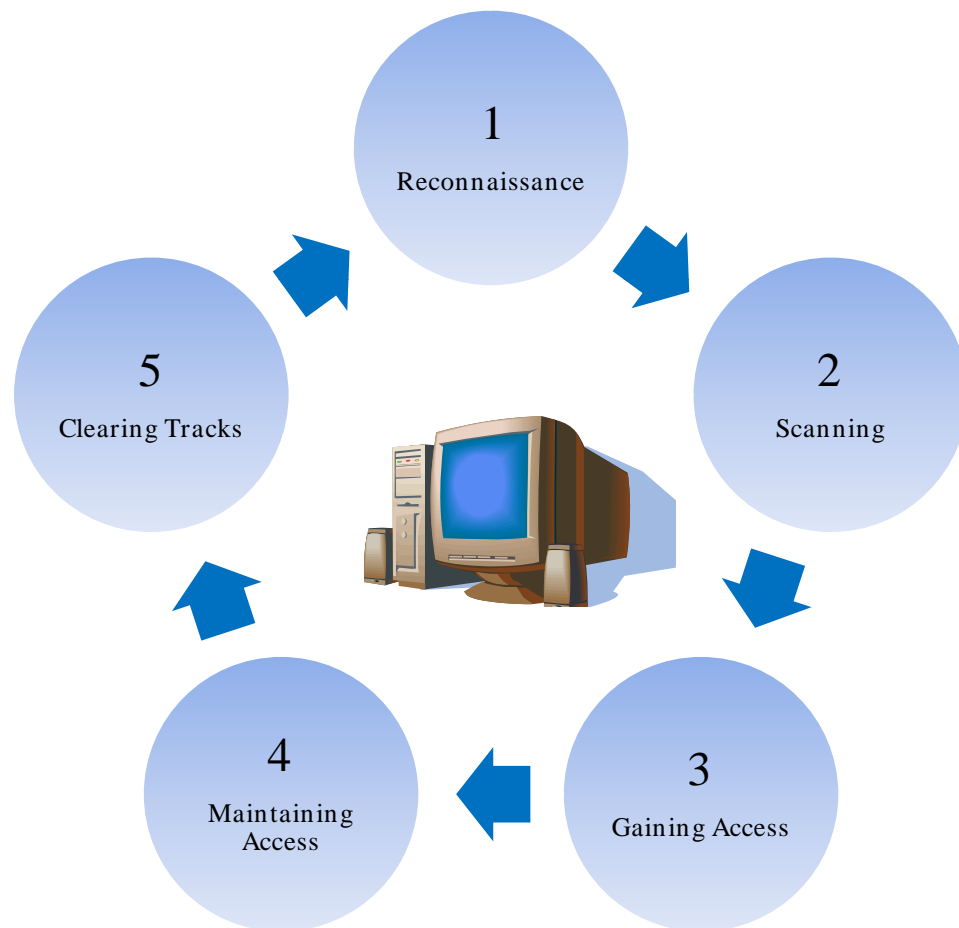
Competitive Intelligence gathering

Tools that aid in Footprinting

Footprinting steps



Revisiting Reconnaissance



Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack

It involves network scanning, either external or internal, without authorization

Defining Footprinting

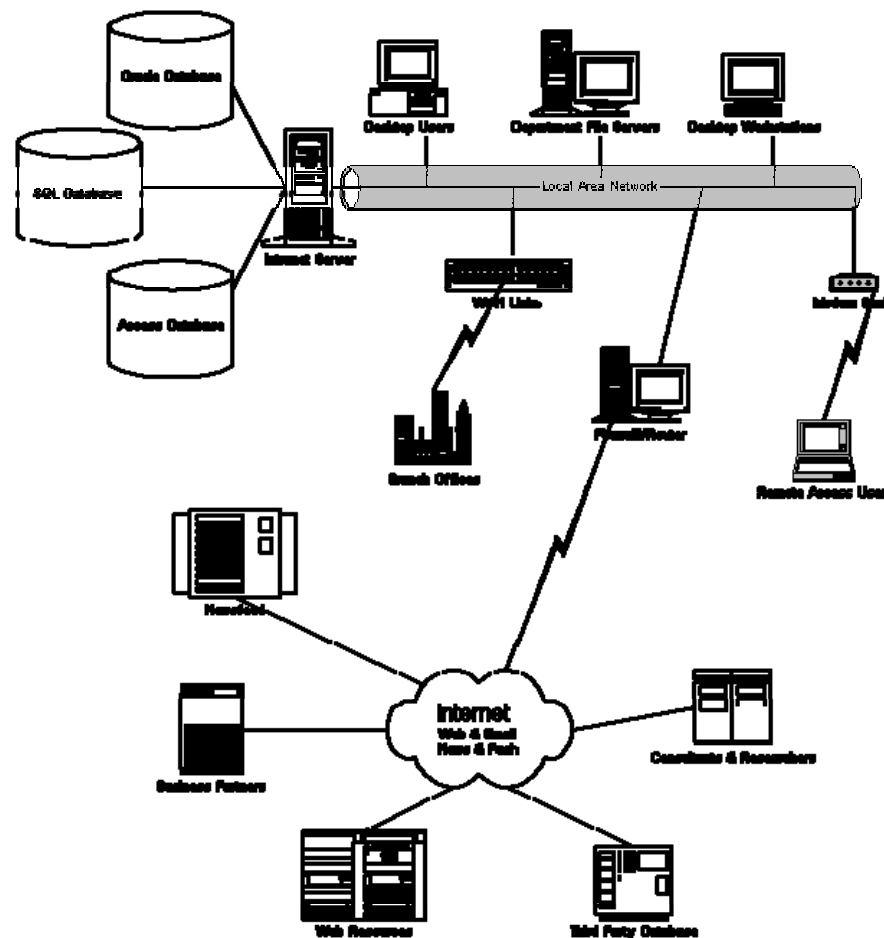


Footprinting is the blueprint of the security profile of an organization, undertaken in a methodological manner

Footprinting is one of the three pre-attack phases

An attacker spends 90% of the time in profiling an organization and another 10% in launching the attack

Footprinting results in a unique organization profile with respect to networks (Internet/intranet/extranet/wireless) and systems involved



Why is Footprinting Necessary

Footprinting is necessary to systematically and methodically ensure that all pieces of information related to the aforementioned technologies are identified

Footprinting is often the most difficult task to determine the security posture of an entity



Areas and Information which Attackers Seek

Internet

- Domain Name
- Network blocks
- IP addresses of reachable systems
- TCP and UDP services running
- System architecture
- ACLs
- IDSes running
- System enumeration (user and group names, system banners, routing tables, and SNMP info)

Remote access

- Analog/digital telephone numbers
- Remote system type
- Authentication mechanisms

Intranet

- Networking protocols used
- Internal domain names
- Network blocks
- IP addresses of reachable systems
- TCP and UDP services running
- System architecture
- ACLs
- IDSes running
- System enumeration

Extranet

- Connection origination and destination
- Type of connection
- Access control mechanism



Information Gathering

Information Gathering Methodology

Unearth initial information

Locate the network range

Ascertain active machines

Discover open ports/ access points

Detect operating systems

Uncover services on ports

Map the network



Unearthing Initial Information

Hacking tool

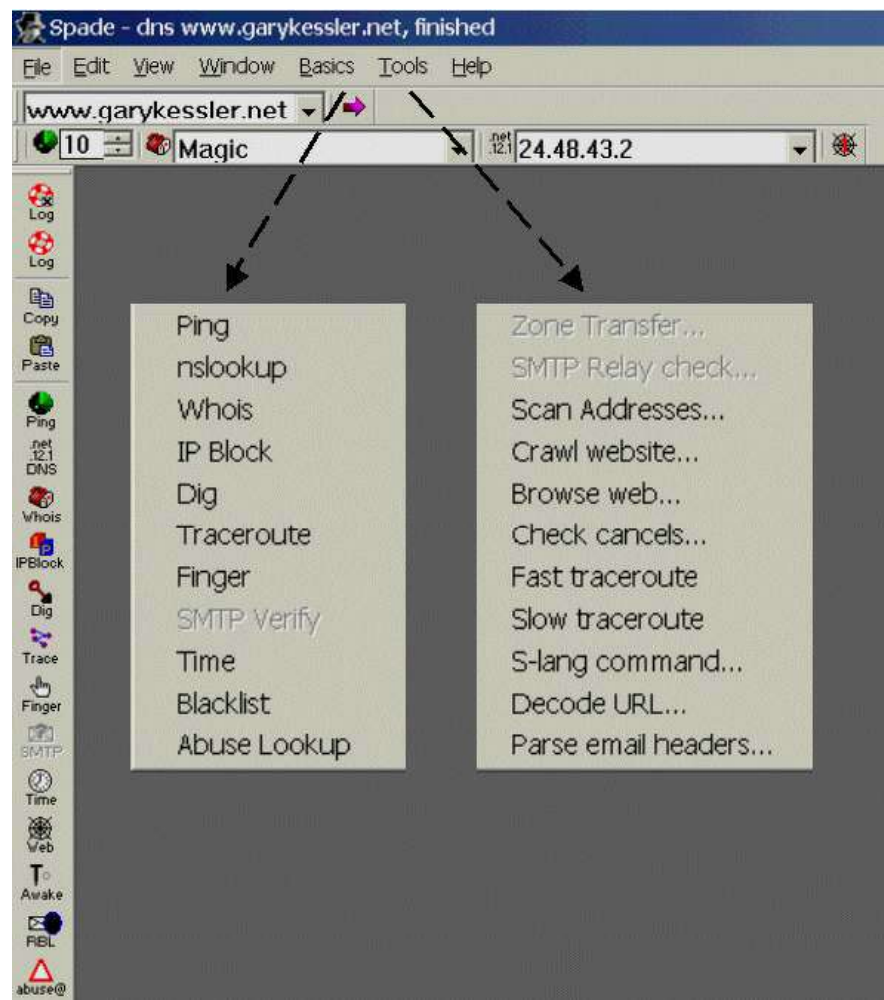
Sam Spade

Commonly includes:

- Domain name lookup
- Locations
- Contacts (telephone / mail)

Information Sources:

- Open source
- Whois
- Nslookup





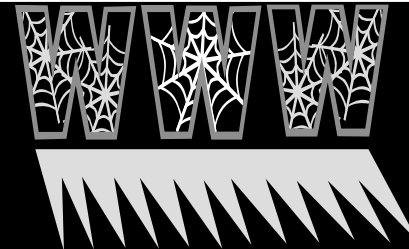
Search for a company's URL using a search engine such as Google

Type the company's name in the search engine to get the company's URL

Google provides rich information to perform passive reconnaissance

Check newsgroups, forums, and blogs for sensitive information regarding the network





By taking a guess, you may find an internal company URL

You can gain access to internal resources by typing an internal URL

- beta.xsecurity.com
- customers.xsecurity.com
- products.xsecurity.com
- Partners.xsecurity.com
- Intranet.xsecurity.com
- Asia.xsecurity.com
- Namerica.xsecurity.com
- Samerica.xsecurity.com
- Japan.xsecurity.com
- London.xsecurity.com
- Hq.xsecurity.com
- Finance.xsecurity.com
- www2.xsecurity.com
- www3.xsecurity.com

Extracting Archive Of a Website

You can get all information of a company's website since the time it was launched at www.archive.org

- For example: www.eccouncil.org

You can see updates made to the website

You can look for employee's database, past products, press releases, contact information, and more

**WEB
PAGE**





[Web](#) | [Moving Images](#) | [Texts](#) | [Audio](#) | [Software](#) | [Education](#) | [Patron Info](#) | [About IA](#)

[Forums](#) | [FAQs](#) | [Contributions](#) | [Jobs](#) | [Donate](#)

Search: All Media Types

Universal access
to human knowledge

[Upload](#) Anonymous User ([login](#) or [join us](#))

Announcements [\(more\)](#)

[Zotero and Internet Archive join forces](#)

[80 Libraries Going Open](#)

[More bandwidth](#)

Web

85 billion pages



[Take Me Back](#)

[Advanced Search](#)

Welcome to the
Archive

[RSS](#)

The Internet Archive is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public.

Moving Images

115,148 movies

[Browse](#) [\(by keyword\)](#)

[Curator's Choice](#) [\(more\)](#)



[Star Wars: The Han Solo Affair](#)
Official Star Wars parody from Spite

Live Music Archive

47,053 concerts

[Browse](#) [\(by band\)](#)

[Curator's Choice](#) [\(more\)](#)



[Hot Buttered Rum Live at Great American Music...](#)
Set | Flask Alas! Virginia's Grin
Evolution> Angeline>Cindy Firefly
Idaho Pines Sugaree Well Oiled...

Audio

231,411 recordings

[Browse](#) [\(by keyword\)](#)

[Curator's Choice](#) [\(more\)](#)



[Bathroom Sink](#)
Being yourself is where it's at.

Texts

348,656 texts

[Browse](#) [\(by keyword\)](#)

[Curator's Choice](#) [\(more\)](#)



Enter Web Address:

All

[Adv. Search](#) [Compare Archive Pages](#)

<http://microsoft.com>

1866 Results

dates are not shown. [See all.](#)

site was updated.

becomes available here 6 months after collection. [See FAQ.](#)

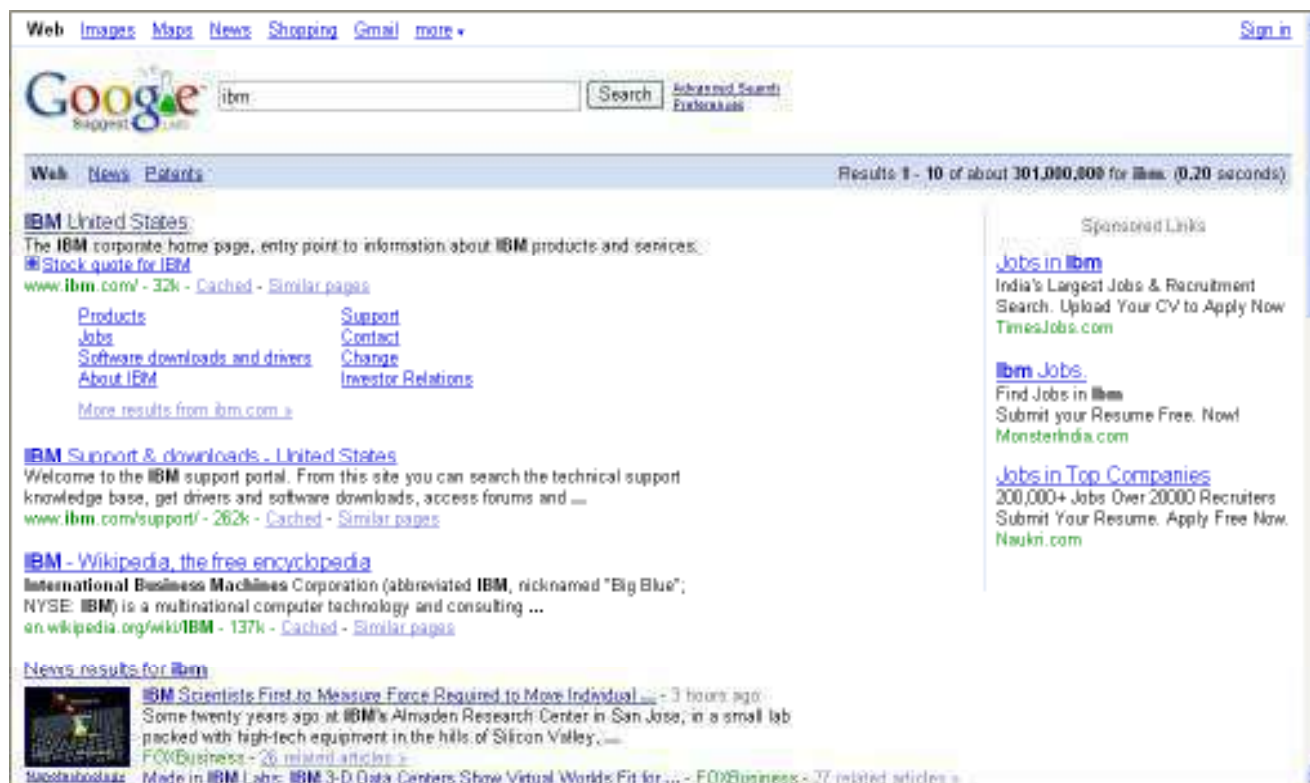
Search Results for Jan 01, 1996 - Aug 26, 2007

1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
0 pages	2 pages	19 pages	103 pages	263 pages	139 pages	28 pages	146 pages	304 pages	152 pages	94 pages
	Dec 05, 1998 * Dec 12, 1998 *	Jan 17, 1999 * Jan 25, 1999 * Feb 03, 1999 * Feb 08, 1999 * Feb 18, 1999 * Feb 22, 1999 * Feb 23, 1999 * Apr 22, 1999 * Apr 23, 1999 * Apr 28, 1999 * Apr 29, 1999 * May 01, 1999 * May 06, 1999 * Oct 04, 1999 * Oct 07, 1999 *	Feb 29, 2000 * Mar 01, 2000 * Mar 02, 2000 * Mar 02, 2000 * Mar 02, 2000 * Mar 03, 2000 * Mar 03, 2000 * Mar 04, 2000 * Apr 07, 2000 * Apr 09, 2000 * May 10, 2000 * May 10, 2000 * May 11, 2000 * May 11, 2000 *	Jan 03, 2001 * Jan 03, 2001 * Jan 04, 2001 * Jan 05, 2001 * Jan 06, 2001 * Jan 06, 2001 * Jan 07, 2001 * Jan 08, 2001 * Jan 08, 2001 * Jan 08, 2001 * Jan 08, 2001 * Jan 08, 2001 * Jan 18, 2001 * Jan 18, 2001 * Jan 30, 2001 * Feb 02, 2001 *	Jan 21, 2002 * Jan 25, 2002 * Jan 27, 2002 * Jun 03, 2002 * Jun 04, 2002 * Jun 05, 2002 * Jul 01, 2002 * Jul 02, 2002 * Jul 03, 2002 * Jul 03, 2002 * Jul 04, 2002 * Jul 07, 2002 * Jul 08, 2002 * Jul 09, 2002 * Jul 11, 2002 *	Jan 30, 2003 * Feb 08, 2003 * Feb 20, 2003 * Mar 21, 2003 * Mar 24, 2003 * Mar 28, 2003 * Apr 11, 2003 * Apr 11, 2003 * May 06, 2003 * May 13, 2003 * May 29, 2003 * Jun 18, 2003 * Jun 18, 2003 * Jun 23, 2003 * Jun 24, 2003 * Jul 17, 2003 *	Feb 08, 2004 * Feb 09, 2004 * Mar 25, 2004 * Apr 01, 2004 * Apr 10, 2004 * Apr 15, 2004 * Apr 18, 2004 * Apr 18, 2004 * May 18, 2004 * May 22, 2004 * May 26, 2004 * Jun 08, 2004 * Jun 09, 2004 * Jun 10, 2004 * Jun 10, 2004 * Jun 12, 2004 *	Jan 04, 2005 * Jan 10, 2005 * Jan 15, 2005 * Jan 16, 2005 * Jan 18, 2005 * Jan 20, 2005 * Jan 21, 2005 * Jan 22, 2005 * Jan 24, 2005 * Jan 25, 2005 * Jan 27, 2005 * Jan 29, 2005 * Jan 29, 2005 * Jan 30, 2005 * Jan 30, 2005 * Jan 31, 2005 *	Jan 01, 2006 * Jan 01, 2006 * Jan 01, 2006 * Jan 01, 2006 * Jan 01, 2006 * Jan 01, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 * Jan 02, 2006 *	Jan 02, 2007 * Jan 03, 2007 * Jan 07, 2007 * Jan 07, 2007 * Jan 08, 2007 * Jan 12, 2007 * Jan 14, 2007 * Jan 17, 2007 * Jan 25, 2007 * Jan 26, 2007 * Jan 28, 2007 * Jan 29, 2007 * Jan 30, 2007 * Jan 30, 2007 * Feb 02, 2007 * Feb 02, 2007 *

Google Search for Company's Info.

Using Google, search company's news and press releases

From this information, get the company's infrastructure details



People Search

You can find personal information using People search

For example, <http://people.yahoo.com>, <http://www.intellius.com>

You can get details like residential addresses, contact numbers, date of birth, and change of location

You can get satellite pictures of private residences



Try our **free** white pages search to access updated phone and address information.
Find friends, colleagues, classmates and more!

US Phone and Address Search

[\(Canada Phone and Address Search\)](#)

First Name/Initial:

Last Name: (required)

City/Town:

State:

Email Search

First Name/Initial:

Last Name:

[Advanced Email Search](#) - [Services and Tools](#)

Reverse Phone Number Search

Phone Number:

Satellite Picture of a Residence





Best PeopleSearch

<http://www.bestpeoplesearch.com/>

BestPeopleSearch.com
"Our Name says it all"

[Home](#) | [Articles](#) | [Help](#) | [Login](#)

[Quick Search](#)

Home
All Searches
Our Guarantee
FAQs
About Us
Contact Us
Link Exchange

Have a Phone Number?

Need a Name and Address?

[Click Here!](#)

[Need Assistance?](#)



The most accurate reverse look up and people search by phone or address on the web. Discover the Best People Search guarantee listed on every people search order page.

Place your order today and find out why Law offices, Collection Agencies and other professionals Trust Best People Search. As a trusted BBB member we have prescreened all third party private investigators that personally complete your requests. This will ensure your order is completed in a professional, confidential and secure manner.

Professionals search through billions of records in order to obtain the most accurate and up-to-date information available.

[Click here](#) to read Customer Reviews and Real Life Stories.
If you have any questions please [contact customer service](#).

People Search by Name

- ◆ [Basic Search by Name / Address or SSN](#)
- ◆ [Comprehensive People Search](#)
- ◆ [Guaranteed Current Address Search](#)
- ◆ [Find Address and Phone number \(w/SSN\)](#)
- ◆ [Find Address and Phone numbers \(w/out SSN\)](#)
- ◆ [How can I find cell phone numbers](#)
- ◆ [Search for cell phone numbers](#)
- ◆ [Verified Current Employer Search w/SSN \(POE\)](#)
- ◆ [Verified Current Employer Search w/o SSN \(POE\)](#)

People Search by Address

- ◆ [Comprehensive People Search](#)
- ◆ [Basic Search by Name / Address or SSN](#)
- ◆ [Reverse Postal or Private Mail Box Lookup \(PMB\)](#)
- ◆ [PO Box Search \(Reverse P.O. Box Lookup\)](#)
- ◆ [How to find cell phone number](#)
- ◆ [How to find out cell phone numbers](#)
- ◆ [Reverse Address Lookup \(name, phone from address\)](#)

People Search by Email Address

- ◆ [Reverse Email Lookup](#)



Most Popular Searches

1. [FREE Social Security Number Verification](#)
2. [Name & Address from Cell number \(Reverse Cell phone lookup\)](#)
3. [Name & Address from Unlisted Number \(Reverse\)](#)

People-Search-America.com

HOME

SUPPORT

FAQS

MEMBER LOGIN

REGISTER

PRIVACY

TERMS AND CONDITIONS



PEOPLE SEARCH

Find information on any phone, mobile cell phone, business, pager, pay phone and even unlisted numbers. Reverse phone number search includes name, address service provider and other details.

* Name :
* City :
* State :



BACKGROUND CHECK

Investigate your boyfriend. View criminal, finance, court and other records. Get the scoop on your daughter's coach or new acquaintance.

* Name :
* City :
* State :



REVERSE PHONE LOOKUP

Find information on any phone, mobile cell phone, business, pager, pay phone and even unlisted numbers. Reverse phone number search includes name, address service provider and other details.



SOCIAL SECURITY

Investigate your boyfriend. View criminal, finance, court and other records. Get the scoop on your daughter's coach or new acquaintance.



 **Switchboard**[®] Your Digital Directory

Find a Business

Find a Person

Maps & Directions

Search by Phone

Area & Zip Codes

Web Search

Find a Business

Business Name or Category

[Choose a Category](#)

Enter a Search term (e.g. john's diner, shows, lawyer)

Location

Enter location (e.g. Address, City, State, or Zip Code)

Search

[Help](#)

Recent Searches

<No Recent Searches>

More Business Search Options

- » [Search by Distance](#)
- » [Browse by Category](#)
- » [Browse by Location](#)
- » [Browse by Name](#)

data by **AQDAM**

Some business data provided by infoUSA, Inc. Copyright © 2007

[About Switchboard](#) | [Contact Us](#) | [Advertising](#) | [Tools and Tips](#) | [Privacy Policy](#) | [Help](#) | [Terms of Use](#)

infospace

[Our Story](#) | [Mobile Products](#) | [Online Products](#) | [Careers](#) | [Press Room](#) | [Investor Center](#)

i2 A ChoicePoint Company

careers case studies info request

VISUALIZE ANALYZE COMMUNICATE

anacubis

anacubis is now part of i2 ChoicePoint

anacubis is now part of i2 ChoicePoint's research and development group. As the world-leading supplier of visual analysis software, i2 ChoicePoint provides investigative analysis solutions for Law Enforcement and Government Agencies. For more information on i2 ChoicePoint software solutions, [click here](#).

i2 ChoicePoint will continue to support all existing anacubis customers. For support on anacubis products, contact [anacubis Support](#), or use the links below.

[anacubis Viewer Help](#)
[Can't see an anacubis visualisation?](#)

Welcome to i2

Home	i2 Analyst's Notebook
Products	i2 Analyst's Workstation
Solutions	i2 Analyst's Workstation TCA
Services	i2 ChartExplorer
Company	i2 ChartReader
	i2 iBase
	i2 iBridge
	i2 iBridge for HOLMES 2
	i2 iXa Framework
	i2 iXv SDK
	i2 PatternTracer
	i2 TextChart
	power2 Built-in



Search Finance

e.g. "CSCO" or "Google"

Recent quotes | [Portfolios](#)

Symbol	Price	Change	Mkt Cap
CSCO	27.50	-1.19 (-4.15%)	166.84B
EWJ	13.64	0.00 (0.00%)	11.04B
F	7.03	-0.16 (-2.23%)	14.83B
INTC	24.38	-0.69 (-2.75%)	142.55B
IWM	73.10	-1.96 (-2.61%)	10.05B
JPM	40.46	-1.49 (-3.55%)	135.91B
MSFT	32.97	-1.14 (-3.34%)	308.45B
SPY	140.95	-3.18 (-2.21%)	60.78B

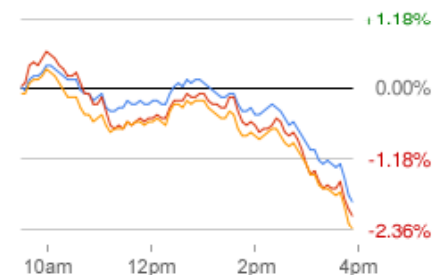
Related news

- [Ford Boosting Sirius Radio Exposure](#)
MSN Money - 7 minutes ago
- [UPDATE: Microsoft Ponders Data Center In Siberia](#)
CNNMoney.com - 1 hour ago - [related articles >](#)
- [Russell 2000: "No man's land" of short-term support](#)
SmallCapInvestor - 5 hours ago - [related articles >](#)
- [Microsoft, Autodesk lose patent appeal](#)
Seattle Post Intelligencer - 11 hours ago - [related articles >](#)
- [JPMorgan Chase to cut 91 jobs at SoCal mortgage operation](#)
San Jose Mercury News - 11 hours ago - [related articles >](#)
- [Live Documents to Challenge Microsoft Office, Google Apps](#)
eWeek - 16 hours ago - [related articles >](#)
- [Russian Ford Talks Fail to End Strike](#)
MSN Money - 18 hours ago - [related articles >](#)
- [Chrysler Aiming to Challenge Ford, Chevy for Police Car Sales](#)
Wall Street Journal - 18 hours ago - [related articles >](#)

Make Google Finance your own. Get quotes, charts, news and more on iGoogle.

[Add an iGoogle Finance homepage](#)

Market summary Nov 26 - Close



Dow	12,743.44	-237.44	(-1.83%)
Nasdaq	2,540.99	-55.61	(-2.14%)
S&P 500	1,407.22	-33.48	(-2.32%)
10y bond	3.83%	-0.17	(-4.25%)

YAHOO! FINANCE

Search: **Web Search**

- HOME
- INVESTING
- NEWS & OPINION
- PERSONAL FINANCE
- MY PORTFOLIOS

GET QUOTES Symbol Lookup Finance Search

Tuesday, November 27, 2007; 7:25AM ET - U.S. Markets open in 2 hours and 5 minutes.

Scottrade - \$7 trades. No share limit. In-depth research.

MARKET SUMMARY



» View more indices Customize summary

» View more bonds

Tue 6:19am ET - Briefing.com
S&P futures vs fair value: +15.0. Nasdaq futures vs fair value: +20.5. ...
 » Read more

TOP STORIES As of 3 minutes ago

Citi Sells Stake to Abu Dhabi Fund

AP: Citigroup said late Monday that the Abu Dhabi Investment Authority will invest \$7.5 billion in the nation's largest bank, offering needed capital to offset big losses from mortgages and other investments.

- Report: Foreclosures to Hit Metro Areas - AP
- Oil Prices Extend Losses in Europe - AP
- Stock Futures Point to Higher Open - AP
- Hollywood Labor Talks Set to Resume - AP

» View more top stories

More News on Markets, Companies and Economy

FOCUS ON RETIREMENT brought to you by Fidelity

How Much Income You'll Really Need
 An old rule of thumb says to plan for a retirement income of 70 to 80 percent of your current income. But you may want to wipe this estimate from your brain...

» More Retirement Stories...

VIDEOS

- Christmas Tune-up**
Provided by: FOXA
- Tipping in the Holiday Spirit - ABC News
- Late selloff erases Black Friday rally - SmartMoney
- Northern Rock troubles - CNN News

» View all videos

QUOTES

- Recent Quotes
- My Portfolios

Your most recently viewed tickers will automatically show up here if you type a ticker in the Get Quotes box on the top of the page.

Footprinting Through Job Sites

You can gather company's infrastructure details from job postings

Look for company's infrastructure postings such as "looking for system administrator to manage Solaris 10 network"

This means that the company has Solaris networks on site

- E.g., www.jobsdb.com



Job requirements

Employee profile

Hardware information

Software information



The screenshot shows the JobsDB.com website. At the top, there is a navigation bar with links: Home, About Us, Press Room, Events, Career@JobsDB, and Contact Us. Below this is a banner for 'the CV BUILDER' with the text 'THE BEST START TO GETTING THE BEST JOB IS HAVING THE BEST CV' and a price tag of 'only \$87.00'. The main content area includes a 'Job Seeker Login' form with fields for Username, Password, and Location (set to USA), and buttons for Submit, Reset, and Forgot Password. To the right of the login form is a 'Take a tour on MyJobsDB' section with a 'Register Now!' button. Further right is a 'Job Seekers' section with links to 'Subscribe Regional Job Alert' and 'Subscribe China Job Alert', and a note that users can unsubscribe at any time with no obligation. Below these sections are two lists: 'Jobs by Country' and 'Jobs by Category'. The 'Jobs by Country' list includes USA, Australia, Hong Kong, India, Indonesia, Korea, Malaysia, Philippines, Singapore, and Taiwan. The 'Jobs by Category' list includes Accounting, Administrative/Secretarial, Banking/Finance, Engineering, Recruitment Consultancy, General Management, I.T., Manufacturing/Production, Marketing, Retail/Wholesale, Telecommunications, and Sales. At the bottom, there are sections for 'JobsDB Resources For Job Seekers', including 'Career Tips' (with a 'Hot Topic' icon) and 'Interview Advise'. The 'Career Tips' section has a link for 'What do the employers look for in job seekers? Should I continue Studying?'. The 'Interview Advise' section has a link for 'Gain confidence in job interviews'. There is also an 'Advance Search' button and an 'Other Useful Links' section.

Footprinting Through Job Sites(cont'd)

Designation

System Administrator / DBA (Position is based in U.S.A.)

Job Description

This position is based in Long Beach LA, CA

* We are looking for a System Administrator cum DataBase Administrator, who can take care of one our Existing Account.

* The Major role would be to do System Software Installations, Configurations and Monitoring the impact of building out of a number of environments from scratch.

* Major interaction of this profile would be with QA Lead / Team in Deploying the code from one to another environment.

Duration : 9 Months

Desired Profile

- 1) Strong AIX & Solaris System Admin Skills
- 2) Should be proficient in UNIX scripting and manual commands
- 3) WebSphere ADMIN v5 required
- 4) Configuration Management Tool experience (PVCS, CVS, etc.)
- 5) Code deployment from one environment to another
- Perl Scripting
- 6) Experience working with Hosting provider

** The perfect choice would be somebody who has expereince in production environment with a Corporate Portal.

Plus:

- * Certifications
- * Vignette a huge plus
- * Quality assurance on a WebSphere project
- * Vignette release management
- * Load testing tools (Mercury preferred.)

Minimum Experience

2 years

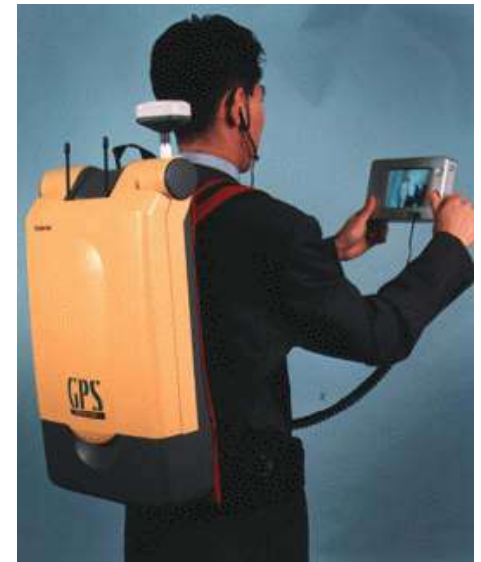


Passive Information Gathering

To understand the current security status of a particular Information System, organizations perform either a Penetration Testing or other hacking techniques

Passive information gathering is done by finding out the freely available details over the Internet and by various other techniques without coming in contact with the organization's servers

Organizational and other informative websites are exceptions as the information gathering activities carried out by an attacker do not raise suspicion





Competitive Intelligence Gathering

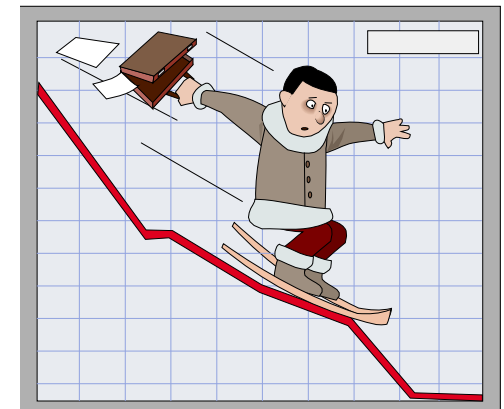
Competitive Intelligence Gathering

‘Business moves fast. Product cycles are measured in months, not years. Partners become rivals quicker than you can say ‘breach of contract.’ So how can you possibly hope to keep up with your competitors if you can't keep an eye on them?’

Competitive intelligence gathering is the process of gathering information about your competitors from resources such as the Internet

The competitive intelligence is non-interfering and subtle in nature

Competitive intelligence is both a product and a process



Competitive Intelligence Gathering (cont'd)

The various issues involved in competitive intelligence are:

- Data gathering
- Data analysis
- Information verification
- Information security

Cognitive hacking:

- Single source
- Multiple source

Ahead of
competition



Why Do You Need Competitive Intelligence



Compare your products with your competitors' offerings

Analyze your market positioning compared to the competitors

Pull up a list of competing companies in the market

Extract salesperson's war stories on how deals are won and lost in the competitive arena

Produce a profile of CEO and the entire management staff of the competitor

Predict their tactics and methods based on their previous track record

<http://ciseek.com>

The CI Resource Index

Competitive Intelligence Resources Categorized

Stop searching. Start Finding. Try **Factiva Companies today. & Executives**

Factiva, a Dow Jones & Reuters Co.

Factiva

[\[Click Banner To Learn More\]](#)

Competitive Intelligence Resource Index - A search engine and listing of sites-by-category for finding CI resources. Ciseek.com

Search and Categories

[Advanced Search](#)

Associations (75)

Associations and Societies in the field of CI and the Like.

Books (96)

Books related to the various topics found in CI activities.

Companies (1355) **new**

Consulting, Market Research, Online Information and Databases.

Documentation (56) **new**

Articles, information and tutorials regarding CI.

Business Intelligence

Fast Integration for Application Development. [Read Reports & Reviews](#)

Education (39) **new**

CI courses and training programs, certificates.

Jobs (4)

CI and KM jobs. CI recruitment companies.

Publications (59) **new**

CI Pubs.; Newsletters, Journals and Magazines.

Software (312) **new**

CI Systems & Portals; organize, gather, analyse, and share information.

Services

Free Newsletter:
 Your Name:
 Your Email:

- ▶ [Recommend](#)
- ▶ [Popular links](#)
- ▶ [CI Bookstand](#)
- ▶ [Advertising](#)
- ▶ [Alexa Toolbar](#)

CI in the News

Free News Feeds for Your Website
 FeedDirect 23 Apr 2005 03:45:00

Frost & Sullivan Honors Best Practices Leaders
 Business Wire via Charlotte Observer 23 Apr 2005 03:45:00

Frost & Sullivan Honors Best Practices Leaders
 Business Wire via Providence Journal 23 Apr 2005 02:36:00

Companies Providing Competitive Intelligence Services

Carratu International

- <http://www.carratu.com>

CI Center

- <http://www.cicentre.com>

CORPORATE CRIME MANAGEMENT

- <http://www.assesstherisk.com>

Marven Consulting Group

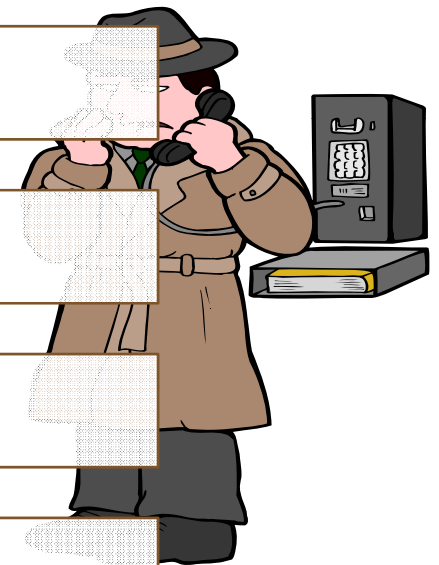
- <http://www.marwen.ca>

SECURITY SCIENCES CORPORATION

- <http://www.securitysciences.com>

Lubrinco

- <http://www.lubrinco.com>





If you can't find a service that meets your requirements please email us

ALPHABETICAL SERVICES LIST: CLICK ON THE NAME FOR FURTHER INFORMATION

- ▶ Anti Counterfeiting
- ▶ Asset Tracing
- ▶ Background Profiles
- ▶ Brand Protection
- ▶ Competitive Intelligence
- ▶ Computer Forensics
- ▶ Computer Fraud
- ▶ Computer Imaging
- ▶ Computer Security
- ▶ Corporate Investigations
- ▶ Corporate Security
- ▶ Covert Audits
- ▶ Data Interrogation
- ▶ De-bugging
- ▶ Domain Name investigation
- ▶ Due Diligence
- ▶ Employee Vetting
- ▶ Environmental Issues
- ▶ Firstline Response
- ▶ Forensic Accounting
- ▶ Franchise Enforcement
- ▶ Fraud Investigation
- ▶ Grey Market Investigation
- ▶ Information Protection
- ▶ Insurance Fraud
- ▶ Internet Investigation
- ▶ Internal Theft
- ▶ Litigation Support
- ▶ MarketWatch@
- ▶ Mediation Support
- ▶ Mergers & Acquisitions
- ▶ Money Laundering
- ▶ Patent Investigations
- ▶ Pharmaceutical Intelligence
- ▶ Pharma. Patent Infringement
- ▶ Pharma. Counterfeiting
- ▶ Pharma. Investigations
- ▶ Product Monitoring
- ▶ R-check™ search
- ▶ Re-insurance Fraud
- ▶ Status Reporting
- ▶ Surveillance - Static & Mobile
- ▶ Test Purchases
- ▶ Third Party Acquisitions
- ▶ Trademark Infringement
- ▶ Trademark In-use
- ▶ Undercover Operations



CI Centre
 Advanced Counterintelligence,
 Counterterrorism & Security Education

CI Centre Store

For the Spy Catcher in You Audio lectures, CI posters, books, eternal vigilance, intel services, spy catcher, storm petrel, D*I*C*E and more

Robert Hanssen: Colleague, Friend, and Traitor

Wed, 28 Nov, 6:30p; International Spy Museum, lecture by CI Centre President David Major
[Register](#)

CI Centre Podcasts

NEW: Ron Kessler, Daniel Pipes, Nonie Darwish

Required Reading

for Intel Professionals



The Centre for Counterintelligence and Security Studies (CI Centre)[®] | Alexandria, VA | 703-642-7450 or 1-800-779-4007

Home	Courses	D*I*C*E	Speakers
Podcasts	Store		
CI News	CT News	Resources	Books
CI Timeline	SpyDrive		
About Us	Staff	FAQs	Contact
Mailing List	SpyTrek		

Robert Hanssen: Colleague, Friend, and Traitor

Wednesday, 28 November 2007 at 6:30 pm; International Spy Museum, Washington, DC

CI Centre President David Major provides a glimpse into the real personality and psychology of Robert Hanssen, one of the most damaging spies in U.S. history. He will explore why Hanssen's betrayal was so difficult to uncover, his own theories on what motivated the spy, his perspective on Breach, and the status of U.S. counterintelligence in the wake of this profoundly important spy case. Tickets: \$23 [REGISTER](#)

Page updated:
 Tuesday, November 27,
 2007

CI CENTRE MISSION:

The CI Centre provides dynamic, in-depth and relevant education, training and products on counterintelligence, counterterrorism and security. Our programs

Counterintelligence & Espionage News

Terrorism Intel/ War of Ideas News

Competitive Intelligence - When Did This Company Begin? How Did It Develop

Laser D for Annual Reports to Stockholders & 10-Ks (Reference Room - workstation #12)

[EDGAR database](#) - for 10-K and other report filed with the SEC (also [Business Database Selection Tool](#))

International Directory of Company Histories (Reference - HD 2721 D36)

[Mergent Online](#) - company history and joint ventures ([Business Database Selection Tool](#))

Notable Corporate Chronologies (Reference - HD 2721 N67 1995)

[ORION](#), UCLA's Online Library Information System ([Business Database Selection Tool](#))

Enter Search Terms: general electric [for books on GE] , click on button: Search Subject Words

Competitive Intelligence - Who Leads This Company

[ABI/INFORM Global](#) ([Business Database Selection Tool](#))

Search for: microsoft in Subject; AND; biographies in Subject; Search

[Hoover's Online](#) - Company Profile includes Key People. ([Business Database Selection Tool](#))

Also in print as *Hoover's Handbook of American Business* (Reference - HG 4057 A28617)

[National Newspaper Index](#) ([Business Database Selection Tool](#))

Type in: exxon ; Search

Reference Book of Corporate Managements (Reference Index Area, section 5)

Who's Who in Finance and Industry (Reference Index Area, section 5)

Competitive Intelligence - What Are This Company's Plans

ABI/INFORM Global (Business Database Selection Tool)

Search for: mci in Company/Org.; AND; alliances in Subject; OR; market strategy in Subject; Search

LexisNexis Academic (Business Database Selection Tool)

Business; Industry & Market; Keyword: Palm; Industry: Computer & Telecom; Date: Previous six months; Search

Business & Industry® (Web) (Business Database Selection Tool)

200X BUS_IND, Open; Search/Modify, Company Name; Search/Modify, Business Subject, Modify: Company Forecasts; OK

Factiva (Business Database Selection Tool)

Enter free-text terms: intel near plans; Select date: in the last year; Select sources: All Content; Run Search



Competitive Intelligence - What Does Expert Opinion Say About The Company

[ABI/INFORM Global](#) [academics] ([Business Database Selection Tool](#))

[First Call](#) [analyst reports] ([Business Database Selection Tool](#))

FINDEX: Directory of Market Research Reports (Reference - HF 5415.2 F493)

[Market Research Monitor](#) ([Business Database Selection Tool](#))

[Multex](#) [analyst reports] ([Business Database Selection Tool](#))

Nelson's Directory of Investment Research (Reference - HG 4907 N43)

Wall Street Transcript "TWST Roundtable Forums" and "CEO Forums"
Features (Unbound Periodicals - 2nd floor) [analysts' discussion of a given industry, see this [sample issue](#) with Semiconductor Equipment Industry Roundtable]



Competitive Intelligence - Who Are The Leading Competitors

Business Rankings Annual (Reference - HG 4057 A353)

[Hoover's Online](#) - Top Competitors free, More Competitors available, use ([Business Database Selection Tool](#))

Market Share Reporter (Reference - HF 5410 M37)

[U.S. Patent and Trademark Office](#) [identify players in emerging product areas, see also [other patent resources](#)]

[Reference USA](#) [companies by SICs and more] ([Business Database Selection Tool](#))

[TableBase \(Web\)](#) [find market shares within articles] ([Business Database Selection Tool](#))

Ward's Business Directory of U.S. Private and Public Companies (Reference Room, Index Section 1)

World Market Share Reporter (Reference - HF 1416 W67)



Competitive Intelligence Tool: Trellian

Trellian compiles and analyzes internet usage statistics to create a powerful Competitive Intelligence tool that no business should be without



Link Intelligence

Find out which sites send the most traffic to your competitors.



Search Term Intelligence

What keywords drive the most traffic to competing sites?



Campaign Intelligence

Identify search terms your competitors are advertising on.



Benchmarking

Find out how your business compares with other competitors.



Keyword Rankings

Identify the search terms and keywords that your competitors rank on.



Affiliate Partners

Identify the top Affiliate partners sending traffic to your competitors.



Competitive Intelligence Tool: Web Investigator

Web Investigator checks sources, public databases, and proprietary search databases, and allows to download and view reports of records

You can get the report you are looking for

Quickly and efficiently search and locate public records online



Web Investigator: Screenshot





[FAQ](#) | [LOGIN](#) | [HELP](#) | [TERMS](#) | [BUSINESS USERS](#)

 <p>Background Reports</p>	 <p>People Search</p>	 <p>Criminal Records</p>	 <p>Civil Records</p>	 <p>Reverse Searches</p>
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Background Report <input checked="" type="checkbox"/> Business Report <input checked="" type="checkbox"/> Check Your Date <input checked="" type="checkbox"/> Person Report <input checked="" type="checkbox"/> Nanny Check <input checked="" type="checkbox"/> Identity Verification 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> People Search <input checked="" type="checkbox"/> Enhanced Phone Search <input checked="" type="checkbox"/> Investigate Anyone <input checked="" type="checkbox"/> Classmate Search <input checked="" type="checkbox"/> Find Friends <input checked="" type="checkbox"/> Find Relatives 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Arrest Records <input checked="" type="checkbox"/> Court Records <input checked="" type="checkbox"/> Criminal Records <input checked="" type="checkbox"/> DUI/DWI Records <input checked="" type="checkbox"/> Felony/Misdemeanor <input checked="" type="checkbox"/> Sex Offender 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Bankruptcies <input checked="" type="checkbox"/> Birth Records <input checked="" type="checkbox"/> Divorce Records <input checked="" type="checkbox"/> Legal Judgments <input checked="" type="checkbox"/> Marriage Records <input checked="" type="checkbox"/> Property Records 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Reverse Address <input checked="" type="checkbox"/> Reverse Cellphone <input checked="" type="checkbox"/> Reverse Email <input checked="" type="checkbox"/> Reverse Phone <input checked="" type="checkbox"/> Unpublished Phone <input checked="" type="checkbox"/> Reverse SSN

Instant Complete Background Report

First Name: * <input type="text"/>	Last Name: * <input type="text"/>
Middle Initial: <input type="text"/>	City: <input type="text"/>
Approximate age: <input type="text"/>	State: * <input type="text" value="Nationwide"/>

 [Click to start Search](#)

 Our instant nationwide search system will check thousands of sources, public databases, and proprietary search databases and let you download and view the records reports within minutes. You can get the report you are looking for easily and effortlessly right from here.

Enjoy instant data lookups to ensure you are always on top of changes in

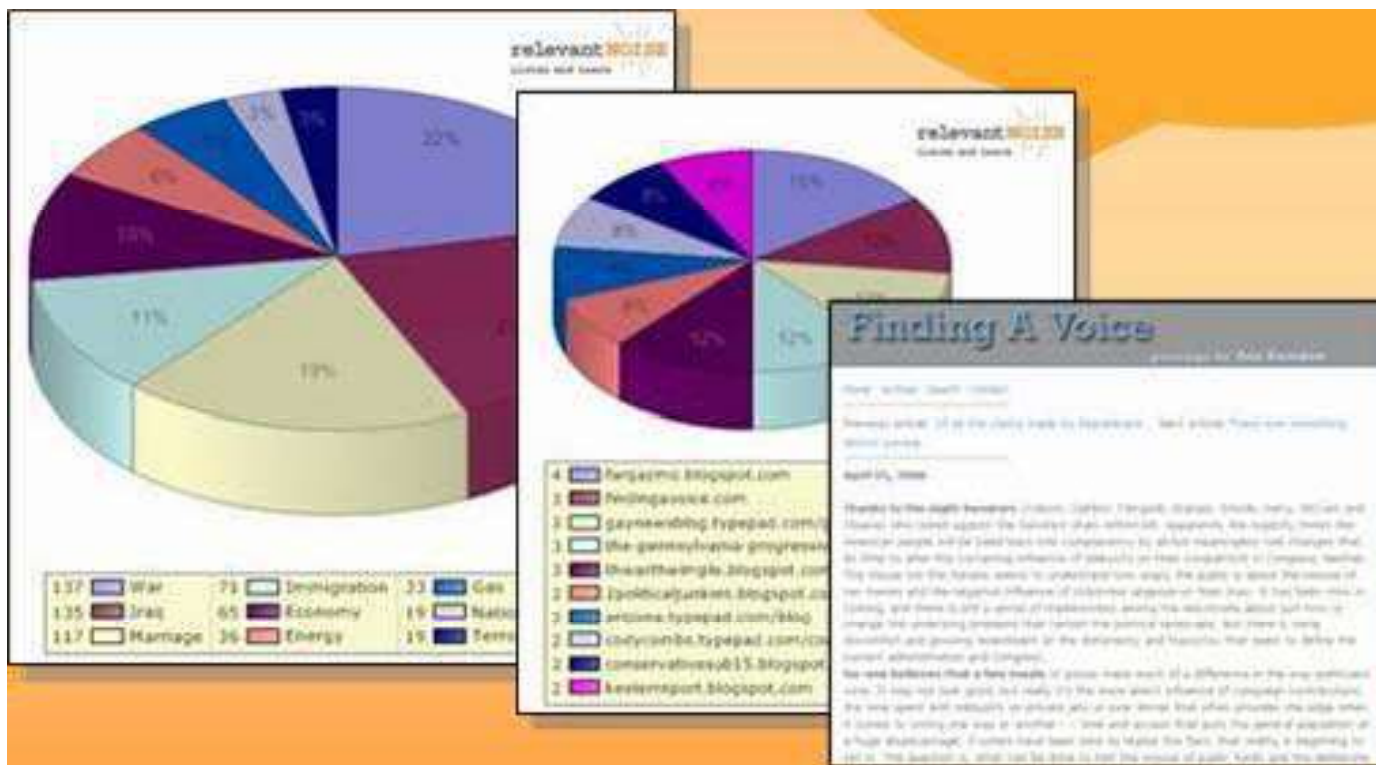
RelevantNoise is a subscription-based online search service that mines social media for business intelligence

It quickly says about your brands across social media and their impact

It helps a business to monitor the blog buzz about its products, services, and company's reputation, plus those of its competitors

It also assesses the relative influence of bloggers using factors such as their tenure, how often they post, and the number of incoming links to help you determine how much the opinions really matter

RelevantNoise: Screenshot



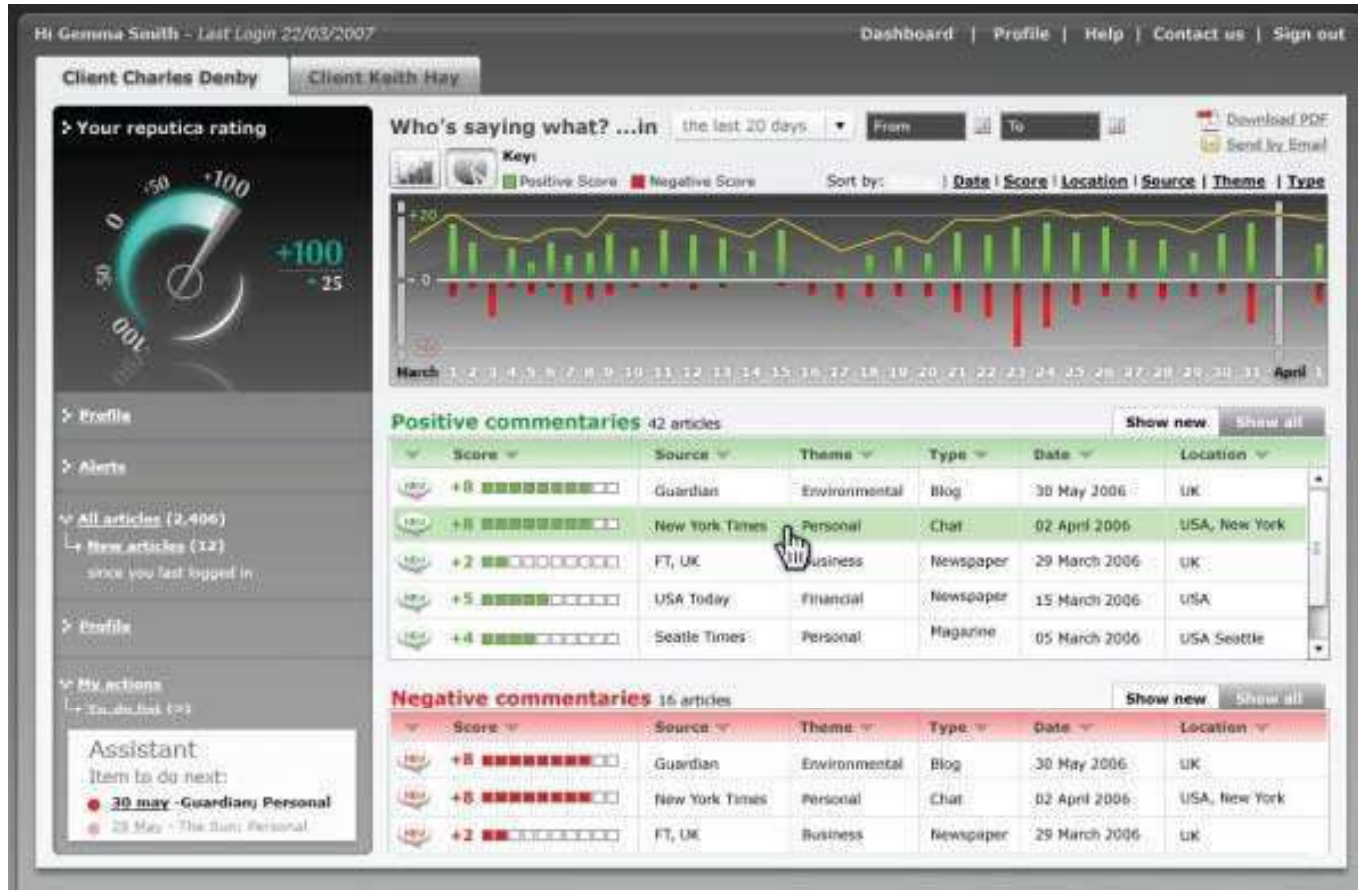
Reputica Dashboard

The Reputica Dashboard provides online source of information about your reputation, with links to the primary sources which caused your Reputica rating to go up or down

You can see how your rating has changed over time, and how it is compared with other companies or competitors



Reputica Dashboard: Screenshot



MyReputation finds out everything that is being said about you online and gets rid of the content you do not like

You can find detailed information from:

Social networks (MySpace, Facebook, LiveJournal, Bebo, and more)

Professional reviewed websites

Blogs

Online news sources

Photograph, video, and audio sharing sites (Flickr, YouTube, etc.)

Millions of additional sites on the "open Internet"

Public and Private Websites

A company might maintain public and private websites for different levels of access

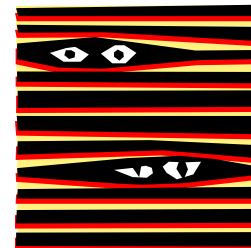
Footprint an organization's public www servers, for example:

- www.xsecurity.com
- www.xsecurity.net
- www.xsecurity.net



Footprint an organization's sub domains (private), for example:

- <http://partners.xsecurity.com>
- <http://intranet.xsecurity.com>
- <http://channels.xsecurity.com>
- <http://www2.xsecurity.com>

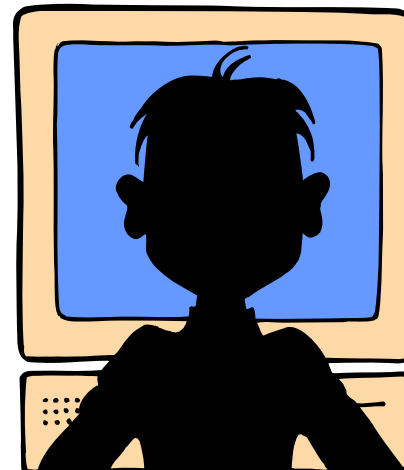




Footprinting Tools

Some Footprinting Tools:

- Whois
- Nslookup
- ARIN
- Neo Trace
- VisualRoute Trace
- SmartWhois
- eMailTrackerPro
- Website watcher
- Google Earth
- GEO Spider
- HTTrack Web Copier
- E-mail Spider





BiLE.pl

- BiLE leans on Google and HTTrack to automate the collections to and from the target site, and then applies a simple statistical weighing algorithm to deduce which websites have the strongest relationships with the target site
- Command:
 - `perl BiLE.pl www.sensepost.com sp_bile_out.txt`

BiLE-weigh.pl

- BiLE-weigh, which takes the output of BiLE and calculates the significance of each site found
- Command:
 - `perl bile-weigh.pl www.sensepost.com sp_bile_out.txt.mine out.txt`

tld-expand.pl

- The tld-expand.pl script is used to find domains in any other TLDs
- Command:
 - `perl exp-tld.pl [input file] [output file]`



vet-IPrange.pl

- The results from the BiLE-weigh have listed a number of domains with their relevance to the target website
- Command:
 - `perl vet-IPrange.pl [input file] [true domain file] [output file] <range>BiLE-weigh.pl`

qtrace.pl

- qtrace is used to plot the boundaries of networks. It uses a heavily modified traceroute using a #custom compiled hping# to perform multiple traceroutes to boundary sections of a class C network
- Command:
 - `perl qtrace.pl ip_address_file] [output_file]`

vet-mx.pl

- The tool performs MX lookups for a list of domains, and stores each IP it gets in a file
- Command:
 - `perl vet-mx.pl [input file] [true domain file] [output file]`



jarf-rev

- jarf-rev is used to perform a reverse DNS lookup on an IP range. All reverse entries that match the filter file are displayed on the screen
- Command:
 - `perl jarf-rev [subnetblock]`
 - `perl jarf-rev 192.168.37.1-192.168.37.118`

jarf-dnsbrute

- The jarf-dnsbrute script is a DNS bruteforcer when DNS zone transfers are not allowed. jarf-dnsbrute will perform forward DNS lookups using a specified domain name with a list of names for hosts
- Command:
 - `perl jarf-dnsbrute [domain_name] [file_with_names]`

Tool: Big Brother

Big Brother is designed to see how network is performing in near real-time from any web browser

It displays status information as web pages or WML pages for WAP-enabled devices

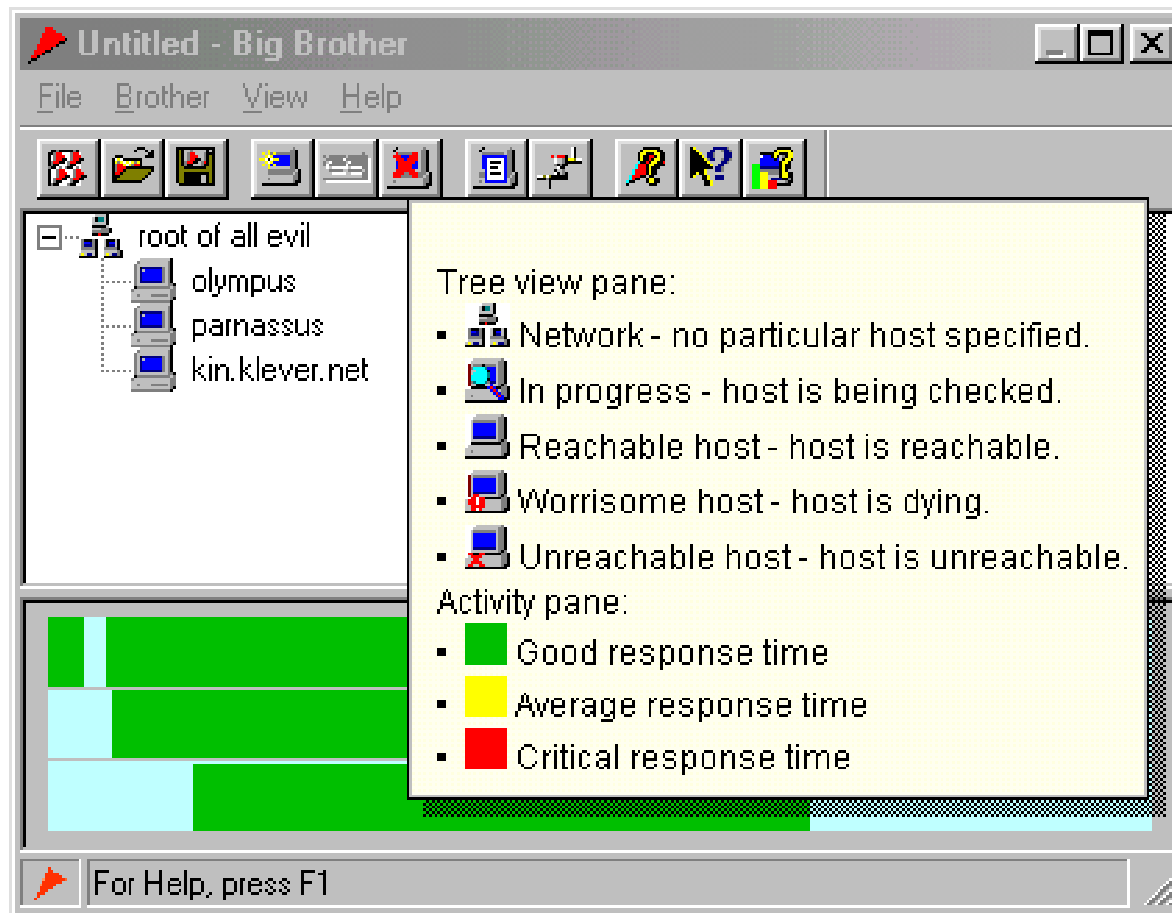
Big Brother uses a client-server architecture combined with methods which push and pull data

Network testing is done by polling all monitored services from a single machine, and reporting these results to a central location (BBDISPLAY)

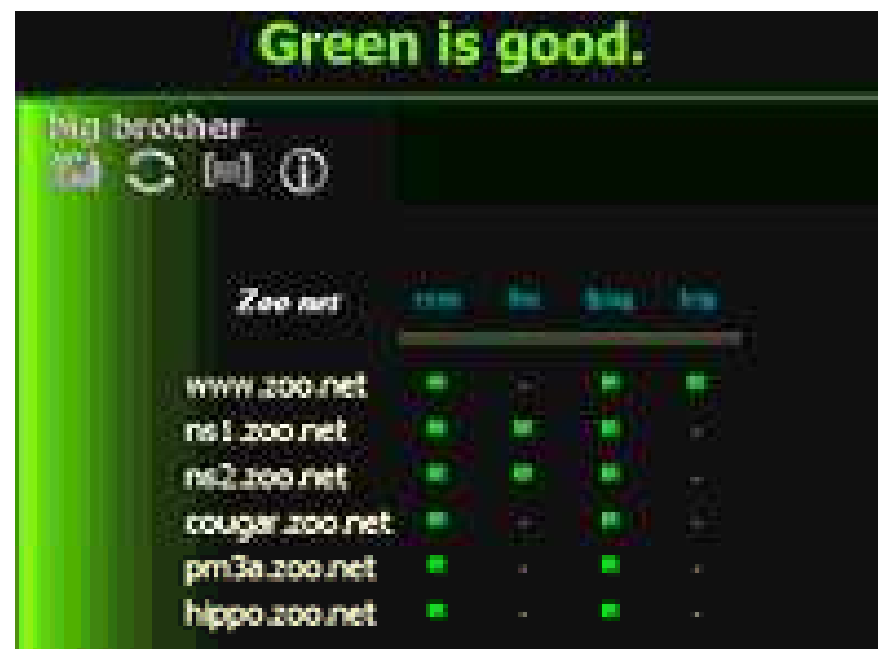
Big Brother includes support for testing ftp, http, https, smtp, pop3, dns, telnet, imap, nntp, and ssh servers



Big Brother: Screenshot 1



Big Brother: Screenshot 2



Tool: BiLE Suite

The BiLE suite contains a number of PERL scripts that can be used by a Penetration Tester to aid in the enumeration phase of a test

BiLE itself stands for Bi-directional Link Extraction utilities

The suite of tools can be used in the footprinting process to find both obvious and non-obvious relationships between disparate

With this information, a Pen Tester may then decide to try and access sites with close relationships with the target as a stepping stone into the target network



Tool: Alchemy Network Tool

Alchemy Network Tools is a software package containing a set of network analysis and diagnostic utilities

It aids network administrators to maintain and manage their networks in the nice graphical interface

Alchemy Network Tools contains the following network utilities:

- Ping
- Traceroute
- NSLookup
- Whois
- HTTP/HTTPS request sender
- SNMP request sender



Alchemy Network Tool: Screenshot

The screenshot shows the 'Traceroute' window in the Alchemy Network Tools application. The window title is 'Alchemy Network Tools' and it has a menu bar with 'File', 'View', 'Tools', and 'Help'. The left sidebar contains a tree view with the following items: System info, Route table, IP stats, ICMP stats, TCP stats, UDP stats, Ping, Traceroute (selected), SNMP, HTTP(S), Lookup, and WhoIs. The main area is titled 'Traceroute' and contains the text 'Displays the route the IP packet follows to a remote host'. Below this, there are input fields for 'Address' (snapfiles.com), 'Hops' (32), 'Count' (1), 'Timeout' (2000), and 'Size' (64). There is a 'Start' button and a checked 'Resolve IP' checkbox. The results are displayed in a table with columns: Hop, From, Time, TTL, and Reply.

Hop	From	Time	TTL	Reply
4	205.152.110.184	16 ms	252	Success
5	65.83.237.100 (AXR00BCT-0-1-3...	15 ms	248	Success
6	65.83.236.59 (AXR01MIA-0-3-1.b...	31 ms	249	Success
7	65.83.236.20 (pxr00mia-1-0-0.bell...	31 ms	248	Success
8	65.208.86.153 (0.so-0-0-0.GW8...	46 ms	247	Success
9	152.63.84.122 (0.so-1-3-0.XL2.MI...	15 ms	246	Success
10	152.63.87.34 (0.so-2-0-0.TL2.AT...	31 ms	245	Success
11	152.63.29.109 (0.so-3-0-0.TL2.L...	94 ms	244	Success
12	152.63.116.106 (0.so-4-0-0.CL2.L...	141 ms	243	Success
13	152.63.117.85 (POS7-0.GW2.LA...	94 ms	243	Success
14	157.130.245.186 (ge4-0-0.jr1.lax.l...	109 ms	241	Success
15	68.28.133.43 (3-0-0-1-1-1...	118 ms	238	Success

Tool: Advanced Administrative Tool (AA)

Advanced Administrative Tools is a multithreaded network and system diagnostic tool

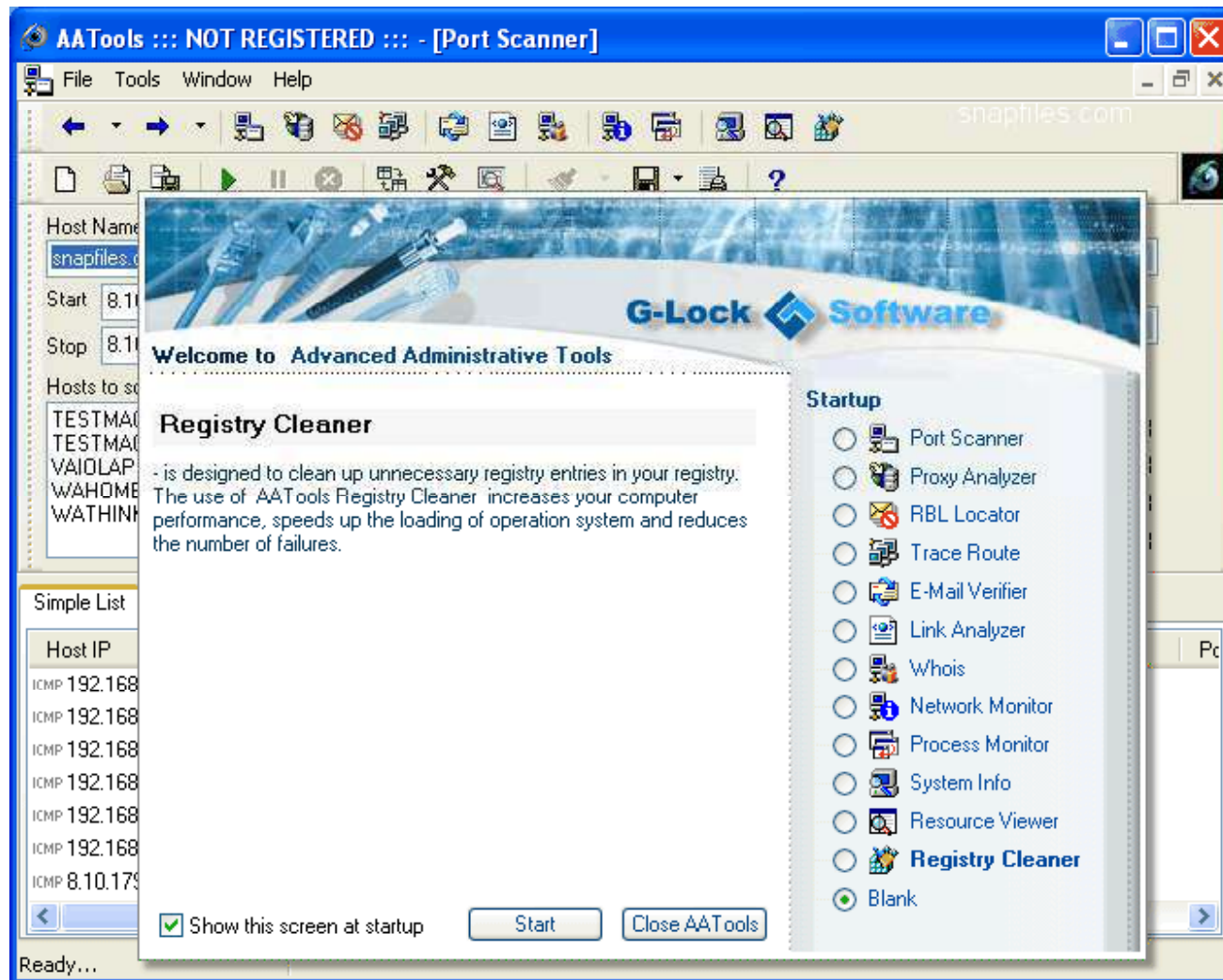
It is designed to gather detailed information and availability status for network and local computer

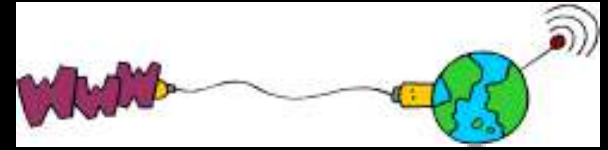
It combines 12 utilities:

- Port Scanner
- Proxy Analyzer
- RBL Locator
- CGI Analyzer
- Email Verifier
- Links Analyzer
- Network Monitor
- Process Monitor
- Whois
- System Info
- Resource Viewer
- Registry Cleaner



Advanced Administrative Tool: Screenshot





My IP Suite combines Domain-to-IP Converter, Batch Ping, Tracert, Whois, Website Scanner and Connection Monitor as well as an IP-to-Country Converter into a single interface

With powerful IP&Web tool you can:

- Lookup IP address for a single or list of domain names and vice versa
- Find out the country associated with a single or list of domains or IP addresses
- Perform batch and continuous pings on multiple servers
- Trace IP addresses to their destination and investigate connection problems
- Determine name, date, last-modified, version, and operation system of the remote web server
- Allow to scan any given web site and produce a list of links found in the site, using several criteria to filter results
- Monitor all TCP/IP connections from computer to the Internet automatically

My IP Suite: Screenshot 1

The screenshot shows the 'My IP Suite' application window. The main area is titled 'Website Scanner' and displays the URL 'http://www.shareit.com'. Below the URL, it reports '(1) 13164 links found. stopping... Done.' There are three sections for configuration: 'Page Scan' with options 'All Links', 'In the WebSite' (selected), and 'In the Same Path'; 'Links Type' with options 'All Links', 'In the Website' (selected), and 'In the Same Path'; and a 'Filter' section. To the right, the 'Http Head' section shows the following details: HTTP/1.1 200 OK, Date: Sat, 18 Oct 2003 17:16:45 GMT, Server: Apache, P3P: policyref="https://secure.element5.com/w3c/p3p.xml", CP="CAO DSP COR ADMo PSA CONo HIS OUR SAMo UNRo LEG UNI", Transfer-Encoding: chunked, Keep-Alive: timeout=10, max=69. The bottom section displays a list of found links with their file extensions (gif, htm).

Extension	URL
gif	http://www.shareit.com/pages/e-commercefulfillmentservices/e-commercefulfillmentservices.gif
gif	http://www.shareit.com/pages/freepalmpilotdownloads/freepalmpilotdownloads.gif
htm	http://www.shareit.com/pages/freepalmpilotdownloads/freepalmpilotdownloads.htm
gif	http://www.shareit.com/pages/internationaldistribution/internationaldistribution.gif
htm	http://www.shareit.com/pages/internationaldistribution/internationaldistribution.htm
gif	http://www.shareit.com/pages/softwarepublishing/softwarepublishing.gif
htm	http://www.shareit.com/pages/softwarepublishing/softwarepublishing.htm
htm	http://www.shareit.com/pages/palmfreeware/palmfreeware.htm
gif	http://www.shareit.com/pages/palmfreeware/palmfreeware.gif
gif	http://www.shareit.com/pages/fulfillmentsoftware/fulfillmentsoftware.gif
htm	http://www.shareit.com/pages/fulfillmentsoftware/fulfillmentsoftware.htm
gif	http://www.shareit.com/pages/windowscefreeware/windowscefreeware.gif
htm	http://www.shareit.com/pages/windowscefreeware/windowscefreeware.htm
htm	http://www.shareit.com/pages/handheldsoftware/handheldsoftware.htm

My IP Suite: Screenshot 2

My IP Suite

File Function View Help

IP-to-Domain Converter

Domain Name:

IP Address:
 216.109.118.68
 216.109.118.70
 216.109.118.71
 216.109.118.74
 216.109.118.76

Host Name:

IP Address:

Domain / Host Name:

IP Neighborhood: 20

IP Neighborhood will take an IP address and do a resolve for the last and next number IPs. This is not often found, but can be very useful to see what other website domains are hosted by the same ISP

Batch Conversion

From Domain / Host Name to IP Address

From IP Address to Domain / Host Name

Done!

Domain / Host Name	IP Address
tx1.udb.scd.yahoo.com	66.218.71.36
tx2.udb.scd.yahoo.com	66.218.71.37
tx3.udb.scd.yahoo.com	66.218.71.38
tx4.udb.scd.yahoo.com	66.218.71.39
tx5.udb.scd.yahoo.com	66.218.71.40
tx6.udb.scd.yahoo.com	66.218.71.41
tx7.udb.scd.yahoo.com	66.218.71.42
tx8.udb.scd.yahoo.com	66.218.71.43
nfs-tx100.udb.scd.yahoo.com	66.218.71.44
nfs-tx101.udb.scd.yahoo.com	66.218.71.45
udb1.udb.scd.yahoo.com	66.218.71.47
dns1.scd.yahoo.com	66.218.71.48

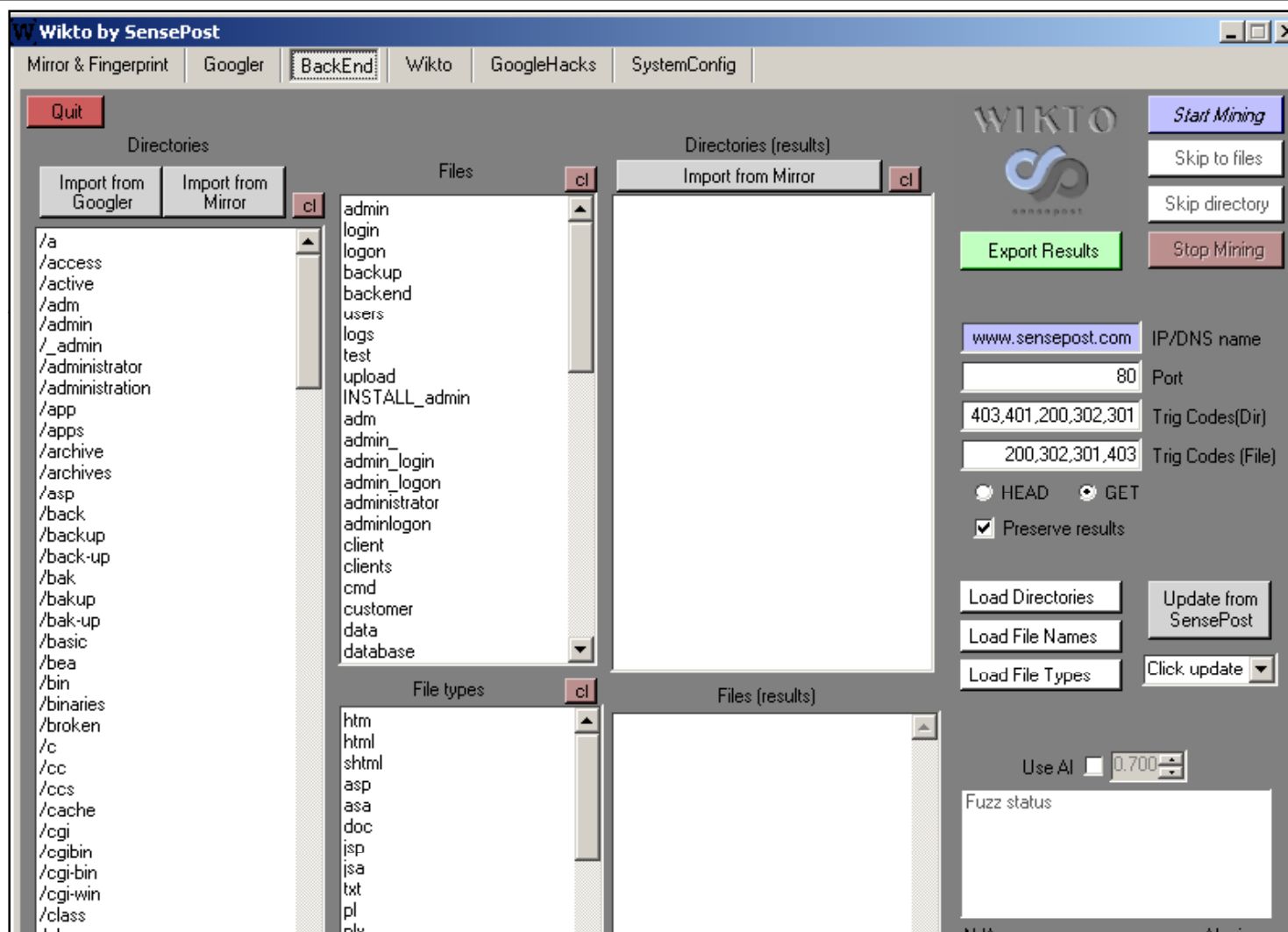
66.218.71.0
 66.218.71.1
 66.218.71.2
 66.218.71.3
 66.218.71.4
 66.218.71.5
 66.218.71.6
 66.218.71.7
 66.218.71.8
 66.218.71.9
 66.218.71.19
 66.218.71.20
 66.218.71.21
 66.218.71.22
 66.218.71.23
 66.218.71.24
 66.218.71.25
 66.218.71.26
 66.218.71.27

Total: 56

Finished: 47
 Successful: 47
 Failed: 0

Whois Tools

Wikto Footprinting Tool



Tool: Whois Lookup

With whois lookup, you can get personal details and contact information about the domain

- For example, www.samspace.com



Registrant:
targetcompany (targetcompany-DOM)
XXX Everest Blk A.Enclave
Ameerpet
Hyderabad
Andrapradesh,500038
IN
Domain Name: targetcompany.COM

Registrant:
targetcompany (targetcompany-DOM)
Street Address
City, Province
State, Pin, Country
Domain Name: targetcompany.COM

Administrative Contact:
R****, J**** (RJXX2-ORG) targetcompany@HDI.VSME.INDIA.IN
targetcompany
XXX, Everest Block, A.Enclave,
Ameerpet
Hyderabad, Andrapradesh 500038
IN 91 40 XXXX 329X Fax- 91 40 XXXX 329X
Technical Contact:
S*****, V**** (VSXX) techcontact@WEBINDIA.COM
XXXX Inc
XXX & Sons
Hoffman Estates, IL 60194
US. 408/XXX-XXXX 408/XXX-XXXX
Record expires on 14-Oct-200X.
Record created on 13-Oct-1997.
Database last updated on 12-Mar-2003 07:49:04 EST.

Administrative Contact:
Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX
Technical Contact:
Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

Domain servers in listed order:
NS1.WEBINDIA.COM 204.XXX.140.X01
NS2.WEBINDIA.COM 204.XXX.141.X01

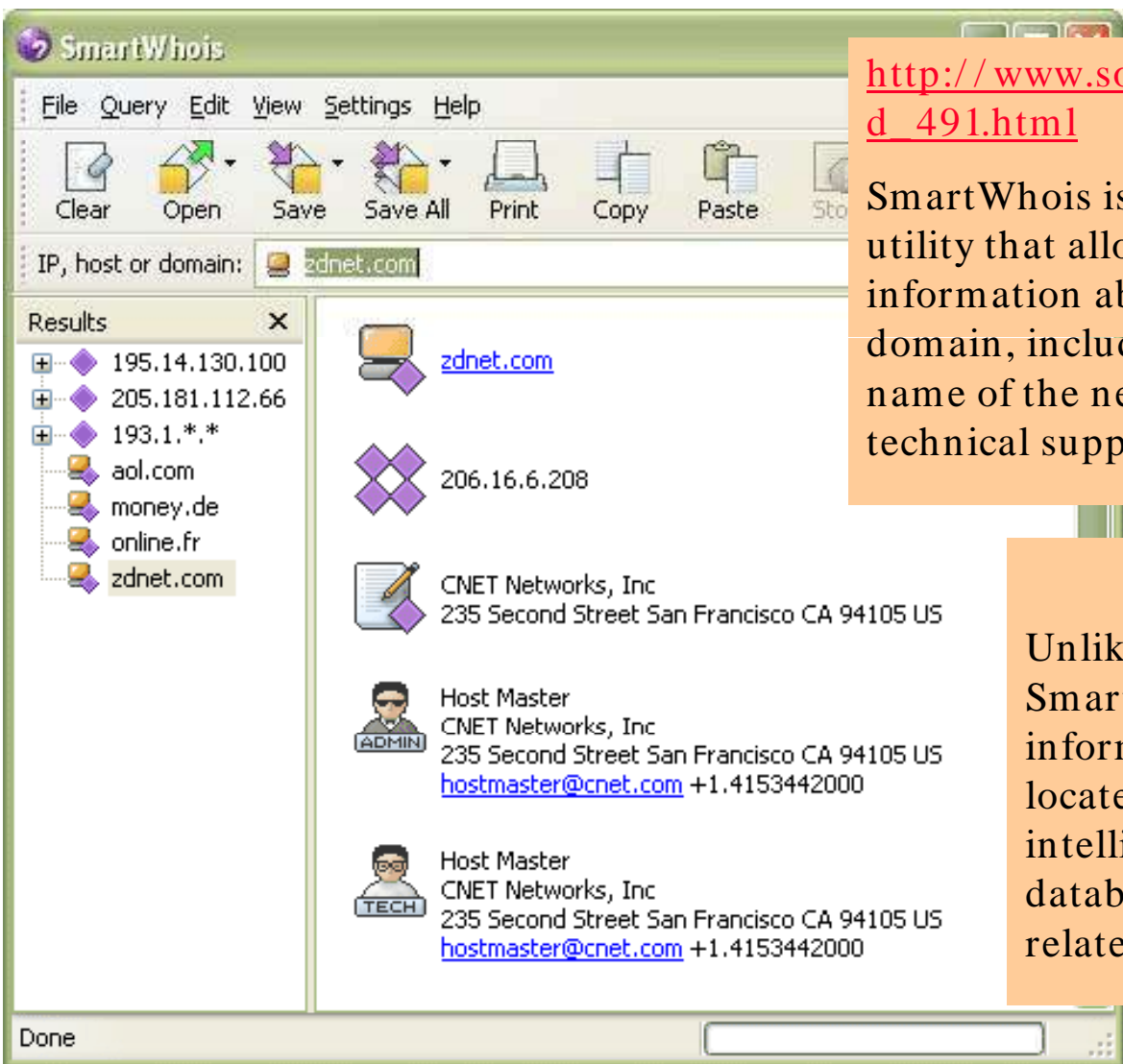
Domain servers in listed order:
NS1.WEBHOST.COM XXX.XXX.XXX.XXX
NS2.WEBHOST.COM XXX.XXX.XXX.XXX

Tool: SmartWhois

http://www.softdepia.com/smartwhois_download_491.html

SmartWhois is a useful network information utility that allows you to find out all available information about an IP address, host name, or domain, including country, state or province, city, name of the network provider, administrator, and technical support contact information

Unlike standard Whois utilities, SmartWhois can find the information about a computer located in any part of the world, intelligently querying the right database and delivering all the related records within a short time



Tool: ActiveWhois

ActiveWhois is a WHOIS tool that allows to retrieve domain specific information and displays it in an organized overview

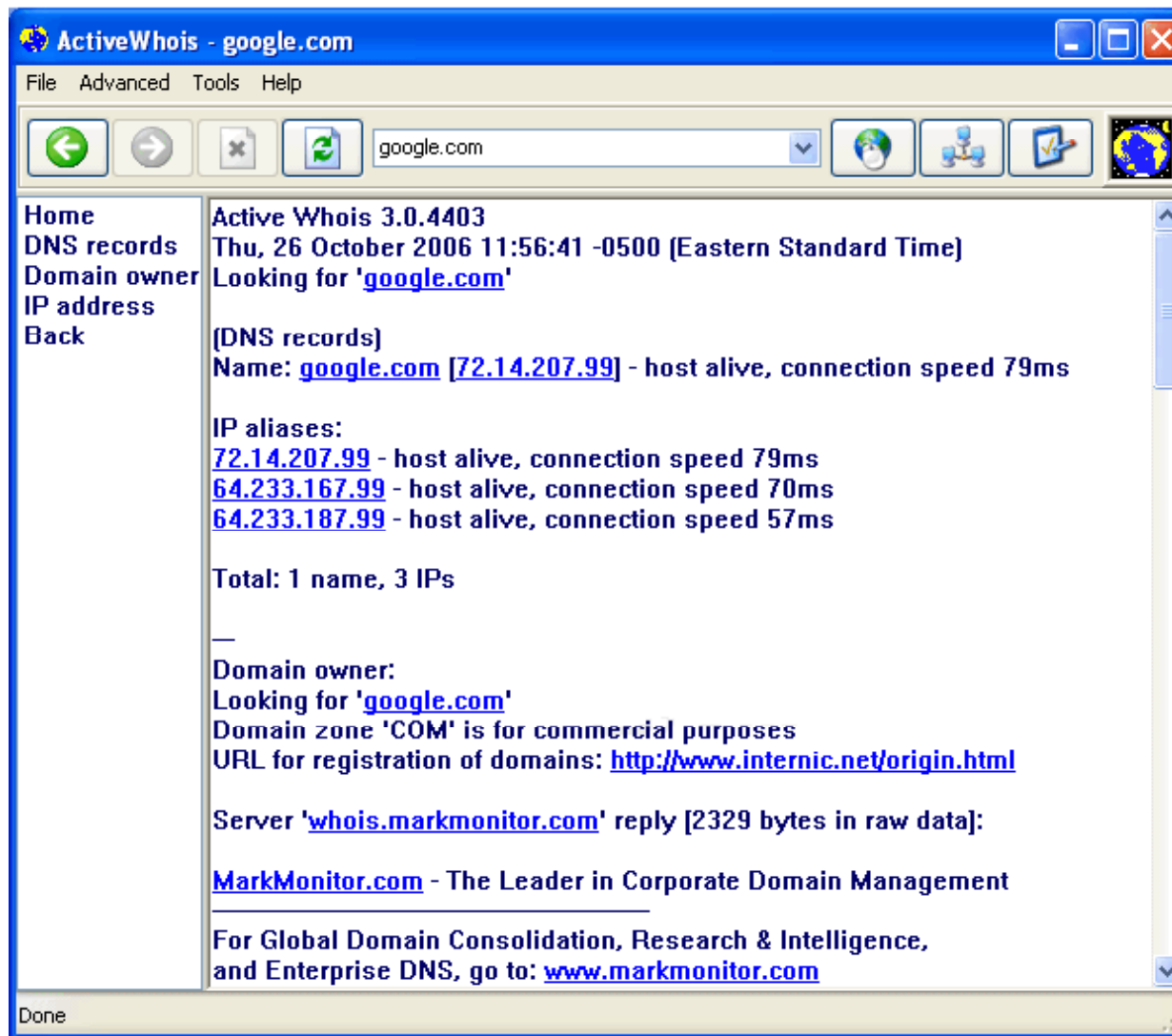
Information includes DNS information, IP address, and connection speed, as well as all standard domain owner information

The program hyperlinks all additional domains that are found in results (emails and URLs); launching a lookup for a linked domain quickly by simply clicking on it

ActiveWhois Browser also includes a Direct Whois option, which allows to manually specify server to query as well as supports international domains and Internet Explorer/ Firefox integration



ActiveWhois: Screenshot



Tool: Lan Whois

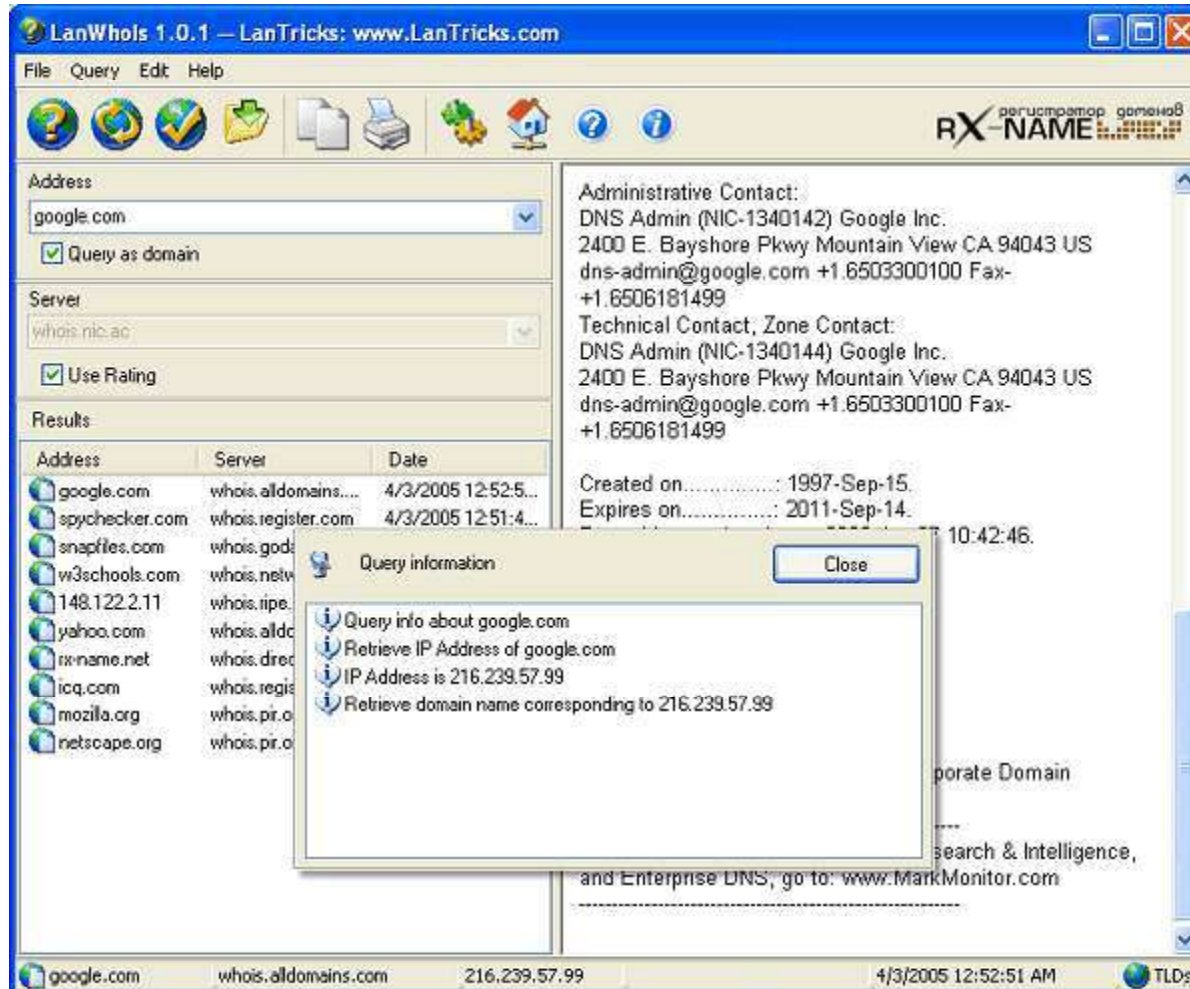
LanWhois allows to lookup owner's information for any given domain name or IP address

It archives results for easy reference and also allows to save or print information

This program includes a database of international WHOIS servers that can be updated online

In addition, LanWhois offers IE toolbar integration for easy access from the browser

Lan Whois: Screenshot



Tool: CountryWhois

CountryWhois is a utility for identifying the geographic location of an IP address

It is especially focused on IP-to-country identification and does not need to contact external Whois servers

Can be used to:

- Analyze server logs
- Check e-mail address headers
- Identify online credit card fraud
- Determine quickly and accurately the country of origin by IP address



CountryWhois: Screenshot

The following result show the product most probably uses a reverse lookup to resolve the IP addresses and manages to accurately identify the country of origin

The screenshot shows the CountryWhois application window. The 'Query' field contains 'zone-h.org'. Below it, a table lists the results of several queries. At the bottom, a 'Statistics' section displays a bar chart showing the distribution of countries: United States (30.00%), United Kingdom (40.00%), Canada (10.00%), Netherlands (10.00%), and Estonia (10.00%).

Query	Date	Status	IP Address	Country	Country Code
microsoft.com	04/01/2007 14:24:...	Completed	207.46.232.182	United States	US
logicallysecure.com	04/01/2007 14:25:...	Completed	91.84.23.170	United Kingdom	GB
bbc.co.uk	04/01/2007 14:25:...	Completed	212.58.228.155	United Kingdom	GB
vulnerabilityassessment.co....	04/01/2007 14:28:...	Completed	213.171.218.210	United Kingdom	GB
wirelessdefence.org	04/01/2007 14:30:...	Completed	213.171.218.183	United Kingdom	GB
securityfocus.com	04/01/2007 14:30:...	Completed	205.206.231.13	Canada	CA
sans.org	04/01/2007 14:30:...	Completed	64.112.229.131	United States	US
divepaint.nl	04/01/2007 14:30:...	Completed	213.193.212.208	Netherlands	NL
tamosoft.com	04/01/2007 14:31:...	Completed	66.39.102.85	United States	US
zone-h.org	04/01/2007 14:31:...	Completed	213.219.122.11	Estonia	EE

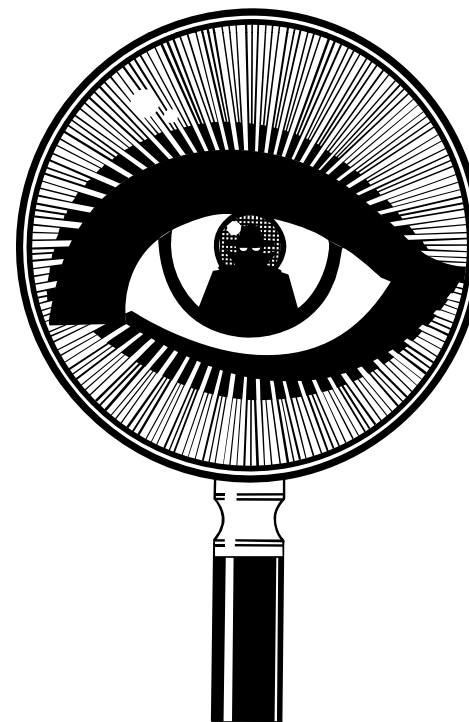
Country	Country Code	Count	Percent
United States	US	3	30.00%
United Kingdom	GB	4	40.00%
Canada	CA	1	10.00%
Netherlands	NL	1	10.00%
Estonia	EE	1	10.00%

Tool: WhereIsIP

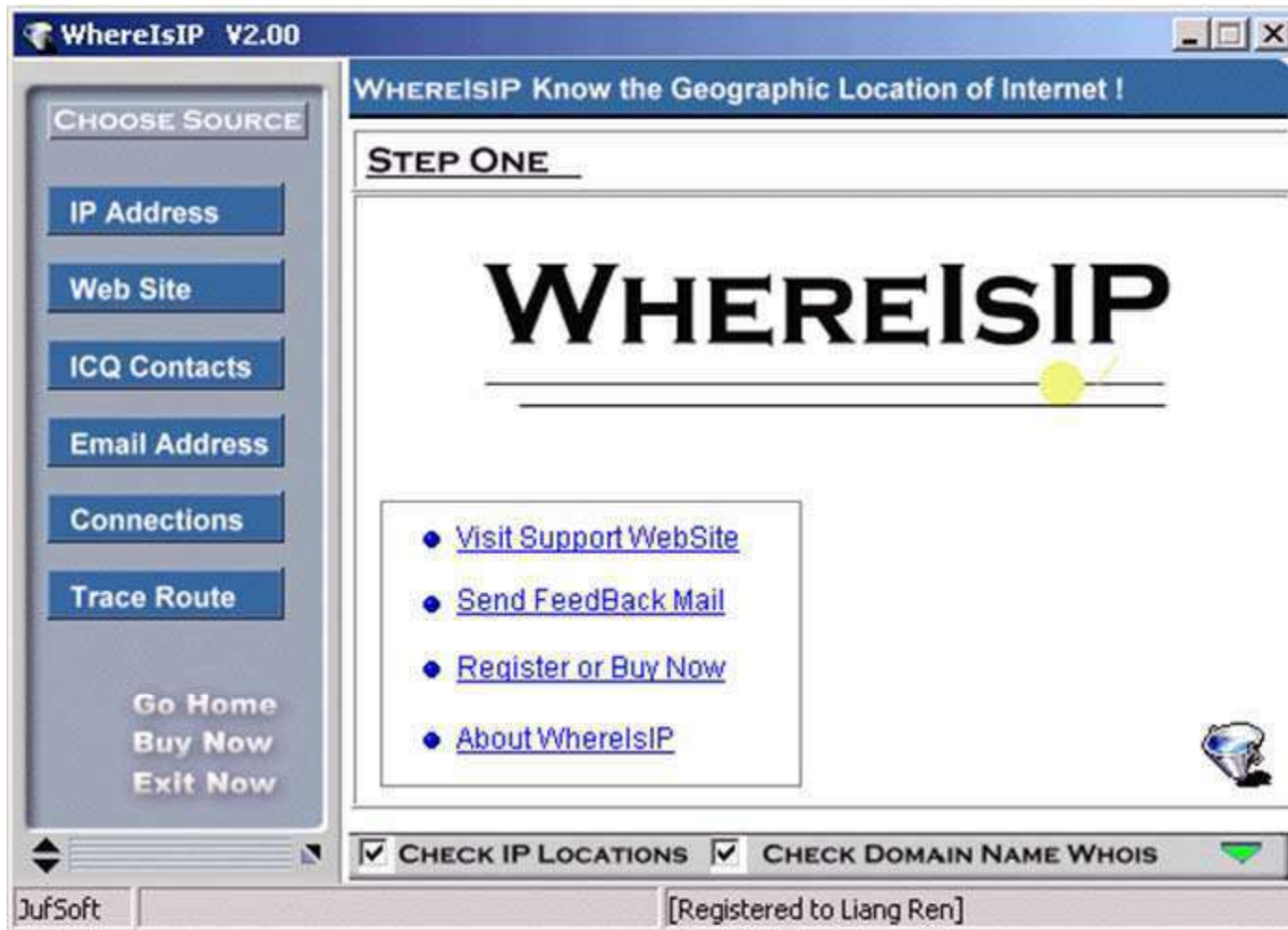
WhereIsIP helps to find out the geographic location of an IP address, domain name, ICQ contacts, website, and e-mail sender

Features:

- Powerful Internet address geographic location analysis ability
- Domain Name research function; it can reverse-resolve a IP address to domain name



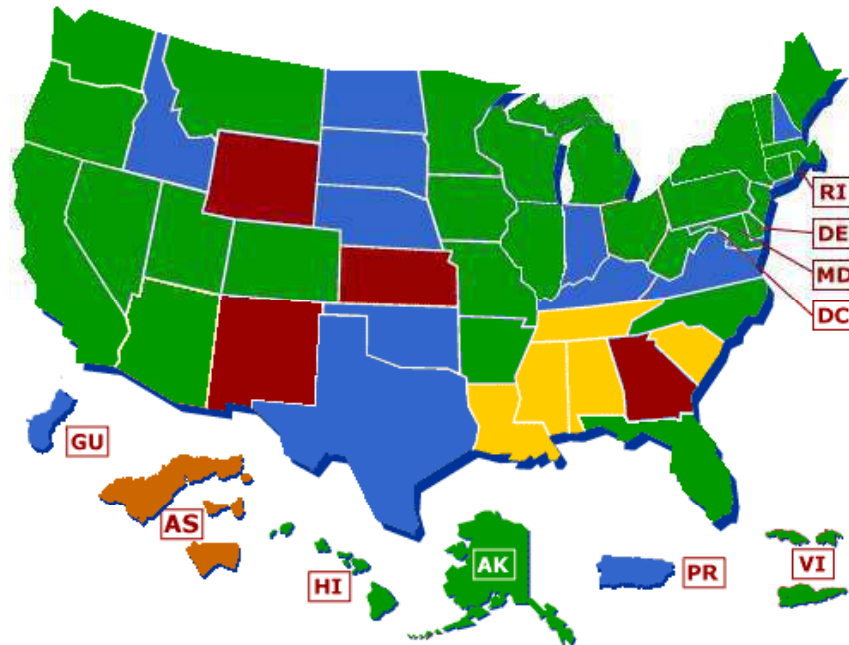
WhereIsIP: Screenshot



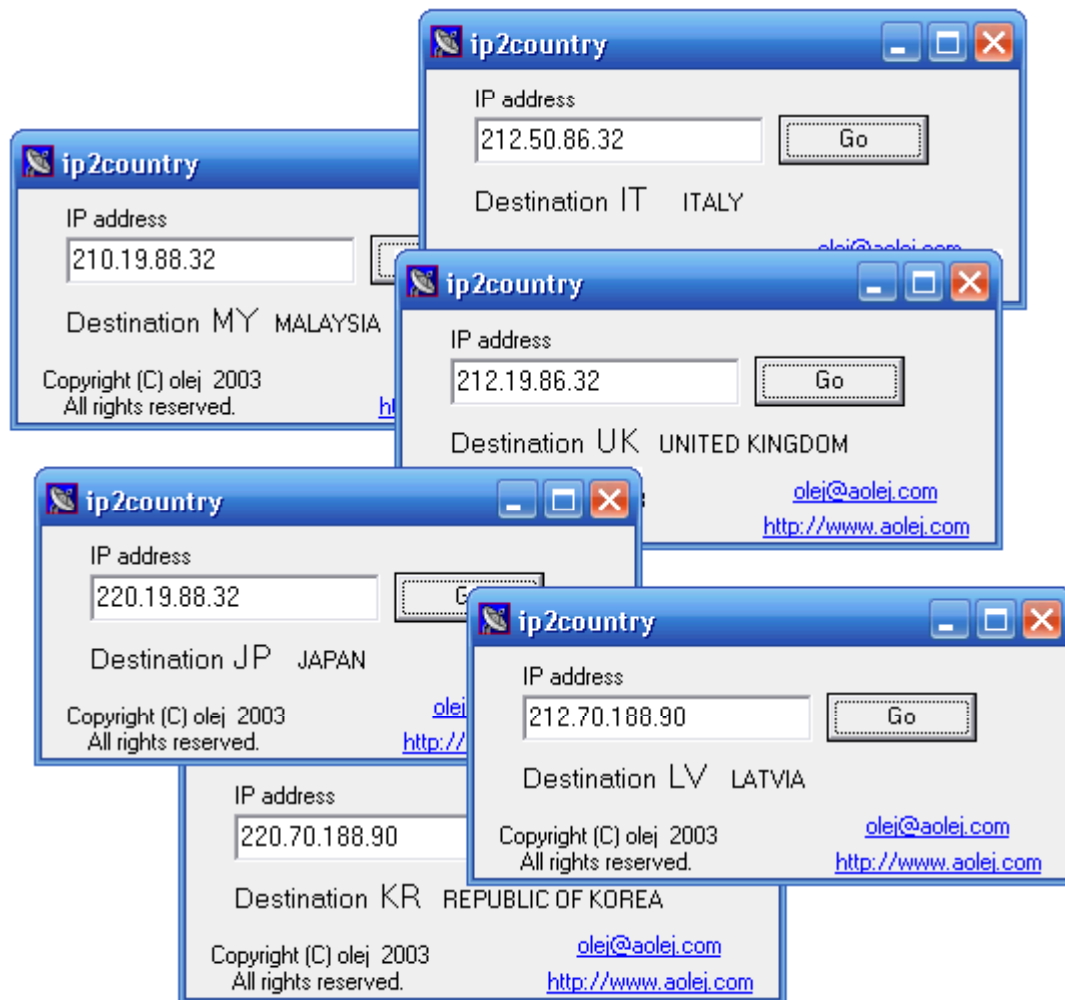
Tool: ip2country

ip2country is utility for converting IP's address to the country's name

Enter any IP address and the country's name is displayed



Ip2country: Screenshot



Tool: CallerIP

Use CallerIP to easily see when someone has connected to the computer, report IP address, and run a trace on that IP address

Using CallerIP Professional, CallerIP can be setup as a server, so you can monitor computer and its connections

Features:

- Receives instant alerts for high risk connections and back doors
- Identifies spyware and suspicious connections to your system
- Reports abuse and illicit activity



CallerIP: Screenshot 1

The screenshot shows the CallerIP Professional Edition application window. The main area features a world map with call origin labels for 'United States (2)' and 'Switzerland (2)'. A menu is open over the map, with 'Show Current Callers' selected. Below the map is a table of current callers and two side panels: 'Identification Report' and 'Callers History'.

Current Callers

Establish	In/O	Cou	Remote IP	Remote F	Local IP	Local Poi	Application	State
00:18.11	?	-	85.204.225.34	5222	10.9.0.39	49158	-	Establish
00:18.11	?	loca	10.9.0.11	55423	10.9.0.39	49348	-	Establish
00:18.11	?	CH	82.197.167.13	80	10.9.0.39	49369	-	Establish
00:18.11	?	CH	194.209.78.14	80	10.9.0.39	50821	-	Time Wai
00:18.11	?	US	209.85.129.16	80	10.9.0.39	50823	-	Time Wai
00:18.11	?	US	209.85.129.16	80	10.9.0.39	50827	-	Time Wai

Callers History

- [209.85.129.164](#) (US)
- [194.209.78.14](#) (CH)

CallerIP: Screenshot 2

The screenshot shows the CallerIP application window. At the top, there is a menu bar with 'File', 'Options', and 'Help'. Below the menu bar is an address input field containing '68.1.17.2' and a 'go' button. A status bar below the address field reads 'Finished. For detailed route information: [run VisualRoute](#).' The main area features a world map with a red crosshair centered on Atlanta, GA, USA. To the right of the map are two panels: 'Identification Report' and 'Callers History'. The 'Identification Report' panel contains the following information:

Found: Address 68.1.17.2 (pop.east.cox.net) has been found in Atlanta, GA, USA.

Network Contact Information: The following details refer to the network that the system is on:

- abuse@cox.net
- +1-404-269-7626
- 1400 Lake Hearn Drive
Atlanta

Below the map is a table of active connections:

Established	In/Out	Co	Remote IP	Remote	Local IP	Local I	Process (PID)	State
03:57:1	out	US	216.239.37.1	80	192.168.1.10	4233	CCPXY\SVCS.EXE (Establish
03:57:4t	out	US	198.64.153.9	80	192.168.1.10	4237	CCPXY\SVCS.EXE (Establish
03:57:4t	out	US	198.64.153.9	80	192.168.1.10	4239	CCPXY\SVCS.EXE (Establish

At the bottom left of the window, it says '9 active connections [\(Hide connections table\)](#)'. At the bottom right, there are links for '(Hide report)' and '(Hide callers history)'. The 'Callers History' panel lists several IP addresses with colored status indicators: 216.239.37.147 (orange), 68.1.17.2 (green), 198.64.153.97 (green), 216.239.39.147 (orange), and 216.239.39.99 (orange). There are 'Clear' and 'Hide' buttons at the bottom of this panel.

CallerIP: Screenshot 3

CallerIP's unique IP tracking capability shows the geographical location of a connection so you see can where connections to your system originate

Real-time system monitoring shows remote connections to your system, including the country of origin so you can quickly identify suspect connections.

The network provider is identified for each connection, including contact and abuse reporting information.

High risk and unknown connections are automatically identified, and you can create your own rules for instant notification of a connection by country, port, IP address or process

Establ	In.	Co	Remote IP	Remot	Local IP	Local	Application	State
02:54.5	out	US	216.239.51	80	192.168.1.1	3206	[System]	Time W
02:54.1	out	US	82.165.240	43	192.168.1.1	3223	[System]	Time W
02:54.1	out	US	82.165.240	43	192.168.1.1	3224	[System]	Time W
02:54.1	out	US	82.165					Time W
02:54.1	out	US	82.165					Time W
02:54.1	out	US	82.165					Time W
02:55.0	out	US	82.165					Time W
02:55.1	out	US	82.165					Time W
02:55.1	out	US	82.165					Time W
02:55.1	out	US	82.165					Time W

0 active connections (Hide connections table)

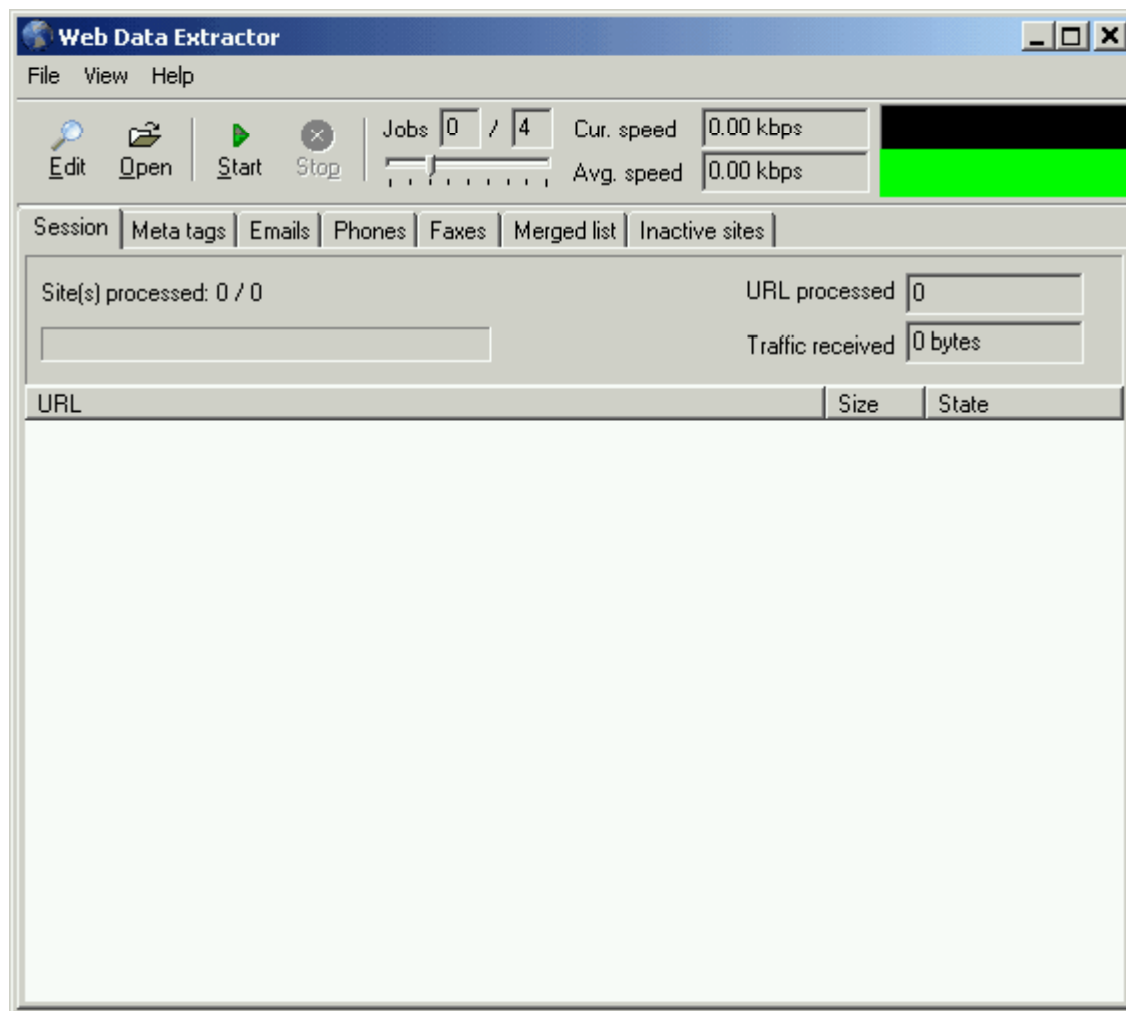
Identification Report
Network Contact Information: The following details refer to the network that the system is on.
 ipar@ccnic.net.cn
 +86-10-62559892
 No.4, Zhongguancun No.4 South Street, Haidian District, Beijing

Callers History
 Connections have been made to or from the following systems. Click one to produce a report.
 64.233.161.104 (US)
 198.65.117.117 (US)
 130.94.30.213 (US)
 198.64.153.97 (US)
 68.1.17.2 (US)

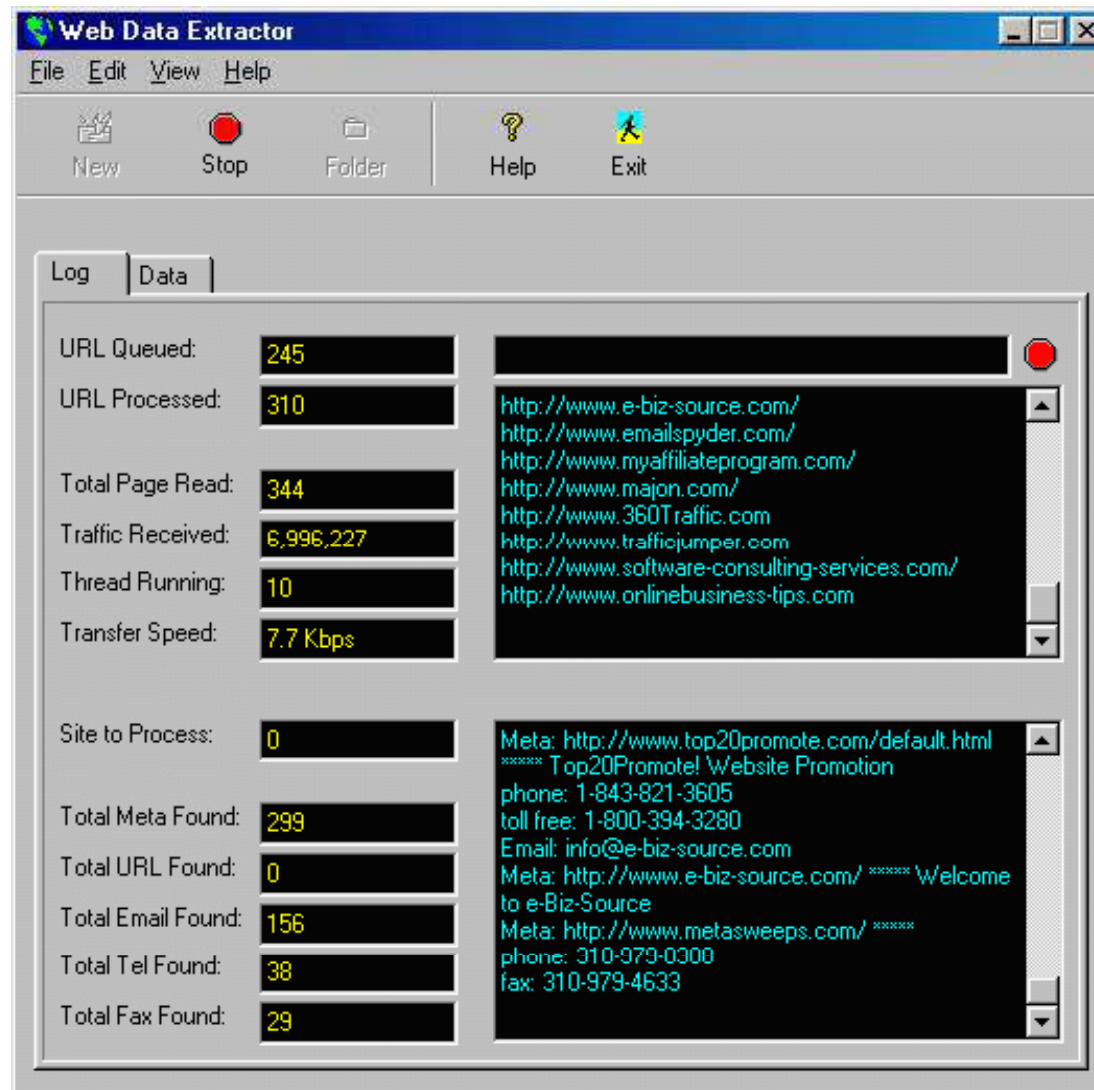
Web Data Extractor Tool

Use this tool to extract the targeted company's contact data (email, phone, fax) from the Internet

Extract url, meta tag (title, desc, keyword) for website promotion, search directory creation, web research



Web Data Extractor Tool: Screenshot



www.samspade.org

www.geektools.com

www.whois.net

www.demon.net



Sam Spade.org

This is a slightly trimmed down version of the SamSpade.org site, while I deal with some issues.

- [The SamSpade.org FAQ](#)
- [Lots of online tools](#)
- [Sam Spade for Windows](#)
- [The Library](#)
- [Link to SamSpade.org](#)

Get SamSpade.org stuff - T-shirts, mugs, mouse pads, boxer shorts, frisbees...

Who is the real Sam Spade? A character created by writer [Dashiell Hammett](#).

Need spam filtering or antivirus software? Try [SpamResource.com](#)

<input type="text"/>	Do Stuff
<input type="text"/>	at <input type="text" value="Magic"/> Whois
<input type="text"/>	IP Whois
<input type="text" value="http://"/>	Decipher
<input type="text" value="http://"/>	Browse
Unavailable <input type="text"/>	Traceroute
<input type="text"/>	Author Search
<input type="text"/>	Locate USPIs
<input type="text"/>	Blackhole

Tool: What is MyIP

WhatIsMyIP.com

The fastest and easiest way to determine your IP address.

Home

IP Command Lines

IP Addresses Explained

Speed Test

What's New

Your IP Is 202.53.13.138

Application Analysis

Manage and troubleshoot applications on the network.

www.networkinstruments.com

Verification IP

World's largest collection of VIPs Verilog, VHDL & SystemVerilog

www.nsysinc.com

1.5 Mbps 900MHz Ethernet

Ultra Long Range; Easily Penetrates Up to 10 Walls or Grove of Trees

www.avalanwireless.com

Hoortech- Saudi Arabia

Access Control, Time & Attendance CCTV, Surveillance-IP Based Systems

www.hoortech.com

Ads by Google

Google Search

DNS Information Extraction Tools

Tool: DNS Enumerator

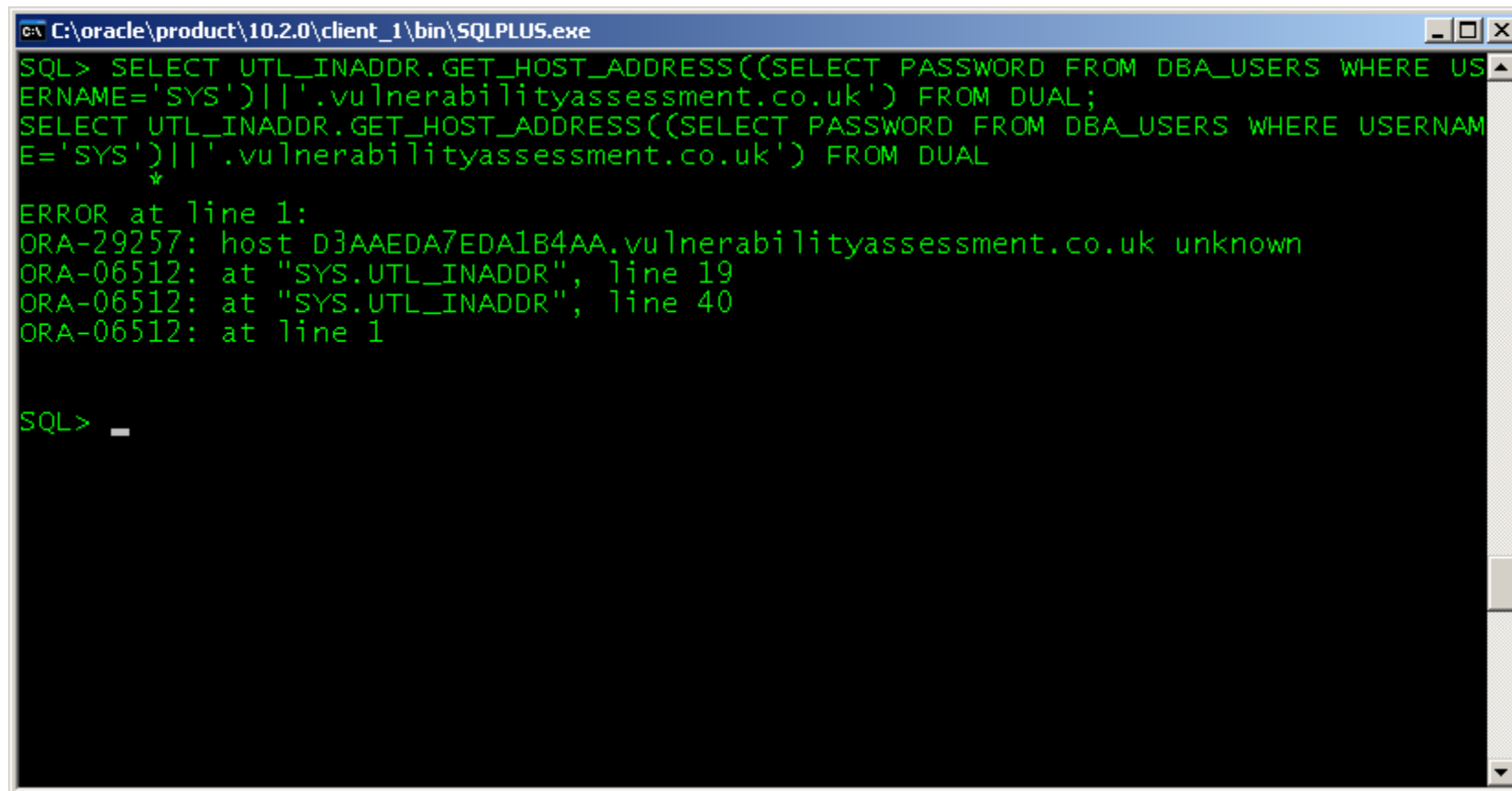
DNS Enumerator is an automated sub-domain retrieval tool

It scans Google to extract the results

```
SELECT UTL_INADDR.GET_HOST_ADDRESS((SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL
*
ERROR at line 1:
ORA-29257: host D3AAEDA7EDA1B4AA.vulnerabilityassessment.co.uk unknown
ORA-06512: at "SYS.UTL_INADDR", line 19
ORA-06512: at "SYS.UTL_INADDR", line 40
ORA-06512: at line 1

SQL> _
```

DNS Enumerator: Screenshot

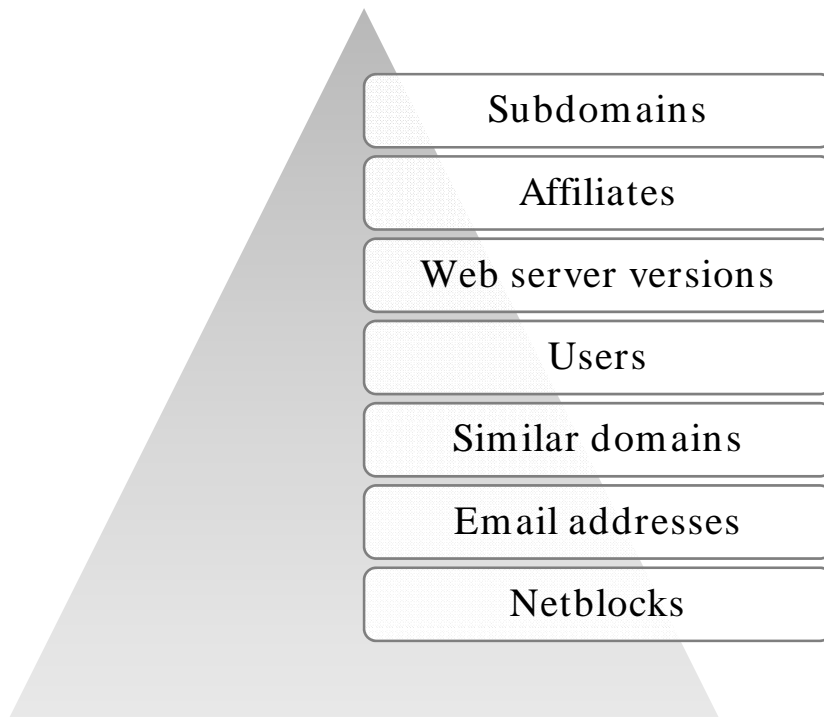


```
C:\oracle\product\10.2.0\client_1\bin\SQLPLUS.exe
SQL> SELECT UTL_INADDR.GET_HOST_ADDRESS((SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL;
SELECT UTL_INADDR.GET_HOST_ADDRESS((SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL
*
ERROR at line 1:
ORA-29257: host D3AAEDA7EDA1B4AA.vulnerabilityassessment.co.uk unknown
ORA-06512: at "SYS.UTL_INADDR", line 19
ORA-06512: at "SYS.UTL_INADDR", line 40
ORA-06512: at line 1

SQL> _
```


Tool: SpiderFoot

SpiderFoot is a free, open-source, and domain footprinting tool which will scrape the websites on that domain, as well as search Google, Netcraft, Whois, and DNS to build up information like:



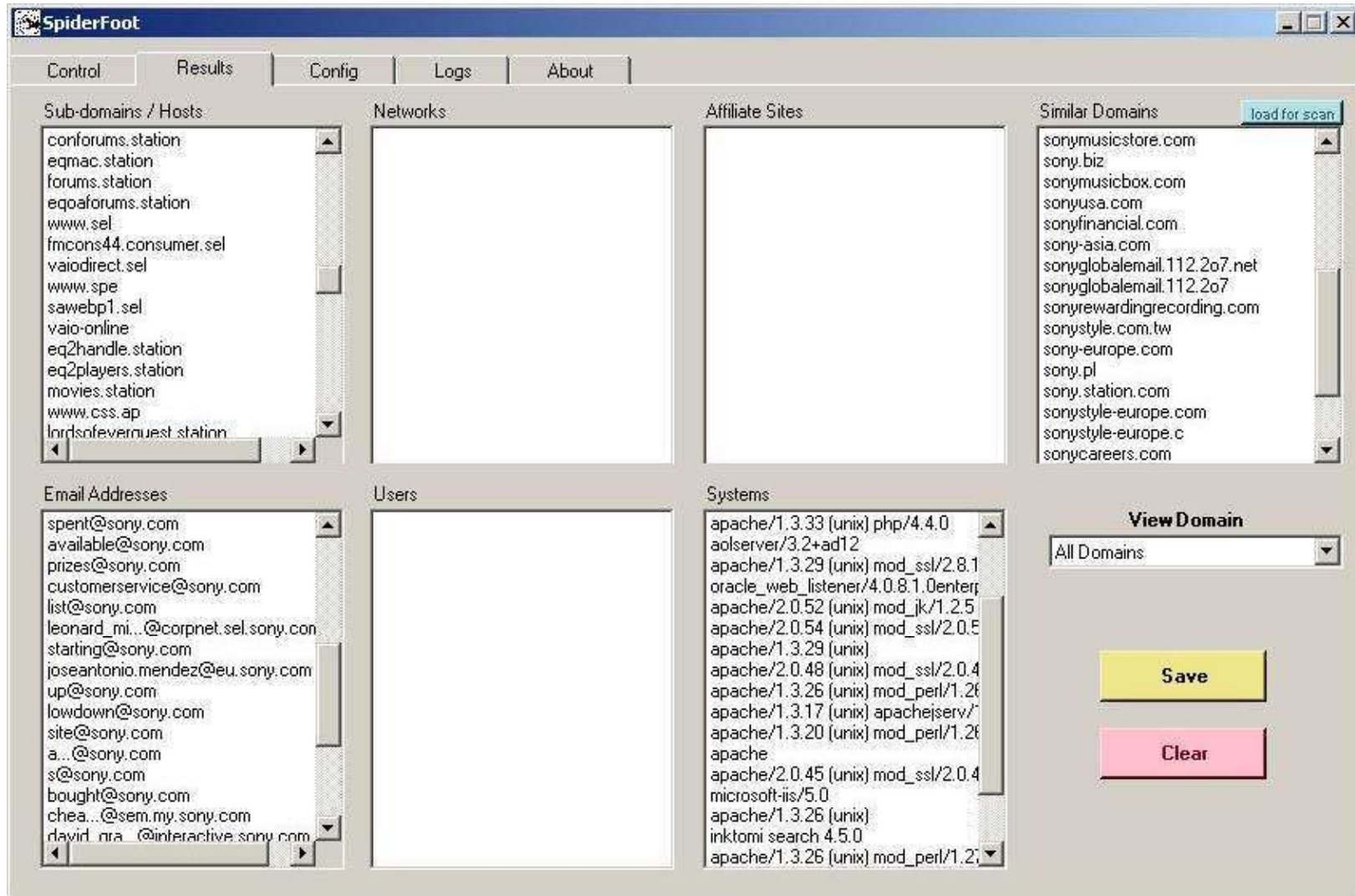
SpiderFoot: Screenshot 1

The screenshot shows the SpiderFoot application window with the following components:

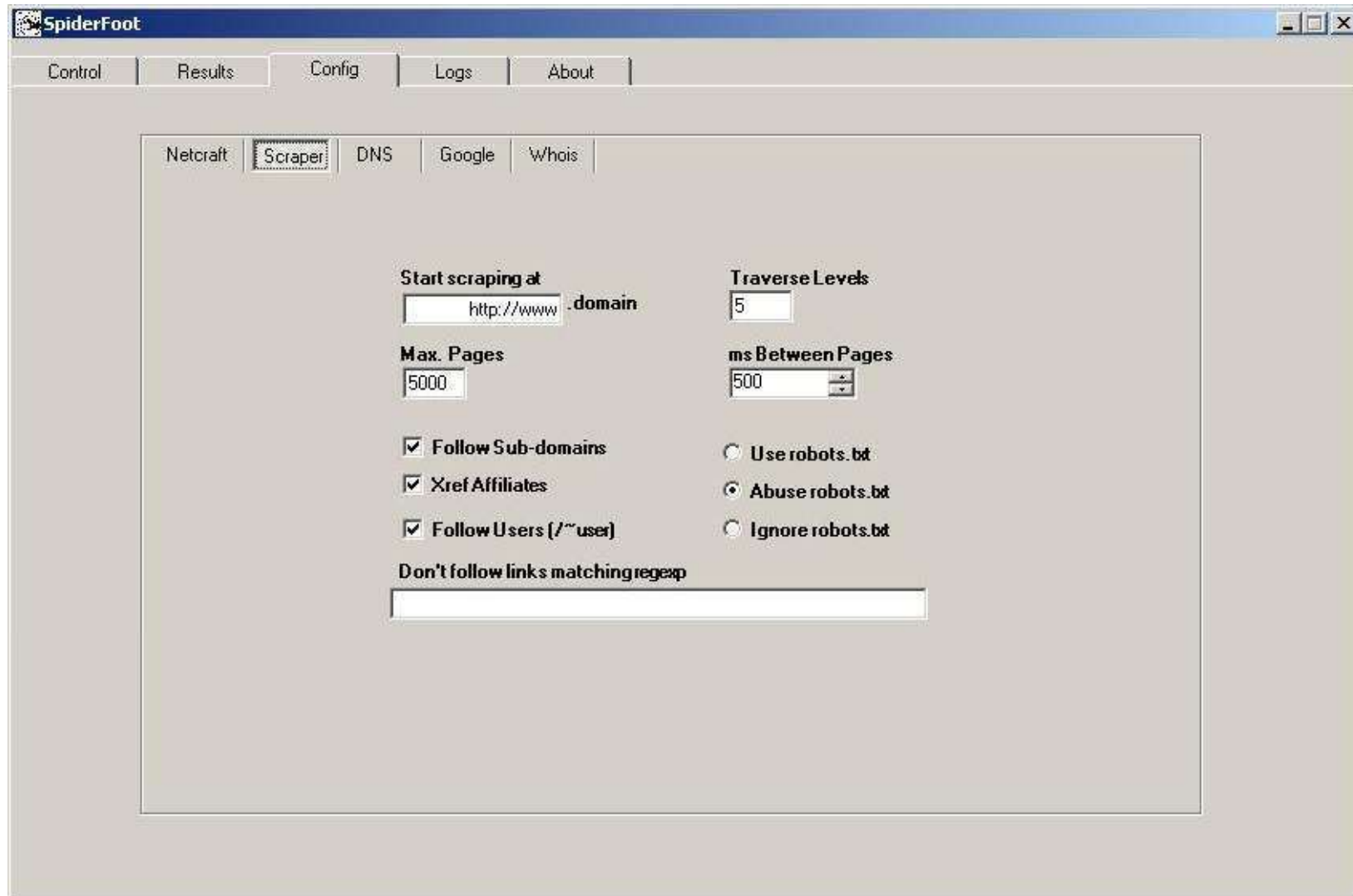
- Control Panel:** Tabs for Control, Results, Config, Logs, and About.
- Domain Names:** A list containing dell.com, ibm.com, toshiba.com, and acer.com. Includes 'Add', 'Del', 'up', and 'down' buttons.
- Discovery Methods:** Checkboxes for Google Web, Website Scraping, Google News, Whois, DNS, and Netcraft, each with a progress bar.
- Total Progress:** A large progress bar at the bottom of the discovery methods section.
- Page fetch results:** A table with columns Method, URL, and Result.
- Buttons:** 'load from file', 'Abort', and 'Clear' buttons.
- Status Bar:** Shows 'Ready', '195', '7957066', and '22'.

Method	URL	Result
Google Web	http://www.dell.com.sg/	OK
Google Web	http://www.dell.com/64bit/	OK
Google Web	http://premier.dell.com/premier/	OK
Google Web	http://www1.us.dell.com/content/default.aspx?c=us&cs=k12home...	OK
Google Web	http://www1.us.dell.com/content/topics/global.aspx/corp/enviro...	OK
Netcraft	http://searchdns.netcraft.com/?restriction=site+ends+with&host=d...	OK
Netcraft	http://bt-www.us.dell.com/	OK
Netcraft	http://catalog.us.dell.com	The remote server returned an error: (403) Forbidden.

SpiderFoot: Screenshot 2



SpiderFoot: Screenshot 3



Tool: Nslookup

Nslookup is a program to query Internet domain name servers. Displays information that can be used to diagnose Domain Name System (DNS) infrastructure

It helps find additional IP addresses if authoritative DNS is known from whois

MX record reveals the IP of the mail server

Both Unix and Windows come with a Nslookup client

Third party clients are also available – for example, Sam Spade

Nslookup: Screenshot

```
cmd.exe - nslookup

C:\WINDOWS>nslookup
Default Server:  zeus.pngcom.com
Address:  206.62.8.10

> www.techrepublic.com
Server:  zeus.pngcom.com
Address:  206.62.8.10

Non-authoritative answer:
Name:    c17-sha-redirect-lb.cnet.com
Address: 216.239.113.101
Aliases: www.techrepublic.com

>
```

Extract DNS Information

Using www.dnsstuff.com, you can extract DNS information such as:

- Mail server extensions
- IP addresses

The screenshot displays the www.dnsstuff.com website interface, organized into three columns: Domain Name Tests, IP Tests, and Hostname Tests. Each tool includes a title, a brief description, an input field, and a 'Lookup' button.

Domain Name Tests (e.g. example.com)	IP Tests (e.g. 192.168.100.1)	Hostname Tests (e.g. www.example.com)
DNS Report See if there are problems with your DNS hosting. www.DNSreport.com	Spam database lookup See if a machine is in any spam database.	DNS lookup Look up a DNS record (A, MX, NS, SOA, etc.)
DNS Timing Check speed of your DNS hosting.	Reverse DNS lookup See if your IP has a reverse DNS entry.	Traceroute Traces the route packets take to this host.
WHOIS Lookup Lists contact info for a domain/IP (about 200 TLDs).	IPWHOIS Lookup Lists contact info for an IP (or domain).	Ping Shows how long it takes for packets to reach a host.
Abuse Lookup Finds abuse contact for a domain from abuse.net.	City From IP Uses geolocation to find the city and country of an IP.	ISP cached DNS lookup Check cached DNS at major ISPs.
	NEW! IP Information Shows lots of information about an IP.	



Extract DNS Information: Snapshot

DNS Lookup: eccouncil.org MX record

Generated by www.DNSstuff.com

How I am searching:

Searching for eccouncil.org MX record at e.root-servers.net [192.203.230.10]: Got referral to TLD1.ULTRADNS.NET. [took 101 ms]
Searching for eccouncil.org MX record at TLD1.ULTRADNS.NET. [204.74.112.1]: Got referral to AUTH2.NS.NYI.NET. [took 44 ms]
Searching for eccouncil.org MX record at AUTH2.NS.NYI.NET. [66.111.15.154]: Reports mail.eccouncil.org. [took 51 ms]

Answer:

Domain	Type	Class	TTL	Answer
eccouncil.org	MX	IN	3600	mail.eccouncil.org [Preference = 5]
eccouncil.org	NS	IN	3600	auth2.ns.nyi.net.
eccouncil.org	NS	IN	3600	auth1.ns.nyi.net.
mail.eccouncil.org	A	IN	3600	66.111.15.34

To see the DNS traversal, to make sure that all DNS servers are reporting the correct results, you can [Click Here](#).

Note that these results are obtained in real-time, meaning that these are **not** cached results. These results are what DNS resolvers all over the world will see right now (unless they have cached information).

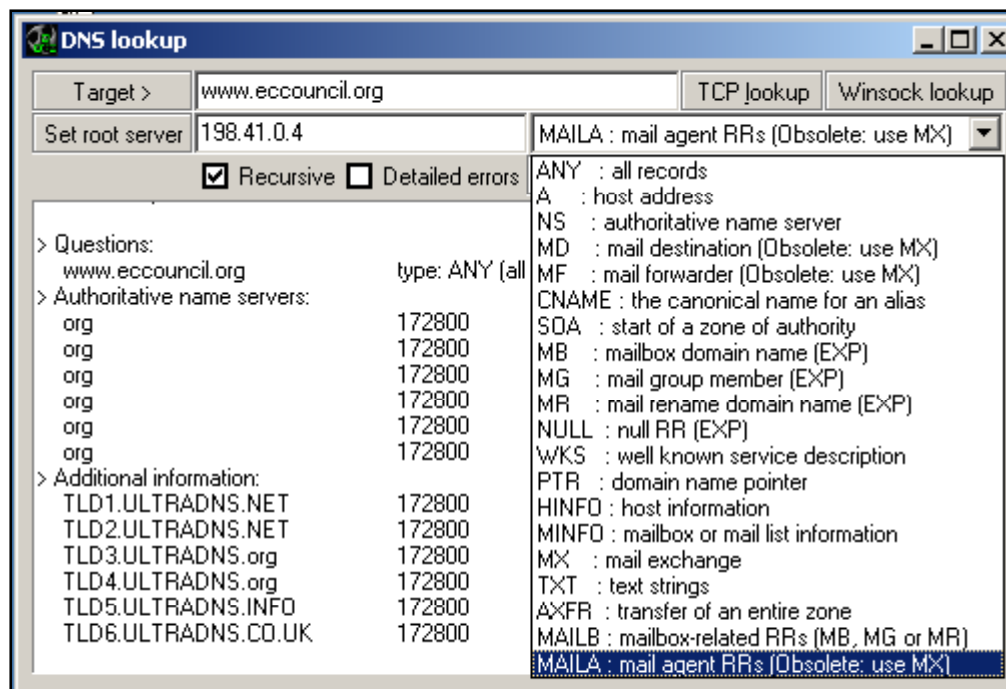
(C) Copyright 2000-2005 R. Scott Perry

Types of DNS Records

A	A host's IP address. An address record allowing a computer name to be translated into an IP address. Each computer must have this record for its IP address to be located.
MX	Host's or domain's mail exchanger(s).
NS	Host's or domain's name server(s).
CNAME	Host's canonical name allows additional names or aliases to be used to locate a computer.
SOA	Indicates authority for the domain.
SRV	Service location record.
RP	Responsible person.
PTR	Host's domain name, host identified by its IP address.
TXT	Generic text record.
HINFO	Host information record with CPU type and operating system

Tool: Necrosoft Advanced DIG

Necrosoft Advanced DIG (ADIG) is a TCP-based DNS client that supports most of the available options, including AXFR zone transfer



Tool: Expired Domains

Expired Domains enable to search through a list of expiring domain names by keyword, domain, character length, and other criteria

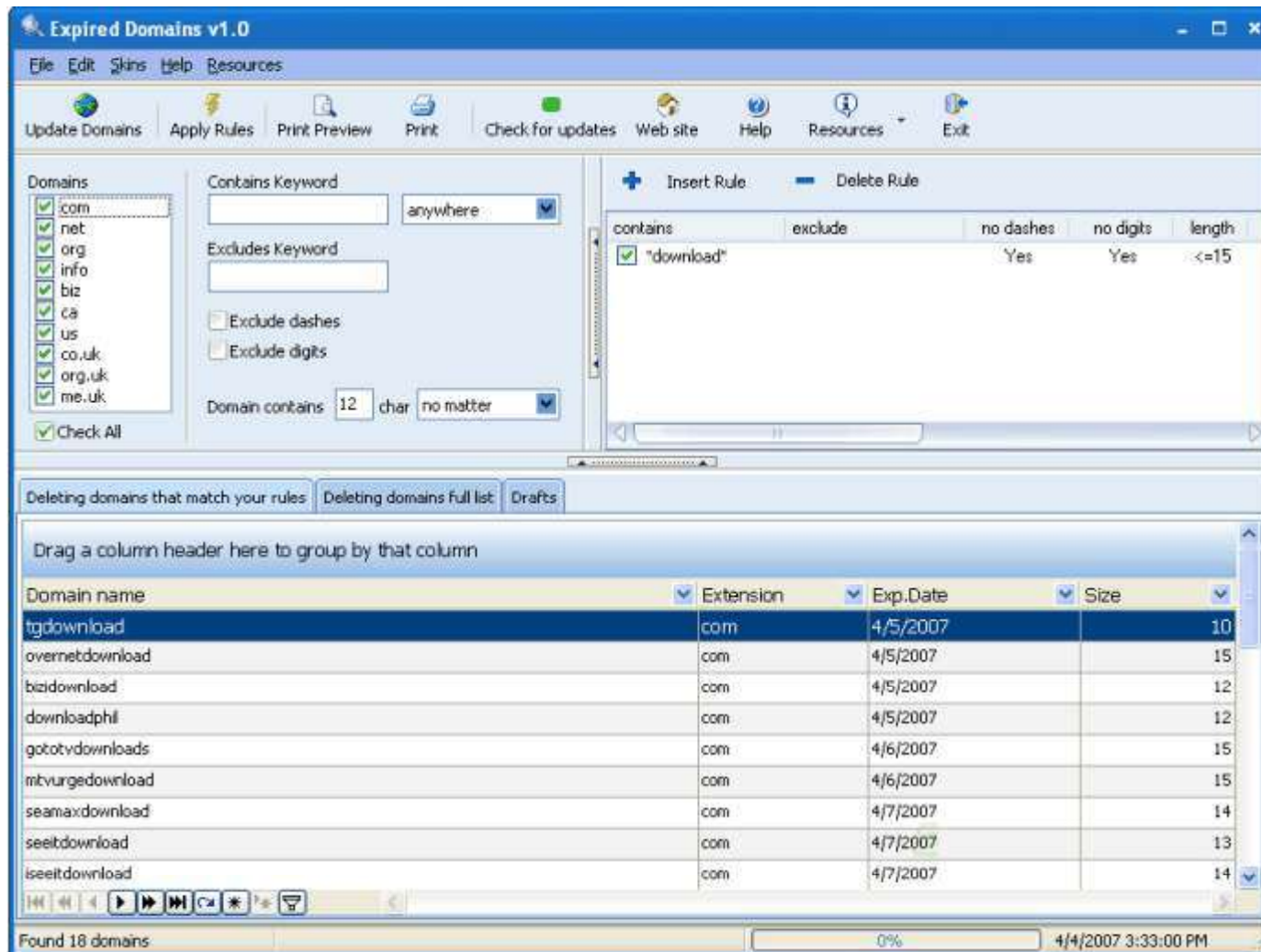
The program can download an updated list of domain names with the click of a button

Multiple filter rules can be created to find domain names that are of interest

List can be printed, exported, and selected and domain can be saved in a draft list



Expired Domains: Screenshot



Tool: DomainKing

DomainKing is a domain name lookup tool that can help to find available domain names, including domains that are about to expire

It can import or extract domain names from a text file and generate them based on keywords

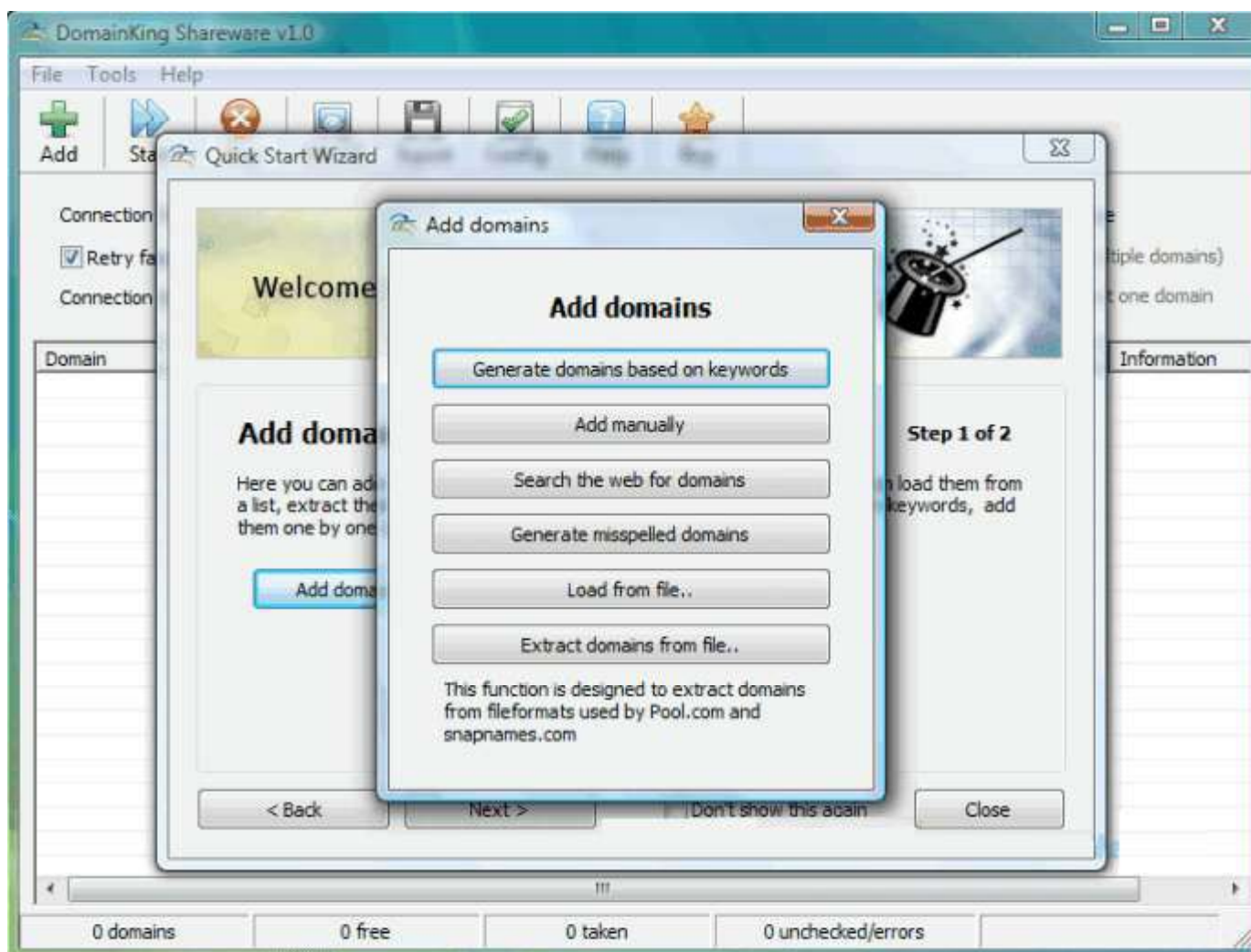
Extract domain names from search engine results, which enable to search for domain names that are expired but still indexed by search engines

DomainKing allows to generate mistyped variations of a domain name

It supports more than 100 domain extensions and provides a fast lookup with color coded results and integrated WHOIS lookup



DomainKing: Screenshot





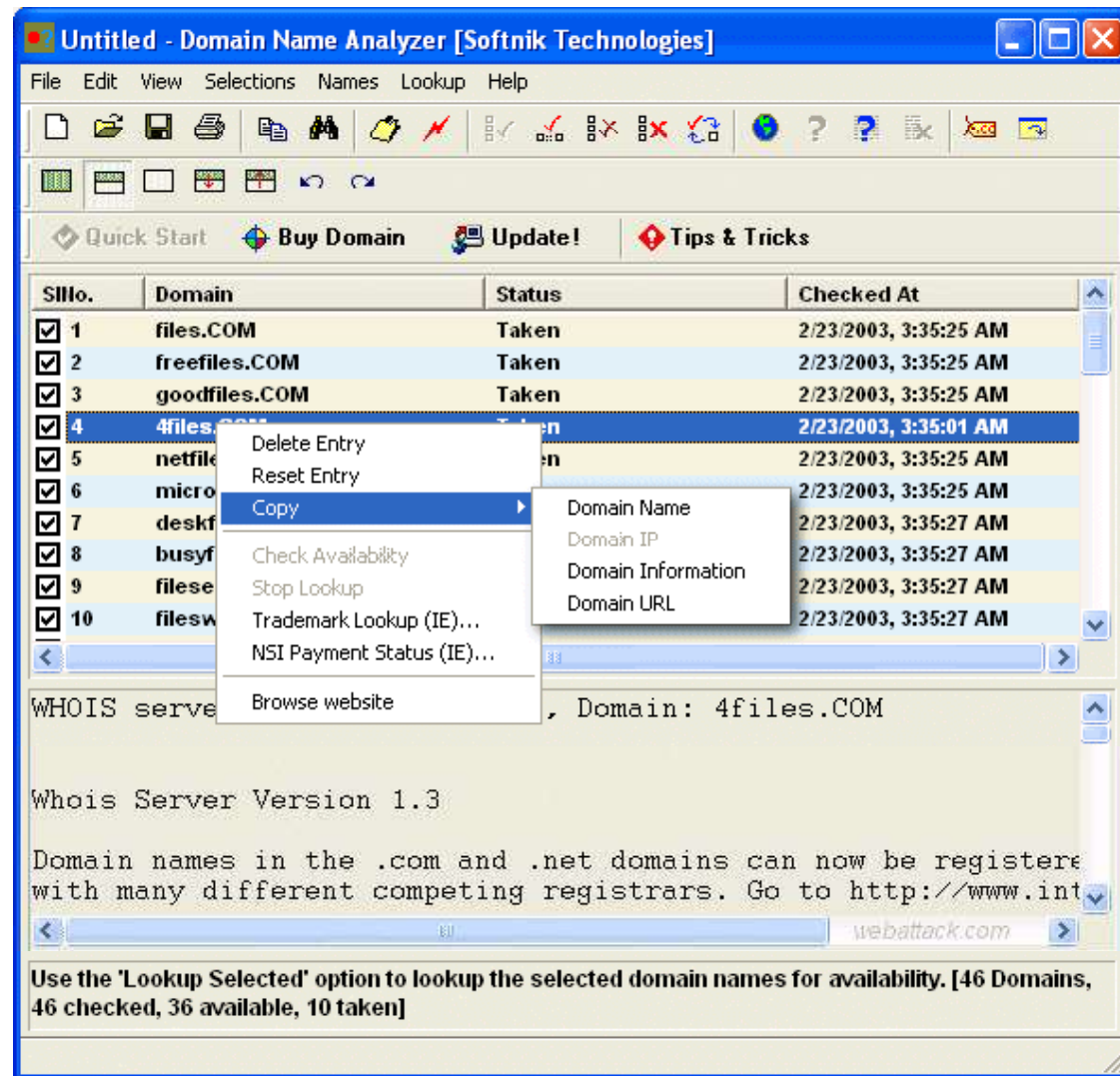
Domain Name Analyzer is a domain name lookup tool that allows to research, find, register, and manage domain names for product or business

It includes options to generate multiple domain names from keywords and then checks them all for availability through a single click

The program is easy to use with a pleasant interface and online help

It supports all global and country code top level domains as well as trademark lookup, favorite registrar configuration, and payment status lookup

Domain Name Analyzer: Screenshot

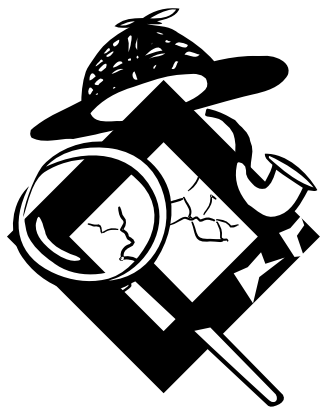


Tool: DomainInspect



DomainInspect is a domain name tool that helps to find available domain names

Manually input domain names, and check if they are registered, or have the program generate a list of domain name combinations based on keyword schemes or keywords specified



Domain list can be imported to check them (multi-threaded), and optionally save, print, or export results to HTML, Excel, Text, XML, or comma-separated

Additional features include integrated trademark lookup, registration option, and more

DomainInspect: Screenshot

The screenshot shows the DomainInspect application window. The main interface is divided into several sections:

- Generator:** Contains input fields for 'Main keyword' (files), 'Website type' (Common), and checkboxes for padding options. A list of generated domain names is shown below.
- TLD:** A list of top-level domains with checkboxes, including .com, .gov, .na, .net, .biz, .org, .coop, .edu, and .info.
- Table:** A table listing domains with columns for Domain Name, Status, Availability, Expiry Date, and Registrar.
- Info Panel:** A detailed view for the selected domain 'webattack.com', showing the response from the WHOIS server.

Domain Name	Status	Availability	Expiry Date	Registrar
webattack.com	Checked	Taken	11-17-2005	REGISTER.COM, INC.
snfiles.com	Checked	Taken	05-07-2004	GO DADDY SOFTWARE
test123.com	Checked	Taken	12-19-2004	BULKREGISTER, LLC.
peppermintshrimp.com	Checked	Taken	04-24-2004	GO DADDY SOFTWARE
spychecker.com	Checked	Taken	10-04-2004	REGISTER.COM, INC.
myfeet smellbad.com	Checked	Available		
files.com	Checked	Taken	02-24-2006	BLUEBERRY HILL COM

Info Panel Content:

Domain name: webattack.com

Response from Whois server whois.register.com

The data in Register.com's WHOIS database is provided to you by Register.com for information purposes only, that is, to assist you in obtaining information about or related to a domain name registration record. Register.com makes this information available "as is," and does not guarantee its accuracy. By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to: (1) allow, enable,

For Help, press F1 | 7 domains (7 checked, 1 available, 6 taken)

Tool: MSR Strider URL Tracer



MSR Strider URL Tracer enables to scan a domain name to see the third party domains that it serves content from and/or whether the site is being redirected

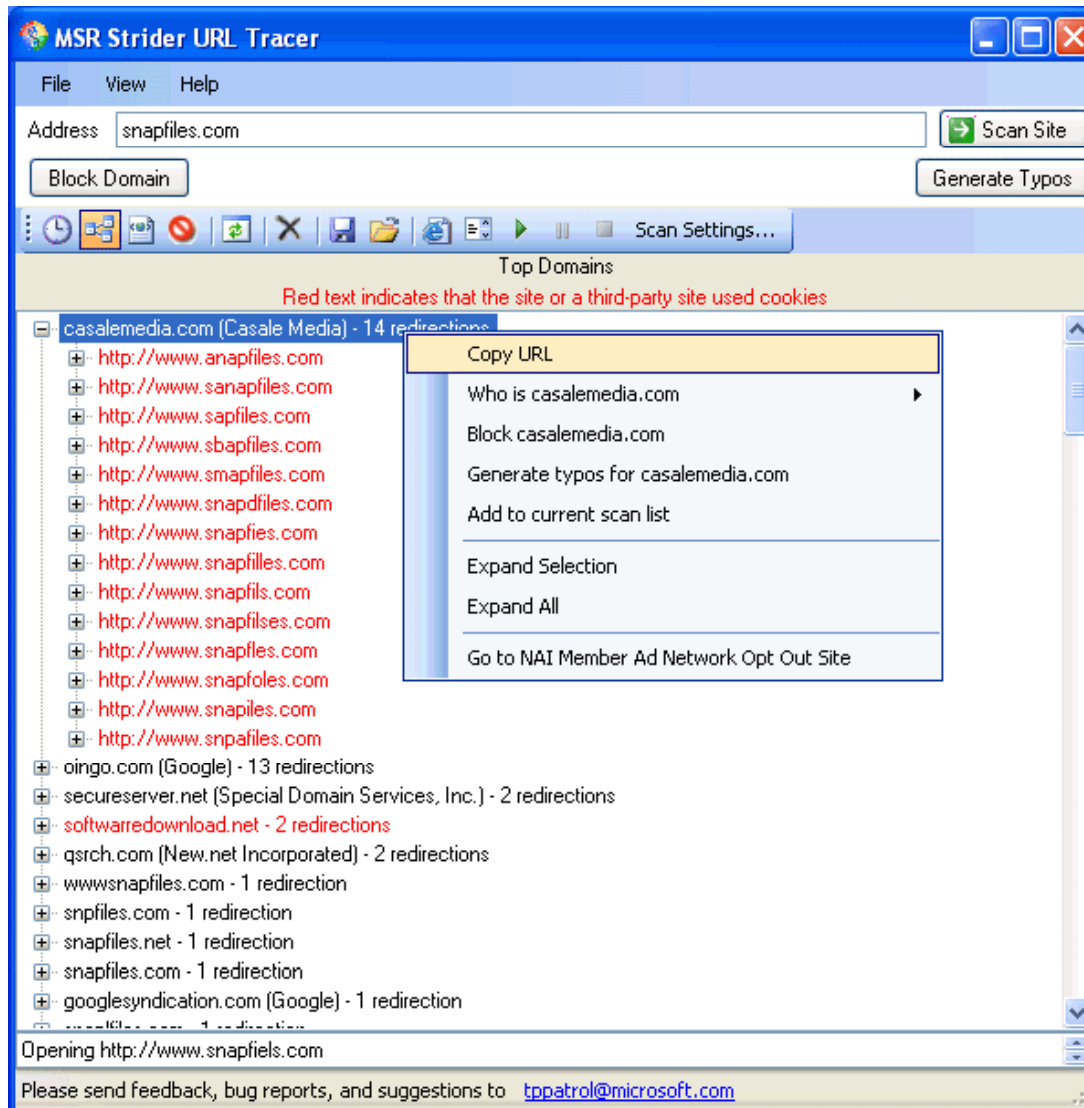
It also includes a feature that allows to generate a list of common typos based on the domain name

It scans and browses the list of generated names in order to spot domains that capitalize on inadvertent URL misspellings (typo-squatting)

It offers a detailed WHOIS lookup as well as an option to block sites, so they can no longer be accessed with Internet Explorer

Strider URL Tracer can also be very useful for webmasters or site owners who want to track down typo-squatting violations

MSR Strider URL Tracer: Screenshot



Tool: Mozzle Domain Name Pro

Mozzle is an advanced domain name search tool that features flexible and customizable domain name creation patterns

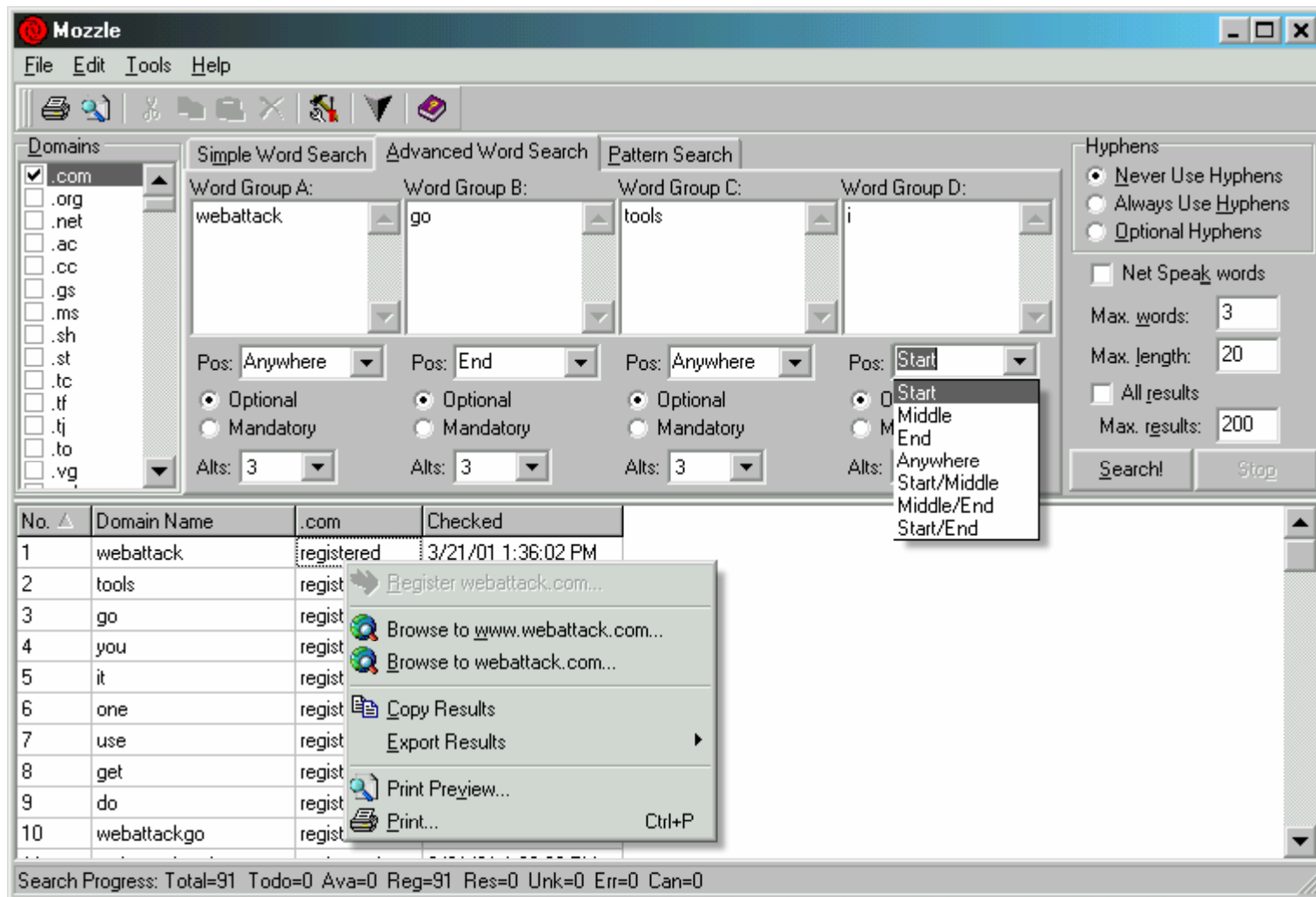
It also allows brainstorming using a built-in automatic thesaurus

Mozzle also includes Net Speak; a feature that generates alternative spellings to domain names, such as "4kids" for the domain name "forkids"

Mozzle offers 3 main search modes:

- Simple Search is the easiest to use
- Advanced Search allows to specify independent groups of alternative words with individual settings for the position of the words in domain name
- Pattern Search includes 5 wildcard characters and allows optional and alternate domain name parts to be specified

Mozzle Domain Name Pro: Screenshot



Domain Research Tool (DRT)

Domain Research Tool is an application that can be used on the initial enumeration of a target network

Functions of DRT:

- Finds domains
- Gathers search engine traffic information
- Enumerates backlinks
- Establishes page ranking statistics with a number of search engines

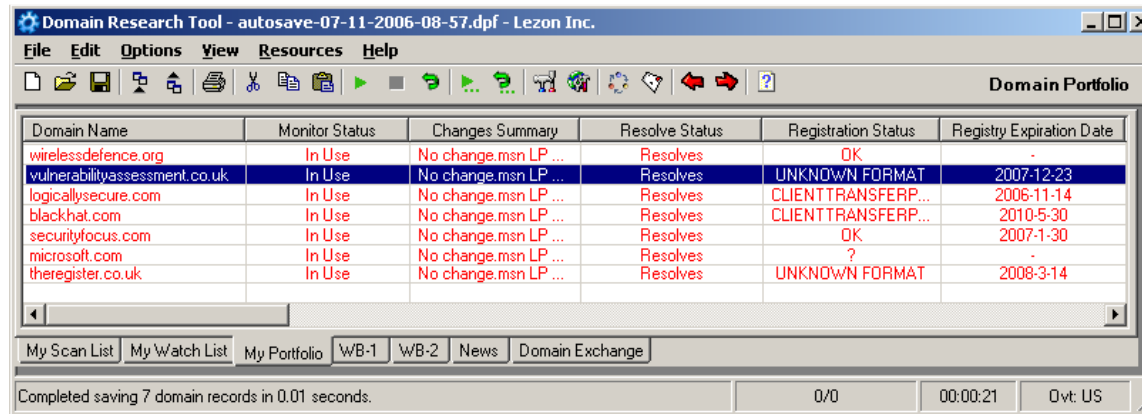
Features:

- BULK Scanning support
- Powerful Proxy Support
- IDN Support
- Typo Generator
- Portfolio Management support
- Watch List
- Type-in Domain Finder



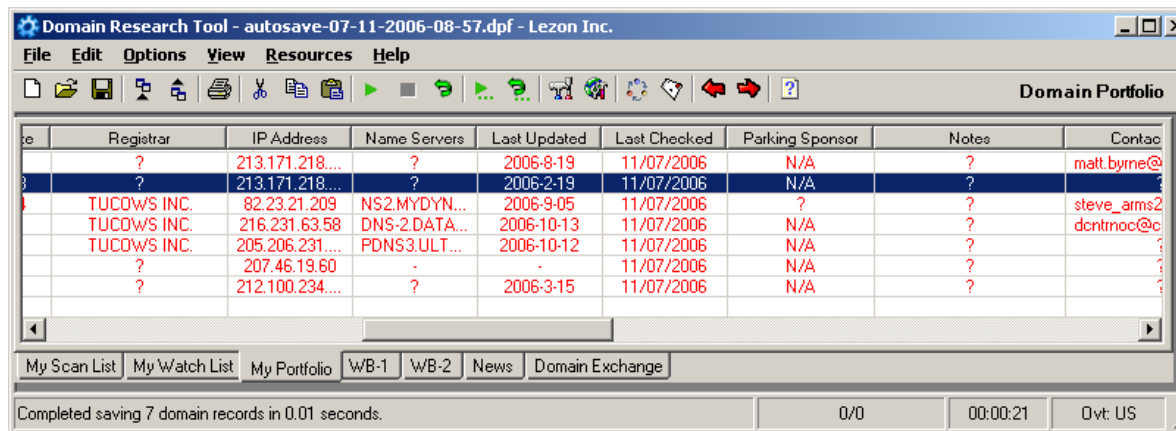
Domain Research Tool (DRT): Screenshots

DRT provides the expiry details for the target domain and that it indeed does resolve



Domain Name	Monitor Status	Changes Summary	Resolve Status	Registration Status	Registry Expiration Date
wirelessdefence.org	In Use	No change.msn LP ...	Resolves	OK	-
vulnerabilityassessment.co.uk	In Use	No change.msn LP ...	Resolves	UNKNOWN FORMAT	2007-12-23
logicallysecure.com	In Use	No change.msn LP ...	Resolves	CLIENT TRANSFERP...	2006-11-14
blackhat.com	In Use	No change.msn LP ...	Resolves	CLIENT TRANSFERP...	2010-5-30
securityfocus.com	In Use	No change.msn LP ...	Resolves	OK	2007-1-30
microsoft.com	In Use	No change.msn LP ...	Resolves	?	-
theregister.co.uk	In Use	No change.msn LP ...	Resolves	UNKNOWN FORMAT	2008-3-14

DRT provides the Domain registration information, Name Server, and Contact Email Address



Registrar	IP Address	Name Servers	Last Updated	Last Checked	Parking Sponsor	Notes	Contact
?	213.171.218...	?	2006-8-19	11/07/2006	N/A	?	matt.byrne@
?	213.171.218...	?	2006-2-19	11/07/2006	N/A	?	
TUCOWS INC.	82.23.21.209	NS2.MYDYN...	2006-9-05	11/07/2006	?	?	steve_arms2
TUCOWS INC.	216.231.63.58	DNS-2.DATA...	2006-10-13	11/07/2006	N/A	?	dcntnoc@c
TUCOWS INC.	205.206.231....	PDNS3.ULT...	2006-10-12	11/07/2006	N/A	?	
?	207.46.19.60	-	-	11/07/2006	N/A	?	
?	212.100.234....	?	2006-3-15	11/07/2006	N/A	?	

Tool: Domain Status Reporter

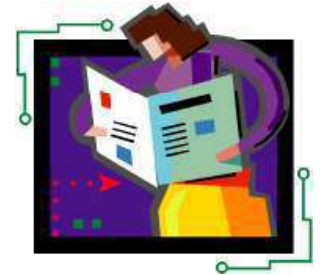
Domain Name Status Reporter is a simple tool that allows you to monitor the status of the selected top level domains

You can add interested Domain names into a list, and then check all of them (or individual ones) for availability

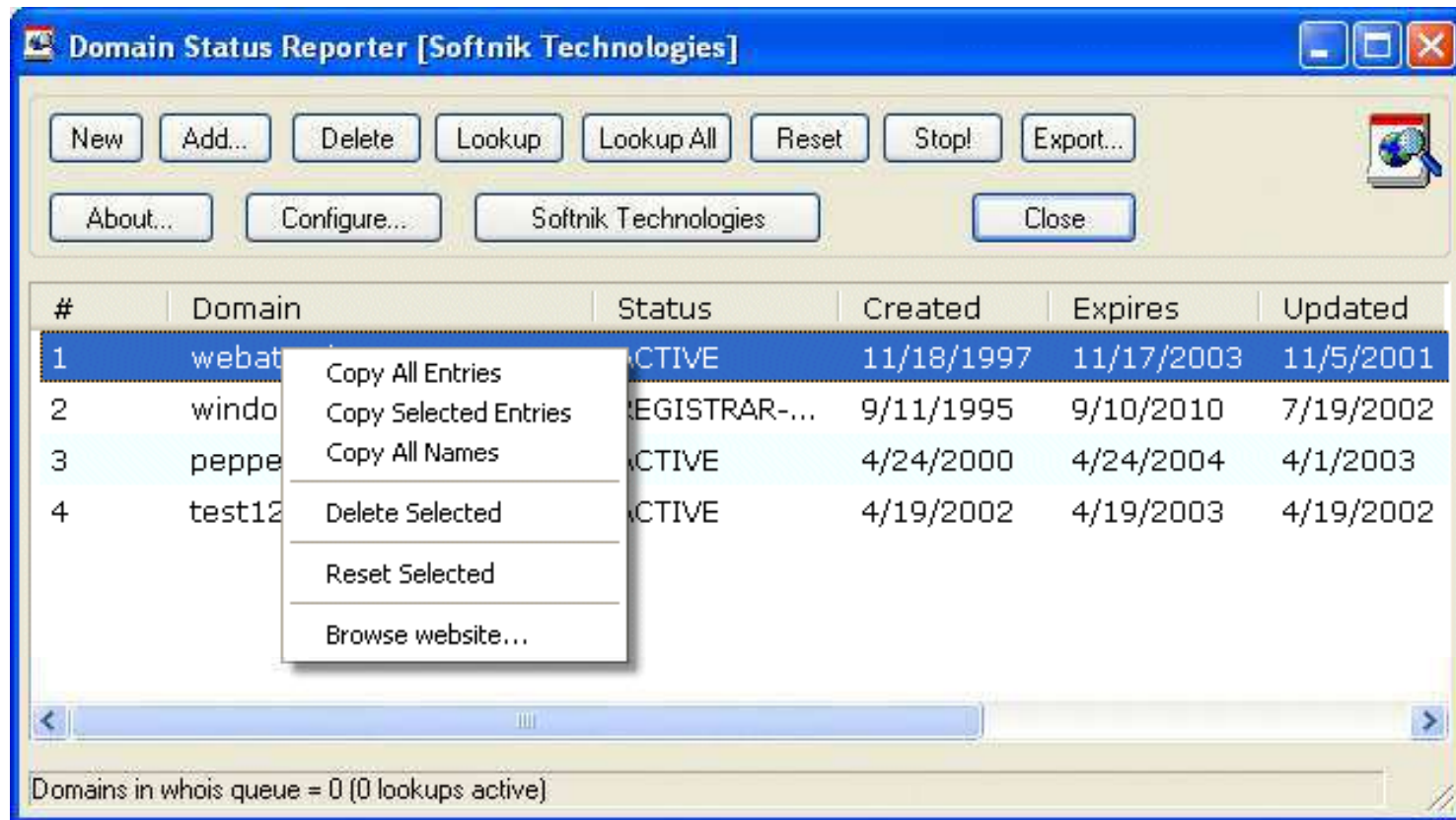
Supported domains include .com, .net, .org, .edu, .info, and .biz

In addition to status, program displays expiration date and last updated date and created date

Settings allow to customize Whois server to be used, as well as domain extensions and keywords in Whois response that indicate that the domain name may be available



Domain Status Reporter: Screenshot



Tool: Reggie

Reggie is an easy to use and flexible domain name checker with a built in 80,000 word English dictionary

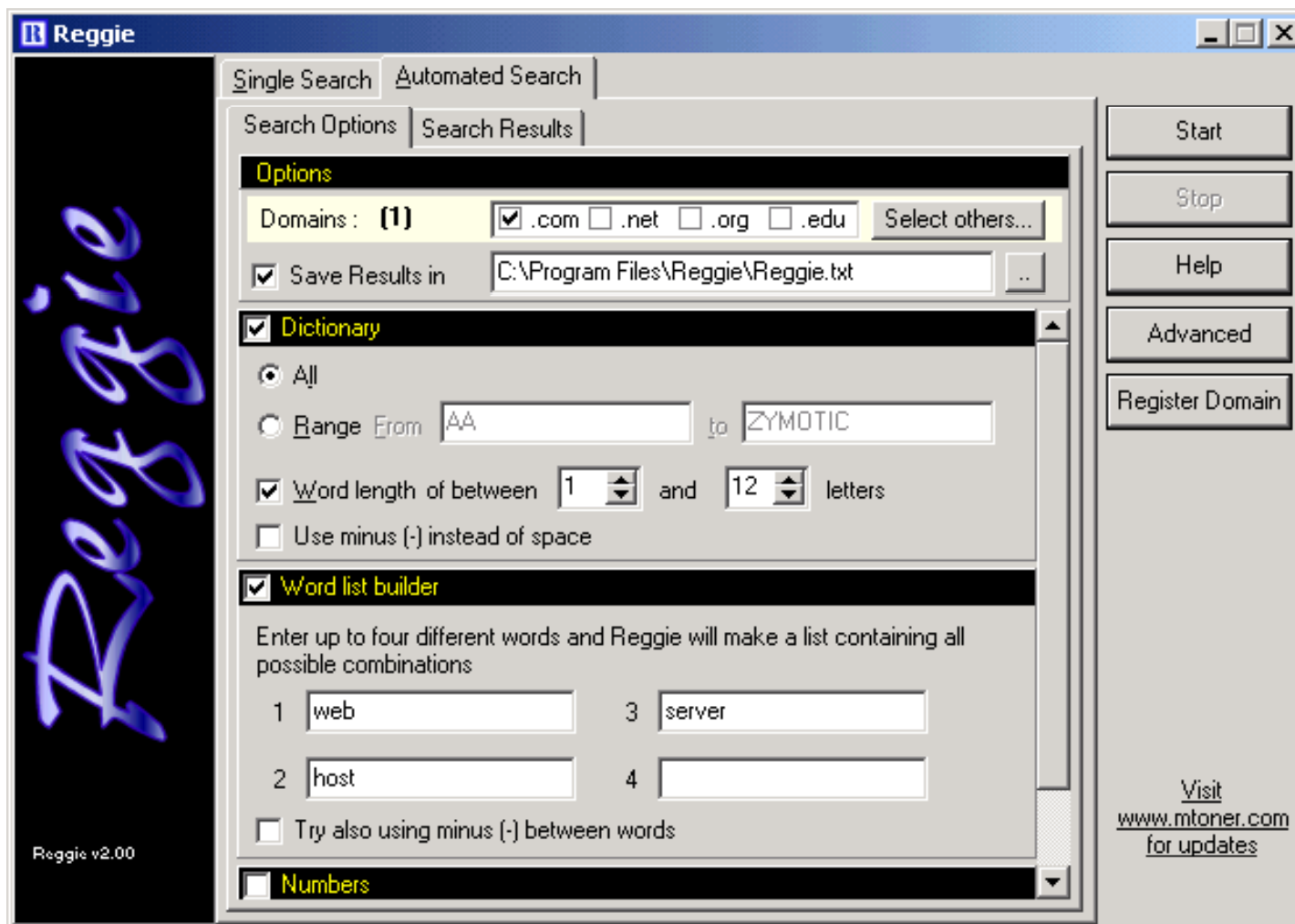
It uses both HTTP and Whois searches and works through firewalls and HTTP authorization

Reggie offers 5 automated search options including a Word List Builder which can build a list using a combination of 4 different words

It also supports "Sounds Like" using Soundex and Metaphone functions to find available domain names

Advanced users can also specify which servers to use for each domain extensions

Reggie: Screenshot



Locating Network Range

Locate the Network Range

Commonly includes:

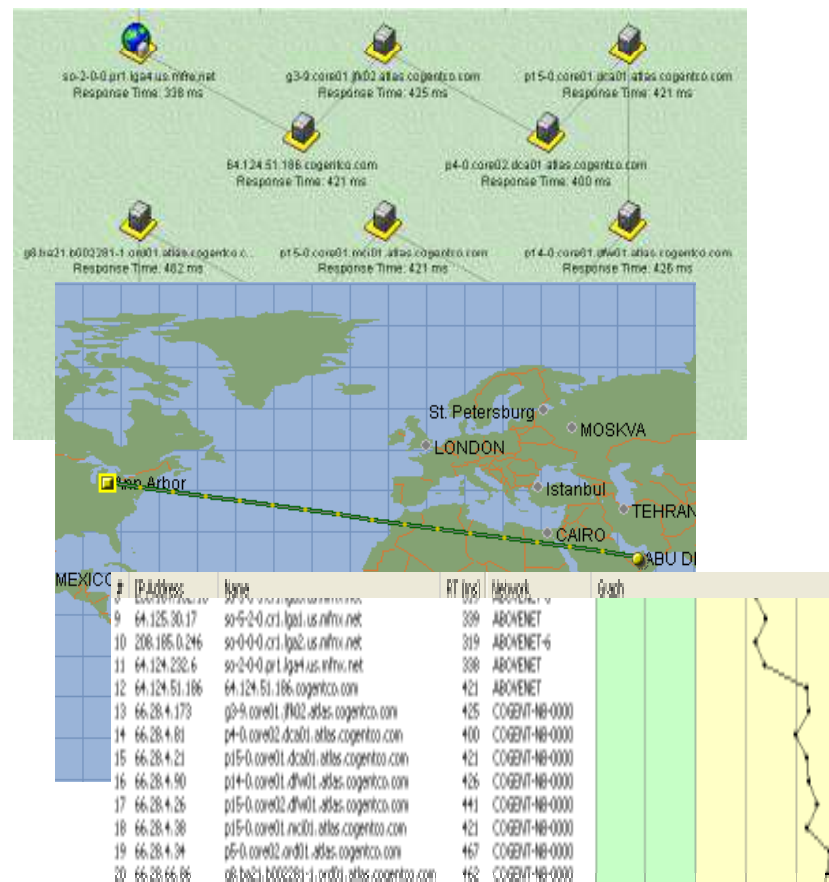
- Finding the range of IP addresses
- Discerning the subnet mask

Information Sources:

- ARIN (American Registry of Internet Numbers)
- Traceroute

Hacking Tool:

- NeoTrace
- Visual Route



ARIN allows searches on the whois database to locate information on a network's autonomous system numbers (ASNs), network-related handles, and other related point of contact (POC)

ARIN whois allows querying the IP address to find information on the strategy used for subnet addressing



Applying the principles of stewardship, ARIN, a nonprofit corporation, allocates Internet Protocol resources; develops consensus-based policies; and facilitates the advancement of the Internet through information and educational outreach.

Announcements

RSS 2.0

Wed, 16 Jan 2008
Call for Community Consultation - Software Repository

Tue, 15 Jan 2008
Join us in Los Angeles for ARIN XXI

Fri, 11 Jan 2008
ARIN Database Upgrade

Thu, 10 Jan 2008
ARIN AC Elects Chair for 2008

Wed, 09 Jan 2008
ARIN Elects Officers for 2008

Wed, 09 Jan 2008
Hotel Information for ARIN XXI in Denver, Colorado

American Registry for Internet Numbers

Registration Services

- Request and manage number resources; Guidelines; Templates; Routing Registry

- ★ [Templates](#)
- ★ [Guidelines](#)
- ★ [ARIN Service Region](#)

Policies

- Policy proposals, manual, and archives

- ★ [Internet Resource Policy Evaluation Process](#)
- ★ [Number Resource Policy Manual](#)

International Community

- Information about other RIRs, Internet community organizations; Number Resource Organization (NRO)

Meetings

- Meeting and sponsorship information; ARIN, Board, and Advisory Council meeting minutes

- ★ [ARIN XXI Meeting](#)

Billing

- Service fee information and online payment forms

- ★ [Fee Schedule](#)
- ★ [Make Payment / Update Billing POC](#)

Membership

- Membership information and benefits, listing of current members

[Need WHOIS help?](#)

- ★ [IPv6 Information Center](#)
- ★ [Legacy RSA Information](#)
- ★ [Network Abuse](#)
- ★ [Contact Us](#)
- ★ [Suggestions](#)
- ★ [Mailing Lists](#)
- ★ [Site Map](#)

ARIN Whois Output: Screenshot

Output from ARIN Whois

[ARIN Home Page](#) [ARIN Site Map](#) [ARIN Whois Help](#) [NEW! Database & Template Conversion Information Center](#)

Search for:

Search results for: 207.46.230.218

```
Microsoft (NETBLK-MICROSOFT-GLOBAL-NET)
One Redmond Way
Redmond, WA 98052
US
Netname: MICROSOFT-GLOBAL-NET
Netblock: 207.46.0.0 - 207.46.255.255
Coordinator:
  Microsoft (ZM39-ARIN) noc@microsoft.com
  425-936-4200
Domain System inverse mapping provided by:
DNS1.CP.MSFT.NET      207.46.138.20
DNS2.CP.MSFT.NET      207.46.138.21
DNS1.TK.MSFT.NET      207.46.232.37
```

IP A
dom

ARIN allows searches on the whois database to locate information on a network's autonomous system numbers (ASNs), network-related handles, and other related point of contact (POC).

Traceroute works by exploiting a feature of the Internet Protocol called TTL or Time To Live

Traceroute reveals the path IP packets travel between two systems by sending out consecutive sets of UDP or ICMP packets with ever-increasing TTLs

As each router processes an IP packet, it decrements the TTL. When the TTL reaches zero, that router sends back a "TTL exceeded" message (using ICMP) to the originator

Routers with reverse DNS entries may reveal the name of routers, network affiliation, and geographic location

Traceroute: Screenshot

```
Command Prompt
C:\>tracert mediacollege.com

Tracing route to mediacollege.com [66.246.3.197]
over a maximum of 30 hops:

  0  <10 ms    <10 ms    <10 ms    192.168.1.1
  1  240 ms    421 ms    70 ms     219-88-164-1.jetstream.xtra.co.nz [219.88.164.1]
  2  20 ms     30 ms     30 ms     210.55.205.123
  3  *         *         *         Request timed out.
  4  30 ms     30 ms     40 ms     202.50.245.197
  5  30 ms     40 ms     40 ms     g2-0-3.tkbr3.global-gateway.net.nz [202.37.245.140]
  6  30 ms     30 ms     40 ms     so-1-2-1-0.akbr3.global-gateway.net.nz [202.50.116.161]
  7  160 ms    161 ms    160 ms    pl-3.sjbr1.global-gateway.net.nz [202.50.116.178]
  8  160 ms    171 ms    160 ms    so-1-3-0-0.pabr3.global-gateway.net.nz [202.37.245.230]
  9  160 ms    161 ms    170 ms    paol-br1-g2-1-101.gnaps.net [198.32.176.165]
 10  180 ms    181 ms    180 ms    lax1-br1-p2-1.gnaps.net [199.232.44.5]
 11  170 ms    170 ms    171 ms    lax1-br1-ge-0-1-0.gnaps.net [199.232.44.50]
 12  240 ms    241 ms    240 ms    nyc-n20-ge2-2-0.gnaps.net [199.232.44.21]
 13  240 ms    251 ms    250 ms    ash-n20-ge1-0-0.gnaps.net [199.232.131.36]
 14  241 ms    240 ms    250 ms    0503.ge-0-0-0.gbr1.ash.nac.net [207.99.39.157]
 15  251 ms    260 ms    250 ms    0.so-2-2-0.gbr2.nvr.nac.net [209.123.11.29]
 16  250 ms    260 ms    261 ms    0.so-0-3-0.gbr1.oct.nac.net [209.123.11.233]
 17  250 ms    260 ms    261 ms    209.123.182.243
 18  250 ms    260 ms    261 ms    sol.yourhost.co.nz [66.246.3.197]

Trace complete.

C:\>
```

Trace Route Analysis

Traceroute is a program that can be used to determine the path from source to destination

By using this information, an attacker determines the layout of a network and the location of each device

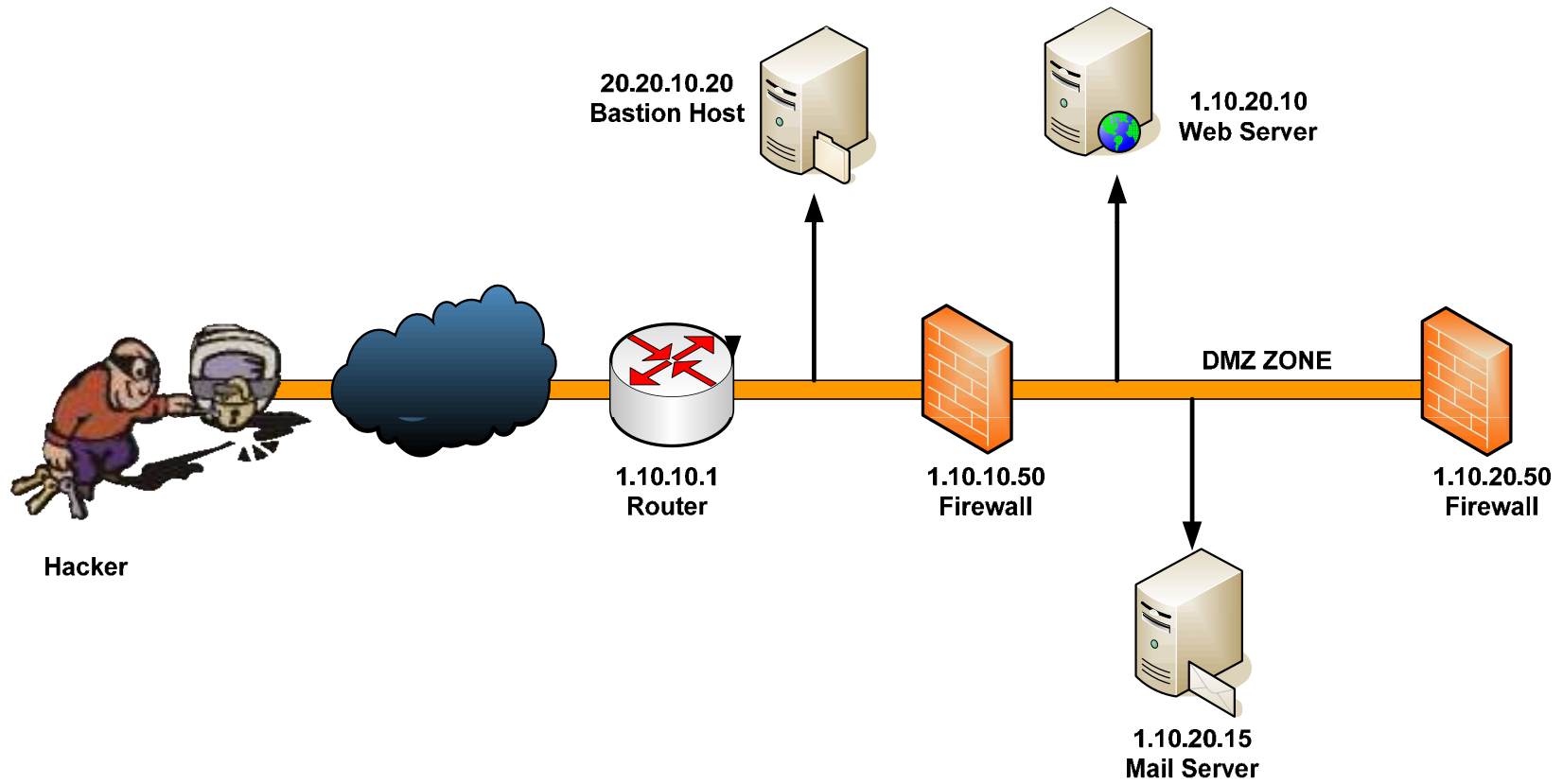
For example: after running several traceroutes, an attacker might obtain the following information:

- traceroute 1.10.10.20, second to last hop is 1.10.10.1
- traceroute 1.10.20.10, third to last hop is 1.10.101
- traceroute 1.10.20.10, second to last hop is 1.10.0.50
- traceroute 1.10.20.15, third to last hop is 1.10.101
- traceroute 1.10.20.15, second to last hop is 1.10.10.50



By putting this information together, you can diagram the network (see the next slide)

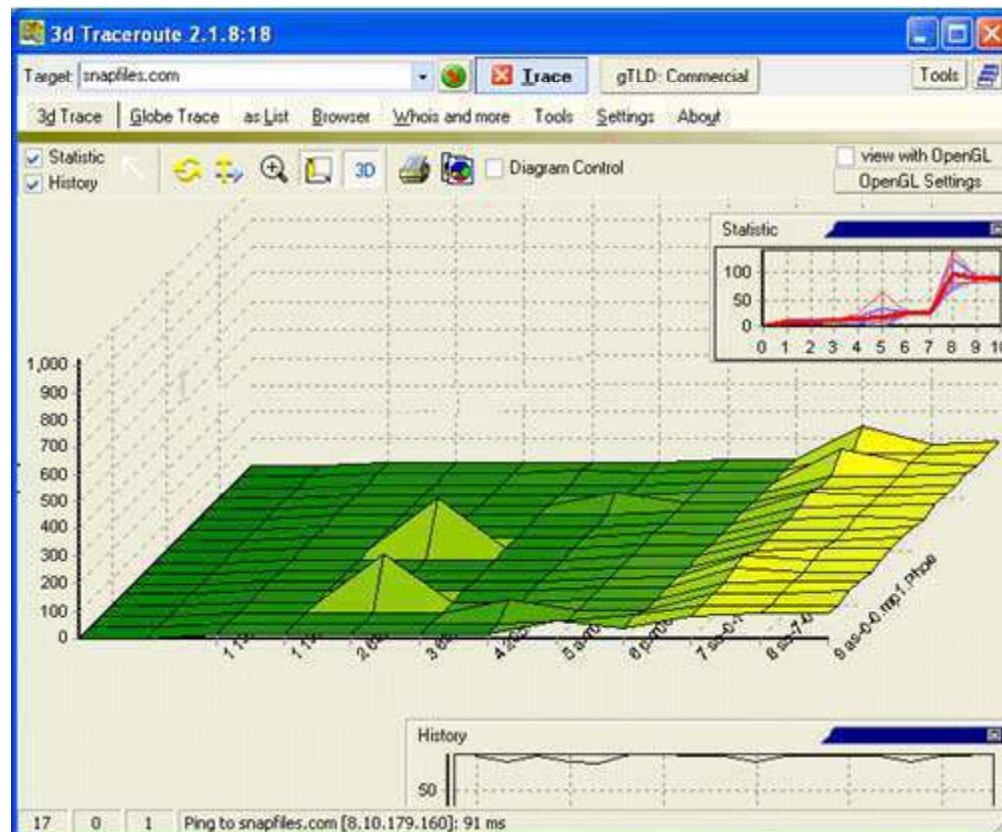
Trace Route Analysis



Tool: 3D Traceroute

3D Traceroute is a full-blown three-dimensional traceroute program that allows you to visually monitor Internet's connectivity

It offers an attractive and fast loading 3D interface as well as optional text results



3D Traceroute: Screenshot 1

3d Traceroute 2.1.8.18

Target: snapfiles.com | Trace | gTLD: Commercial

3d Trace | Globe Trace | as List | Browser | Whois and more | Tools | Settings | About

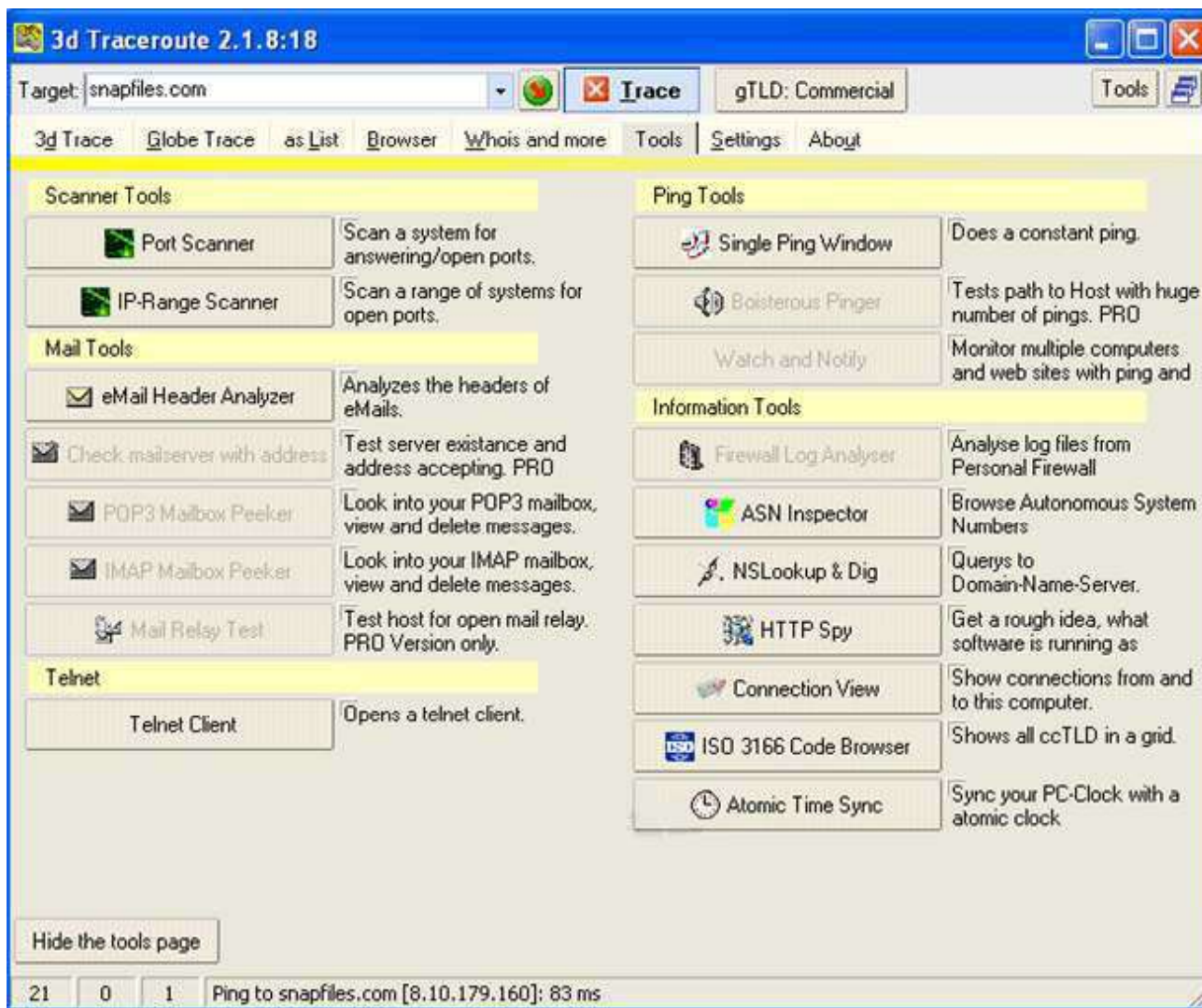
Hop	IP	Hostname	last [ms]	min [ms]	max [ms]	ava. [ms]	var. [ms]	total Loss	perc. Loss
1	192.168.1.1	192.168.1.1	0	0	0	0			
2	65.14.252.8	65.14.252.8	10	9	11	10	1	0	
3	65.14.255.229	65.14.255.229	11	9	12	10	1	0	
4	205.152.145.201	205.152.145.201	11	10	184	18	35	0	
5	65.83.237.8	axr00mia-1-3-0.bellsouth.net	11	11	24	12	3	0	
6	65.83.236.16	pxr00mia-0-0-0.bellsouth.net	10	10	65	13	11	0	
7	65.57.174.5	so-0-1-0-0.gar1.Miami1.Level3.net	25	24	34	26	2	0	
8	4.68.112.45	so-7-0-0.mp2.Miami1.Level3.net	151	24	151	31	26	0	
9	64.159.3.213	as-0-0.mp1.Phoenix1.Level3.net	81	81	144	91	20	0	
10	4.68.98.4	ge-6-1.hsa1.Phoenix1.Level3.net	82	81	90	86	4	0	
11	8.10.179.160	snapfiles.com	83	83	118	89	7	0	

above this level: not good any more 26 ms above this level: bad 125 ms

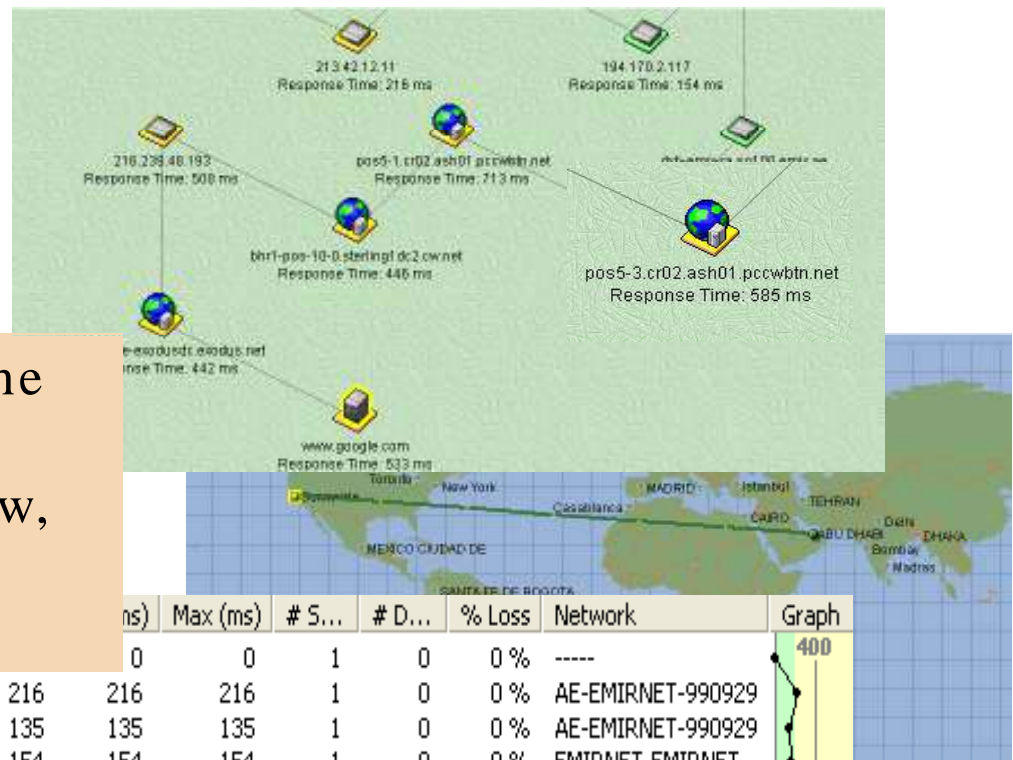
34 0 1 Ping to snapfiles.com [8.10.179.160]: 83 ms

use: Show Day And Night Trace

3D Traceroute: Screenshot 2



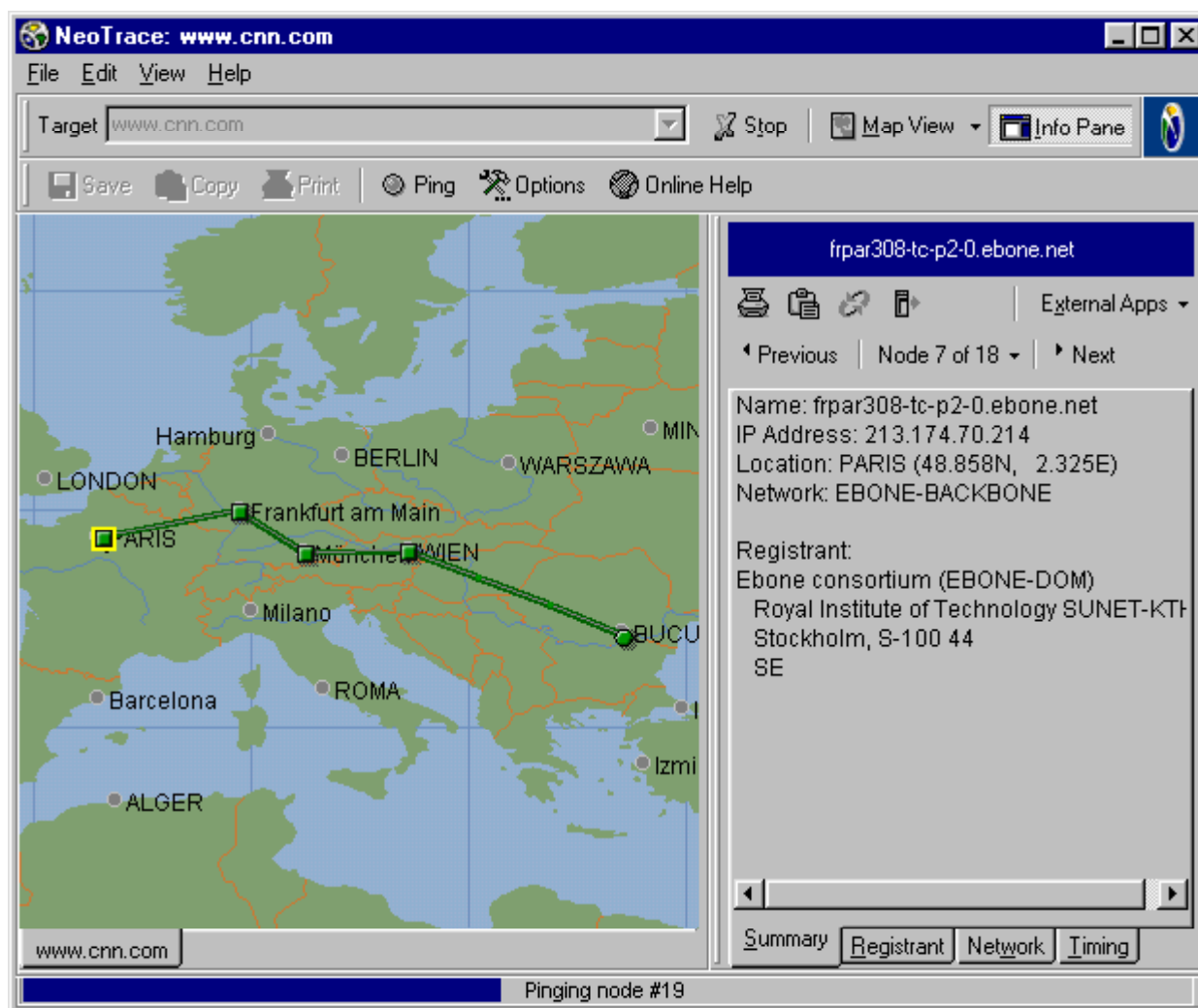
Tool: NeoTrace (Now McAfee Visual Trace)



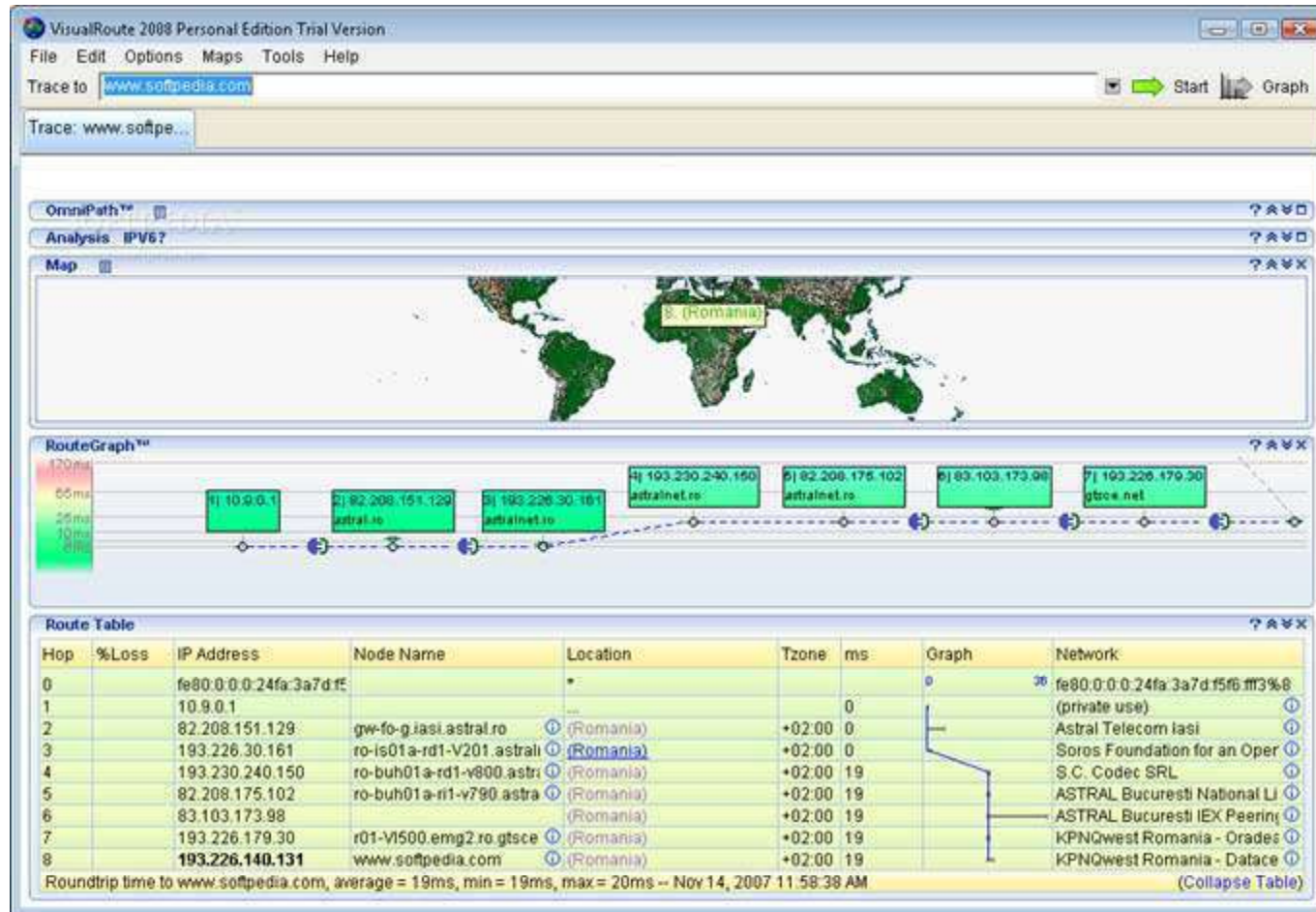
NeoTrace shows the traceroute output visually – map view, node view, and IP view

#	IP Address	Name	Min (ms)	Max (ms)	# S...	# D...	% Loss	Network	Graph
1	217.165.236.73	SAM	0	0	1	0	0 %	----	
2	213.42.12.11	----	216	216	1	0	0 %	AE-EMIRNET-990929	
3	213.42.12.130	----	135	135	1	0	0 %	AE-EMIRNET-990929	
4	194.170.2.117	----	154	154	1	0	0 %	EMIRNET-EMIRNET	
5	195.229.31.66	dx-b-emix-rb.ge130.emix.ae	159	159	1	0	0 %	AE-EMIRNET-971125	
6	195.229.0.234	dx-b-emix-ra.so100.emix.ae	139	139	1	0	0 %	EMIRNET-EMIRNET	
7	166.63.210.62	bcr2.thamesside.cw.net	442	442	1	0	0 %	CW-NETC52	
8	63.216.0.42	pos5-1.cr02.ash01.pccwbtn.net	713	713	1	0	0 %	CAIS-CIDR7	
9	206.24.238.166	bhr1-pos-10-0.sterling1dc2.cw.net	446	446	1	0	0 %	CW-05BLK	
10	216.239.48.193	----	508	508	1	0	0 %	GOOGLE	
11	216.109.88.218	218-google-exodusdc.exodus.net	442	442	1	0	0 %	DC3-8	
12	216.239.39.99	www.google.com	533	533	1	0	0 %	GOOGLE	

NeoTrace: Screenshot



Tool: VisualRoute Trace



It shows the connection path and the places where bottlenecks occur

www.visualware.com/download/

VisualRoute Trace: Screenshot

The screenshot displays the VisualRoute 2008 Personal Edition Trial Version interface. The main window shows a trace to 'www.softpedia.com'. The 'RouteGraph' section visualizes the path through several hops, with a color-coded delay scale on the left. The 'Route Table' section provides a detailed list of hops, including IP addresses, node names, locations, and network identifiers.

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		fe80:0:0:0:24fa:3a7d:f5f6:ff3%8		*			0	fe80:0:0:0:24fa:3a7d:f5f6:ff3%8 (private use)
1		10.9.0.1		...		0		
2		82.208.151.129	gw-fo-g.iasi.astral.ro	(Romania)	+02:00	0		Astral Telecom Iasi
3		193.226.30.161	ro-is01a-rd1-v201.astrali	(Romania)	+02:00	0		Soros Foundation for an Oper
4		193.230.240.150	ro-buh01a-rd1-v800.astr	(Romania)	+02:00	19		S.C. Codec SRL
5		82.208.175.102	ro-buh01a-ri1-v790.astra	(Romania)	+02:00	19		ASTRAL Bucuresti National LI
6		83.103.173.98		(Romania)	+02:00	19		ASTRAL Bucuresti IEX Peering
7		193.226.179.30	r01-v1500.emg2.ro.gtsee	(Romania)	+02:00	19		KPNQwest Romania - Orades
8		193.226.140.131	www.softpedia.com	(Romania)	+02:00	19		KPNQwest Romania - Datace

Roundtrip time to www.softpedia.com, average = 19ms, min = 19ms, max = 20ms -- Nov 14, 2007 11:58:38 AM

Path Analyzer Pro

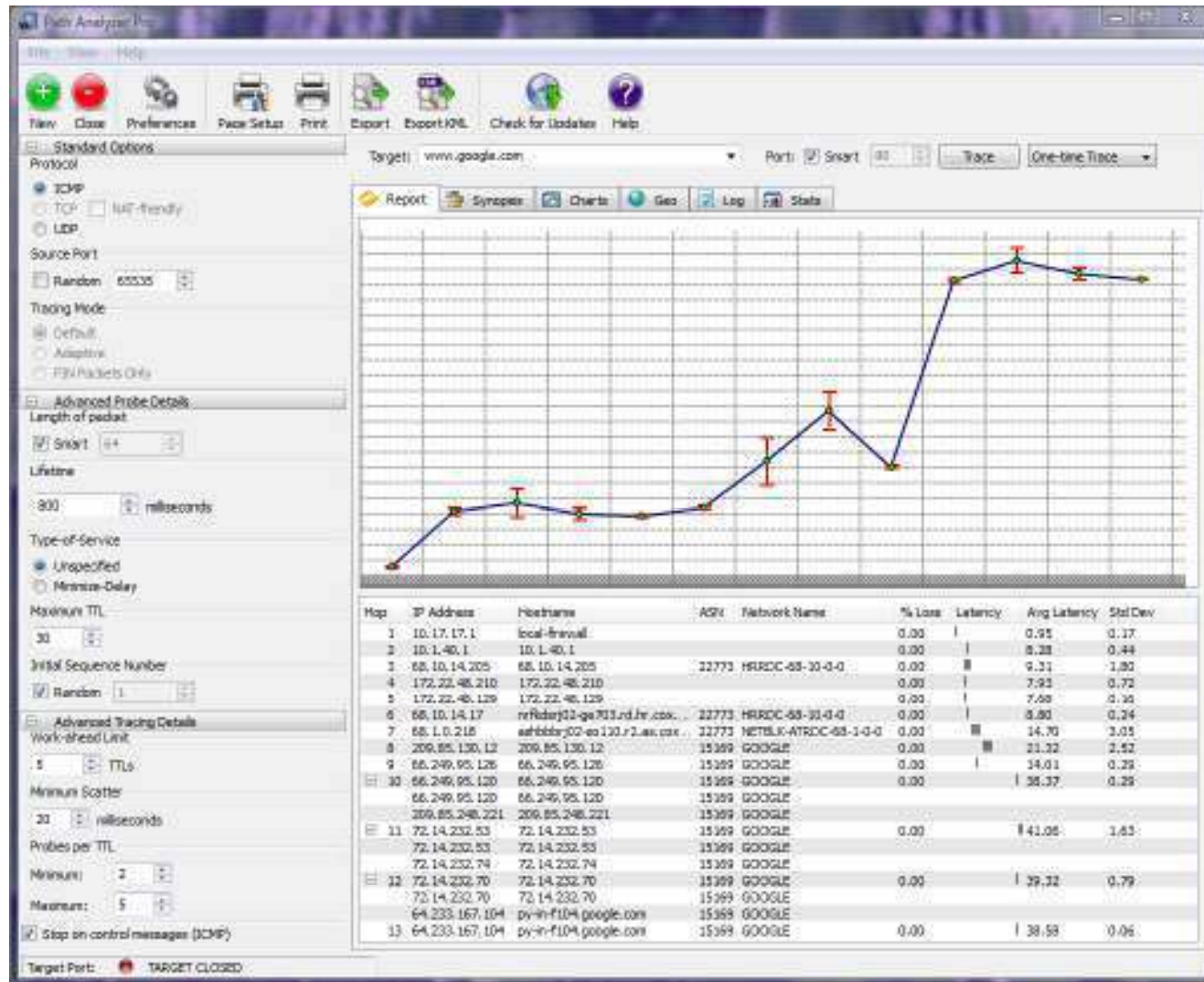
Path Analyzer Pro delivers advanced network route tracing

It traces with performance tests, DNS, whois, and network resolution to investigate network issues

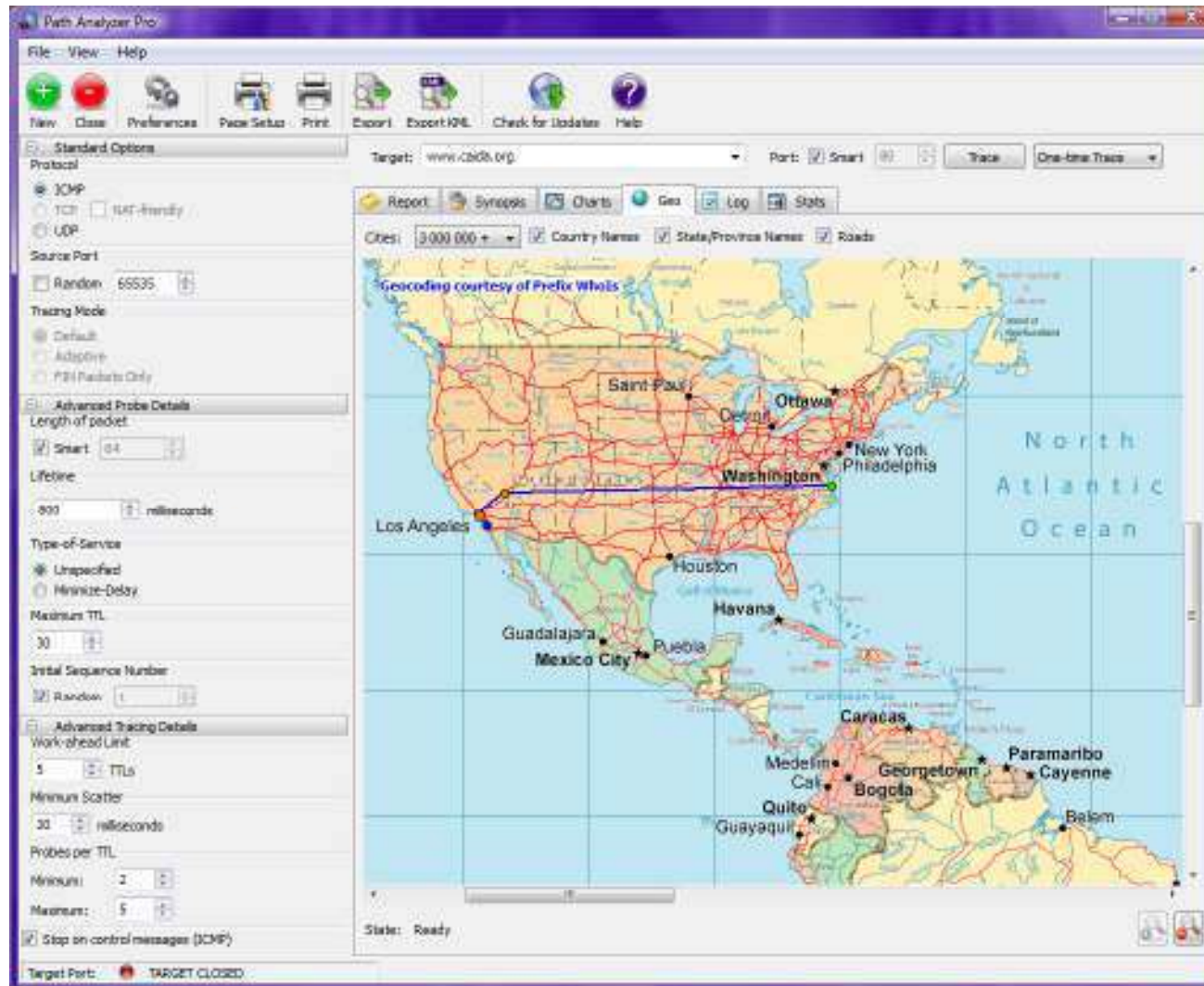
It is integrated with all these powerful features in a simple and single graphical interface



Path Analyzer Pro: Screenshot 1



Path Analyzer Pro: Screenshot 2



Tool: Maltego

Maltego can be used for the information gathering phase of penetration testing making it possible for less experienced testers to work faster and more accurately

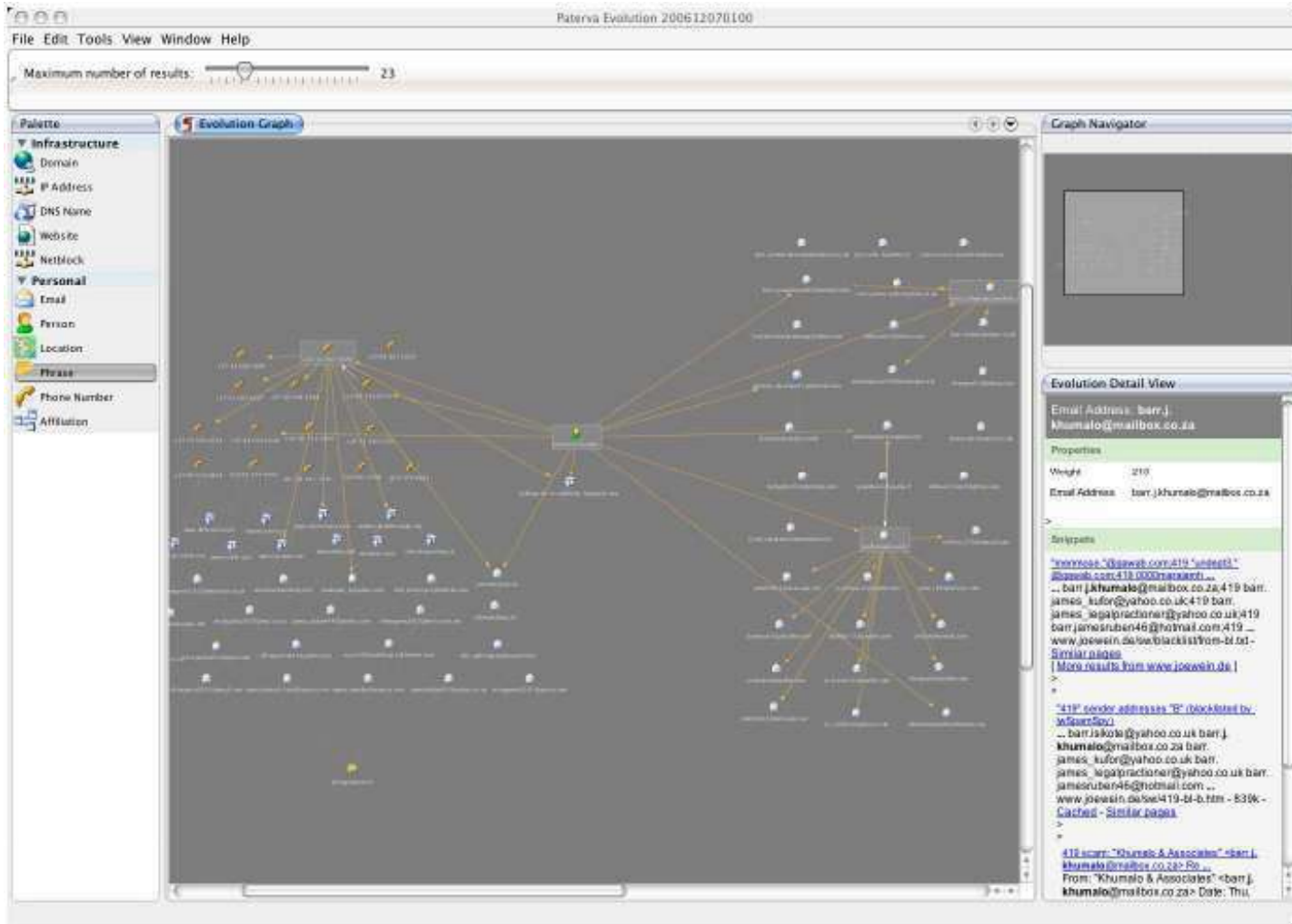
Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate - making it possible to see hidden connections

Maltego has applications in:

- Forensic investigations
- Law enforcement
- Intelligence operations
- Identity fraud investigation
- Identity verification processes



Maltego: Screenshot



Layer Four Traceroute

LFT is a sort of 'traceroute' that often works much faster and goes through many configurations of packet-filters

LFT implements other features such as AS number lookups through several reliable sources, loose source routing, netblock name lookups, and many more

It is the all-in-one traceroute tool because it can launch a variety of different probes using ICMP, UDP, and TCP protocols, or the RFC1393 trace method

Prefix WhoIs widget

Prefix WhoIs widget displays the number of prefixes present within the global Internet routing table and allows the user to submit queries using a familiar Dashboard interface

It allows the user to submit queries in the form of IP addresses

The IP addresses are submitted to the Prefix WhoIs project, an organization that tracks and models the global internet routing table

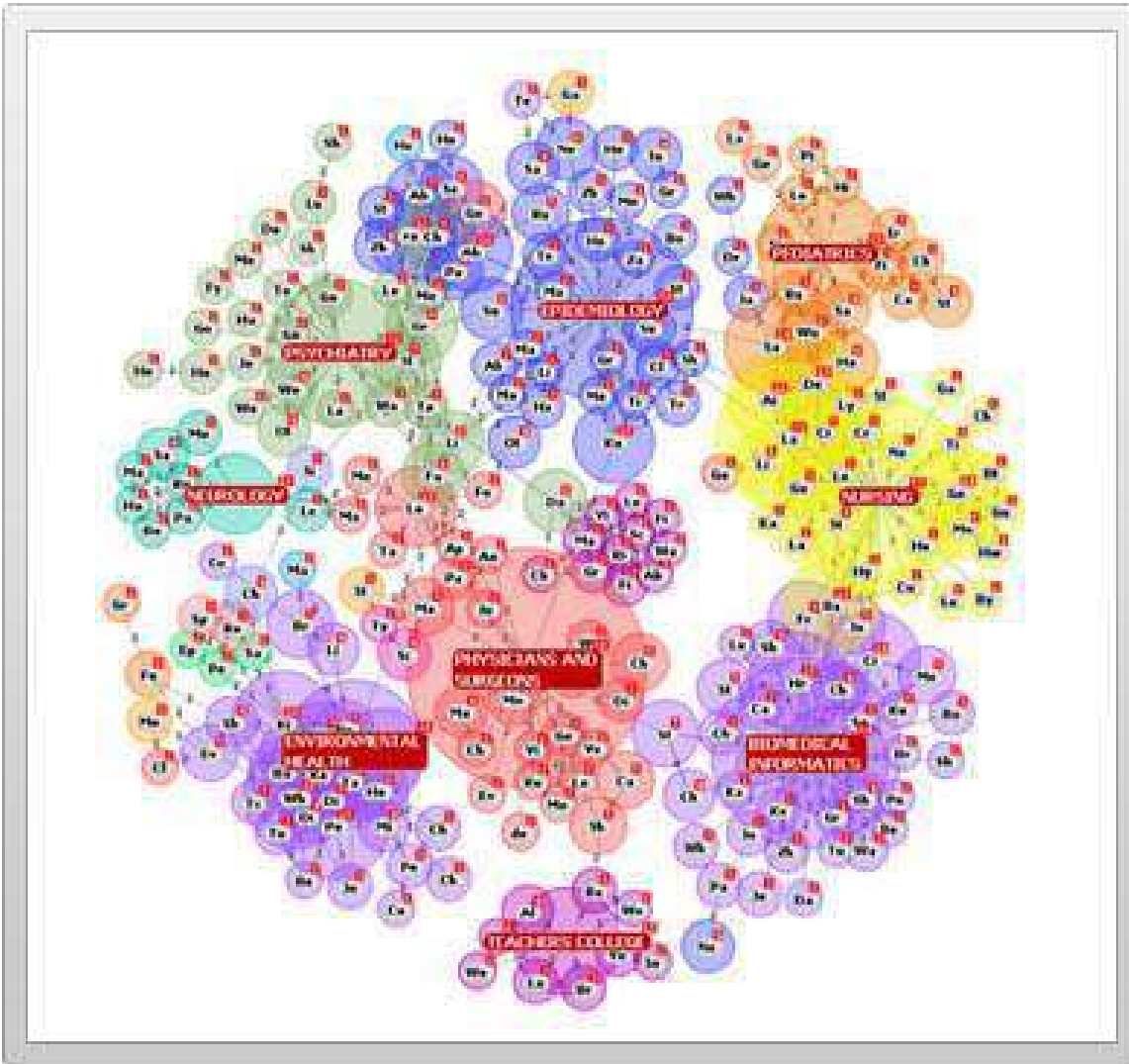
It also displays some useful information, such as the size of the overall table measured in a number of prefixes

Prefix WhoIs widget: Screenshot



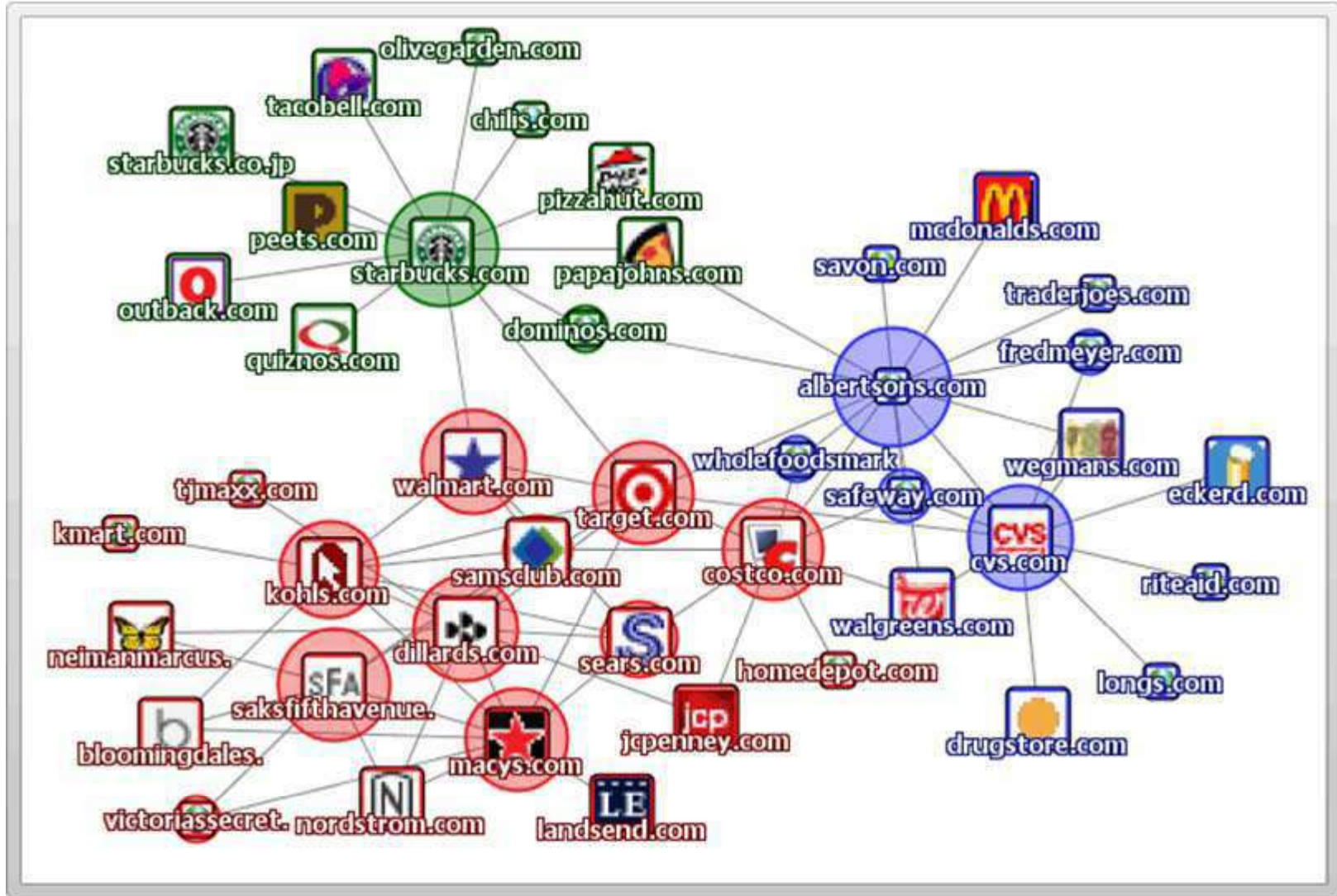
Tool: Touchgraph

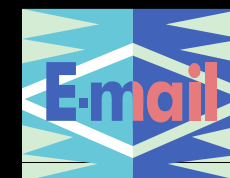
www.touchgraph.com



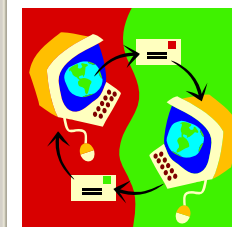
TouchGraph allows for the creation and navigation of interactive graphs. Ideal for organising links, or mind mapping

Touchgraph: Screenshot





Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		217.165.221.153	SAM	*			0	Emirates Internet
1		213.42.12.6	-	(United Arab Emirates)		2537		Emirates Telecommunicati
2		213.42.12.131	-	(United Arab Emirates)		2513		Emirates Telecommunicati
3		194.170.2.117	-	(United Arab Emirates)		2467		Emirates Internet
4		195.229.31.35	auh-emix-rb.ge6303.er	(United Arab Emirates)		2429		Emirates Telecommunicati
5		195.229.31.34	auh-emix-ra.ge6303.er	(United Arab Emirates)		2421		Emirates Telecommunicati
6		62.216.144.25	-	(United Kingdom)	*	2766		FLAG Telecom Limited
7		62.216.140.9	ge-1-0-0.0.core1.sfr1.fl	(United Kingdom)	*	2894		FLAG Telecom Limited
8		166.90.133.165	gige4-1-116.ipcolo2.Sa	San Francisco, CA, US	-08:00	2655		Level 3 Communications, Ir
9		209.244.14.201	gigabithernet4-2.core	San Francisco, CA, US	-08:00	2695		Level 3 Communications, Ir
10		209.247.10.233	so-4-0-0.mp2.SanFran	San Francisco, CA, US	-08:00	3008		Level 3 Communications, Ir
11		64.159.0.218	so-2-0-0.mp2.SanJose	San Jose, CA, USA	-08:00	3073		Level 3 Communications, Ir
12		64.159.2.165	gigabithernet5-2.core	San Jose, CA, USA	-08:00	3009		Level 3 Communications, Ir
13		209.244.3.246	GigabitEthernet5-0.edg	Palo Alto, CA, USA	-08:00	2996		Level 3 Communications, Ir
14		209.245.146.150	Singtel-Level3-oc3.ix.si	...		2962		
15		203.208.182.21	-	Singapore	+08:00	2974		
16		203.208.172.29	p6-8.sngtp-cr2.ix.singte	Singapore	+08:00	3061		
17		202.160.250.154	-	Singapore	+08:00	3029		
18		165.21.12.78	FE-4-0-0.lavender.sing	(Singapore)	+08:00	2995		
19	20	165.21.48.102	-	Singapore	+08:00	3201		
20	30	137.132.19.100	olympus.bic.nus.edu.si	(Singapore)	+08:00	3473		
21	30	137.132.19.100	olympus.bic.nus.edu.si	(Singapore)	+08:00	3276		
22		137.132.19.100	olympus.bic.nus.edu.si	(Singapore)	+08:00	3179		
23		137.132.19.100	olympus.bic.nus.edu.si	(Singapore)	+08:00	3159		National University of Singa



It shows the number of hops made and the respective IP addresses, the node name, location, time zone, and network



Trace completed, [click here](#) for advanced route analysis

You are on day 1 of your 15-day trial of eMailTrackerPro. [Click here to apply a licence](#) or for purchase information [click here](#)

Map

Route to Sender

Analysis:

Email Address: webmaster@softpedia.com

Network Contact Information: The following details refer to the network responsible for the computer that originated the email

- noc@gtstelecom.ro
- +40 21 410 3883
- GTS Telecom Romania
Bucharest Financial Piazza
Calea Victoriei 15, intrarea A, etajul 2
704111 Bucuresti
Romania

Domain Contact Information: The following details refer to the registered contact details for the domain

- Whois Privacy Protection Service, Inc.
- Whois Agent (fcdwptssst@wholsprivacyprotect.com)
+1.4252740657
Fax: +1 4256960234

eMailTrackerPro is the email analysis tool that enables analysis of an email and its headers automatically, and provides graphical results



Re@adNotify



Welcome to ReadNotify.com !

ReadNotify lets you know when email you've sent gets read



[Start here!](#)



[Optional Plugin](#)



[PDF Tracking](#)

Member Sign-in

email:

password:

[Sign-in](#)

[Sign up now - Free!](#)

Your existing email address:

[GO!](#)

Mail Tracking is a tracking service that allows you to track when your mail was read, for how long and how many times, and the place from where the mail has been posted. It also records forwards and passing of sensitive information (MS Office format)

E-mail Spiders

E-Mail Spiders

Have you ever wondered how Spammers generate a huge mailing database?

They pick tons of e-mail addresses by searching in the Internet

All they need is a web spidering tool picking up e-mail addresses and storing them to a database

If these tools run the entire night, they can capture hundreds of thousands of e-mail addresses

Tools:

- Web data Extractor
- E-mail Address Spider



Tool: 1st E-mail Address Spider

1st Email Address Spider 2005

File Search Help

Start Pause Stop Reset Search Save Results... Settings Homepage Buy now

Search by keywords | Start from a specific URL

Please input keyword(s):

Email Address	Title	URL
[1]info@iibaba.org	insurance agents mail - Google Search	http://www.google.com/search?q=insurance+agents+mail
[2]info@kaia.com	insurance agents mail - Google Search	http://www.google.com/search?q=insurance+agents+mail
[3]iibnj@iibnj.org	insurance agents mail - Google Search	http://www.google.com/search?q=insurance+agents+mail
[4]info@insurancenewsnet.c...	MSN Search: insurance agents mail	http://search.msn.com/results.asp?RS=CHECKED&FORM=MSNH&v=1&q=insurance+a...
[5]gsavelli@aol.com	Insurance Agents Web site consultati...	http://www.insurance-web-sales.com/
[6]gsavelli@insurance-web-s...	Insurance Agents Web site consultati...	http://www.insurance-web-sales.com/
[7]info@4insuranceagents.c...	Insurance Agent Resources, Insuranc...	http://www.4insuranceagents.com/
[8]winona@piaga.com	PIA of Georgia - The Professional Ins...	http://www.piaga.com/
[9]dorothy@kaia.com	Independent Insurance Agents & Bro...	http://www.iaa.org/ks/default?contentpreference=ks&activetab=state&activestate=ks
[10]denn@state.de.us	Home Page for Matthew Denn, Dela...	http://www.state.de.us/inscom/

Thread#	Status	URL	De.
2400	[2/60]Reading page content....	http://www.google.com/search?q=insurance+agents+mail&hl=en&lr=&ie=utf-8&start=40&sa=n	1
3876	[3/60]Reading page content....	http://www.ins.state.ny.us/licinfo.htm	2
684	[0/60]Reading page content....	http://cc.msnsccache.com/cache.aspx?q=3236045204164&lang=en-sg&mkt=en-sg&a...	2
3440	[0/60]Reading page content....	http://enews.insurancemail.biz/advertising.asp	2
3444	[6/60]Reading page content....	http://www.alarmchannel.com/	2
1752	[1/60]Reading page content....	http://www.professionalinsuranceagents.co.uk/	2
1716	[0/60]Reading page content....	http://cc.msnsccache.com/cache.aspx?q=3226870941820&lang=en-sg&mkt=en-sg&a...	2

Start search.... | Emails Extracted:28 | Time Elapsed:00:09 | URLs Processed:80 | URLs Queued:209

Power E-mail Collector Tool

Power E-mail Collector is a powerful email address harvesting program

It can collect up to 750,000 unique valid email addresses per hour with a Cable/DSL connection

It only collects valid email addresses

You do not have to worry about ending up with undeliverable addresses

How does it work?

- Just enter a domain that you want to collect email addresses from and press the start button. The program opens up many simultaneous connections to the domain and begins collecting addresses



Power E-mail Collector Tool: Screenshot

Power Email Collector 3.2

File Tools Settings Help

Exit Save Start Stop Reset Settings Help Home

Enter Domain Name: Edit Connections: 31

Th...	Status	Mail Server	Email Address	Valid
1	Connecting	c.mx.mail.yahoo.com	chw@rocketmail.com	20
2	Connecting	b.mx.mail.yahoo.com	cfi@rocketmail.com	66
3	Connecting	c.mx.mail.yahoo.com	cko@rocketmail.com	64
4	Connecting	d.mx.mail.yahoo.com	ckt@rocketmail.com	18
5	Connecting	f.mx.mail.yahoo.com	cmi@rocketmail.com	73
6	Connecting	e.mx.mail.yahoo.com	cmj@rocketmail.com	90
7	Connecting	g.mx.mail.yahoo.com		50
8	Connecting	h.mx.mail.yahoo.com	cmj@rocketmail.com	55
9	Connecting	a.mx.mail.yahoo.com		30
10	Connecting	b.mx.mail.yahoo.com	cow@rocketmail.com	64
11	Connected	c.mx.mail.yahoo.com	czg@rocketmail.com	80
12	Connected	d.mx.mail.yahoo.com	cza@rocketmail.com	75
13	Connecting	e.mx.mail.yahoo.com		50
14	Connected	f.mx.mail.yahoo.com	cyj@rocketmail.com	150
15	Connected	g.mx.mail.yahoo.com	czk@rocketmail.com	79
16	Connected	h.mx.mail.yahoo.com	czh@rocketmail.com	57
17	Connecting	a.mx.mail.yahoo.com	ctj@rocketmail.com	128
18	Connected	b.mx.mail.yahoo.com	czf@rocketmail.com	21
19	Connecting	c.mx.mail.yahoo.com		50
20	Connecting	d.mx.mail.yahoo.com		50
21	Connected	e.mx.mail.yahoo.com	czj@rocketmail.com	59
22	Connecting	f.mx.mail.yahoo.com	cul@rocketmail.com	124
23	Connected	g.mx.mail.yahoo.com	czl@rocketmail.com	55

Collected Emails

- bmw@rocketmail.com
- bmw@rocketmail.com
- bmx@rocketmail.com
- bmy@rocketmail.com
- bmz@rocketmail.com
- bna@rocketmail.com
- bnb@rocketmail.com
- bnc@rocketmail.com
- bne@rocketmail.com
- bnd@rocketmail.com
- bnf@rocketmail.com
- bng@rocketmail.com
- bnh@rocketmail.com
- bnj@rocketmail.com
- bnk@rocketmail.com
- bnl@rocketmail.com
- bnm@rocketmail.com
- bnn@rocketmail.com
- bno@rocketmail.com
- bnp@rocketmail.com
- bnq@rocketmail.com
- bnr@rocketmail.com
- bnr@rocketmail.com

Session Time: 0:1:9 Valid Emails: 1972 Checked Emails: 1972 Valid Emails Per Hour: 111600

Locating Network Activity

Tool: GEOSpider

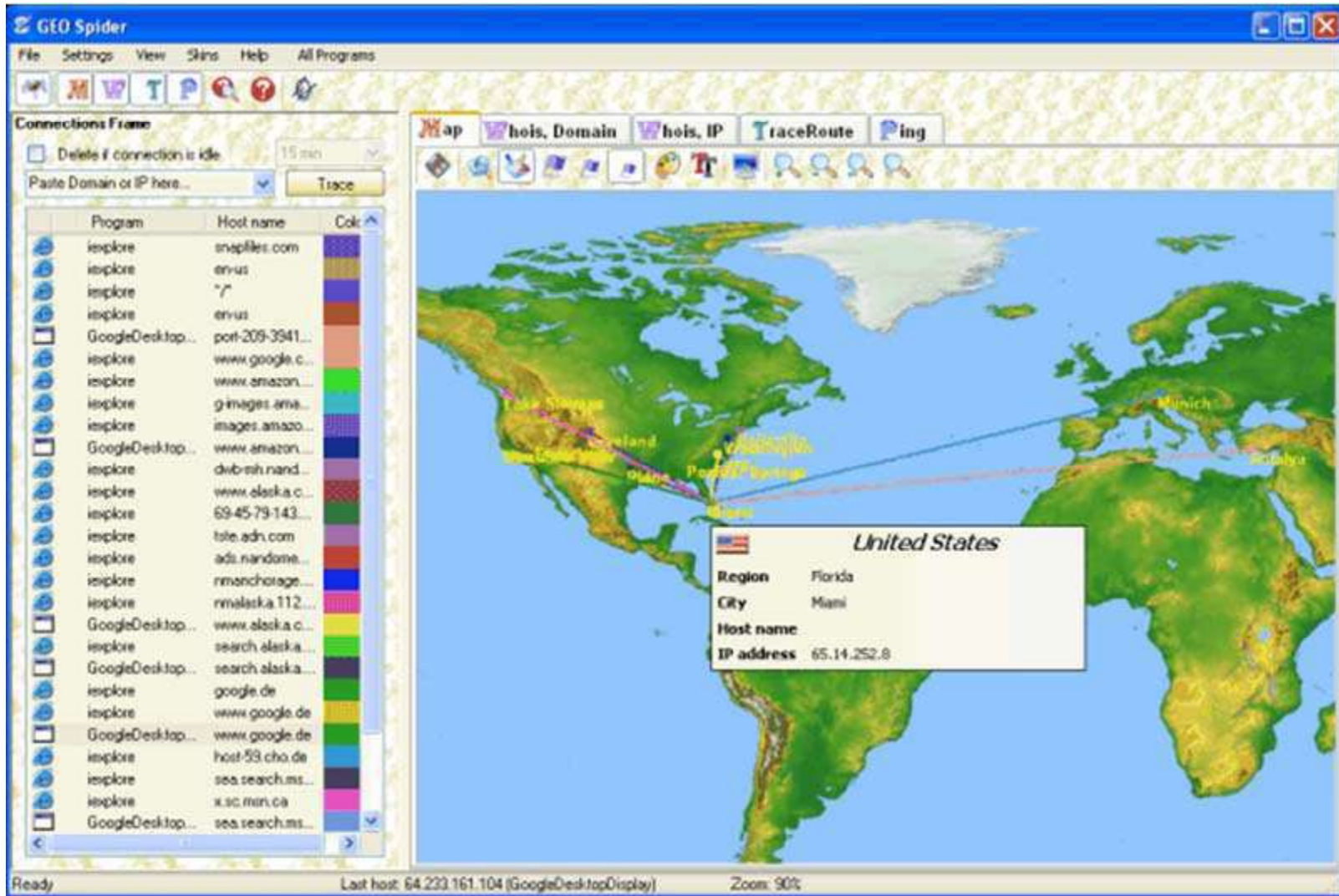


GEO Spider helps you to detect, identify, and monitor your network activity on the world map

You can see website's IP address location on the Earth

GEO Spider can trace a hacker, investigate a website, and trace a domain name

GEOSpider: Screenshot



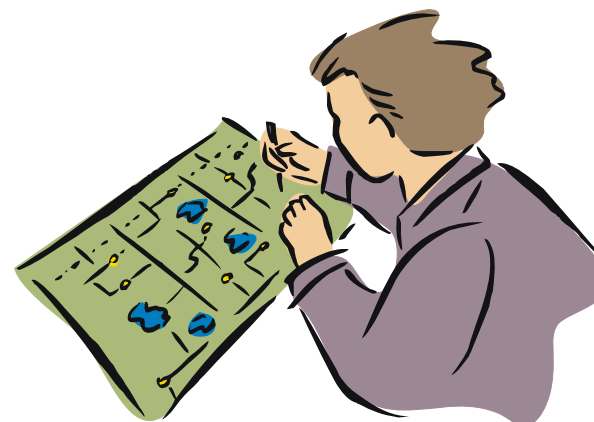
Tool: Geowhere

Geowhere handles many popular newsgroups to find answers to your queries in an easy and fast manner

Geowhere can also seek information from country specific search engines for better results

Use Geowhere to footprint an organization's:

- Newsgroups Search
- Mailing list finder
- Easy Web Search
- Daily News



Geowhere: Screenshot

GeoWhere v2.0 (Deluxe Version)

You can stop this help panel by going in the MISC section of the settings

Music Search

300 Sites	Location	Source
A1OnlineMall - Link To Music - CDs - DVD... Movies, Music, Books & More	http://www.a1onlinemall.co...	FindWhat
In London? Find great music buys in real s...	http://www.abcaz.com/def...	eSpotting
AllCheapMusicEtc.com Discount & Hard T...	http://www.allcheapmusicet...	FindWhat
Mp3's, Music, And More!	http://www.allextremsports...	FindWhat
AMG All Music Guide	http://www.allmusic.com/	Hotbot/Lycos
AMG All Music Guide	http://www.allmusic.com/	DirectHit
Posters and Prints At AllPosters.com!	http://www.allposters.com/	FindWhat

around your area? Currently 475K products in 3,000+ shops across Greater London and beyond.

[Search in results](#)

USA TODAY: Save 33% Off Home Delivery
 Special Internet Offer: Subscribe to USA TODAY and save 33% off Home Delivery. Receive the most up-to-date NEWS, SPORTS, MONEY, and LIFE. You'll get late breaking news from across the nation and

GeoWhere : The easy way to search what you want

Translate

EN ==> FR

Auto-Get search description

Translate

 autour de votre secteur ? Actuellement produits 475K dans 3.000 magasins à travers le grand Londres et là-bas.

kelkoo
 LYCOS
 Dealtime United Kingdom
 abcaz in your high street

Web Search
 Newsgroups Search
 Chat Forum Finder
 Find Identical Files
 Easy Web Search

Daily News
 Sport News

Currencies
 Units Convertor
 Road Planner

Bookmark Tester
 Internet Kit
 Domain Name
 Proxy Finder
 Proxy Analyzer

Settings ?

Favorites

GEOWHERE

GoogleEarth

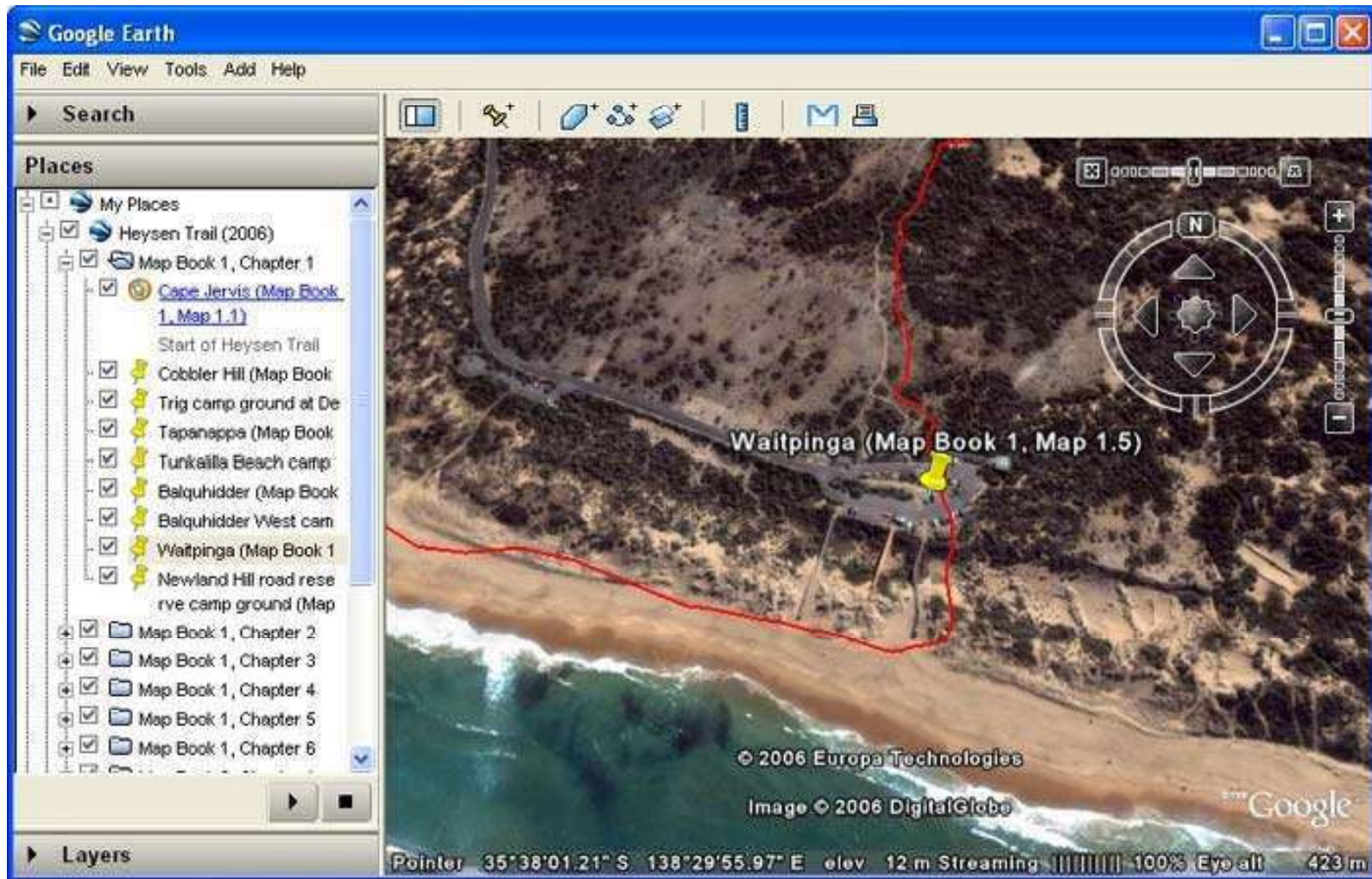
Google Earth puts a planet's worth of imagery and other geographic information right on your desktop

You can footprint the location of a place using GoogleEarth

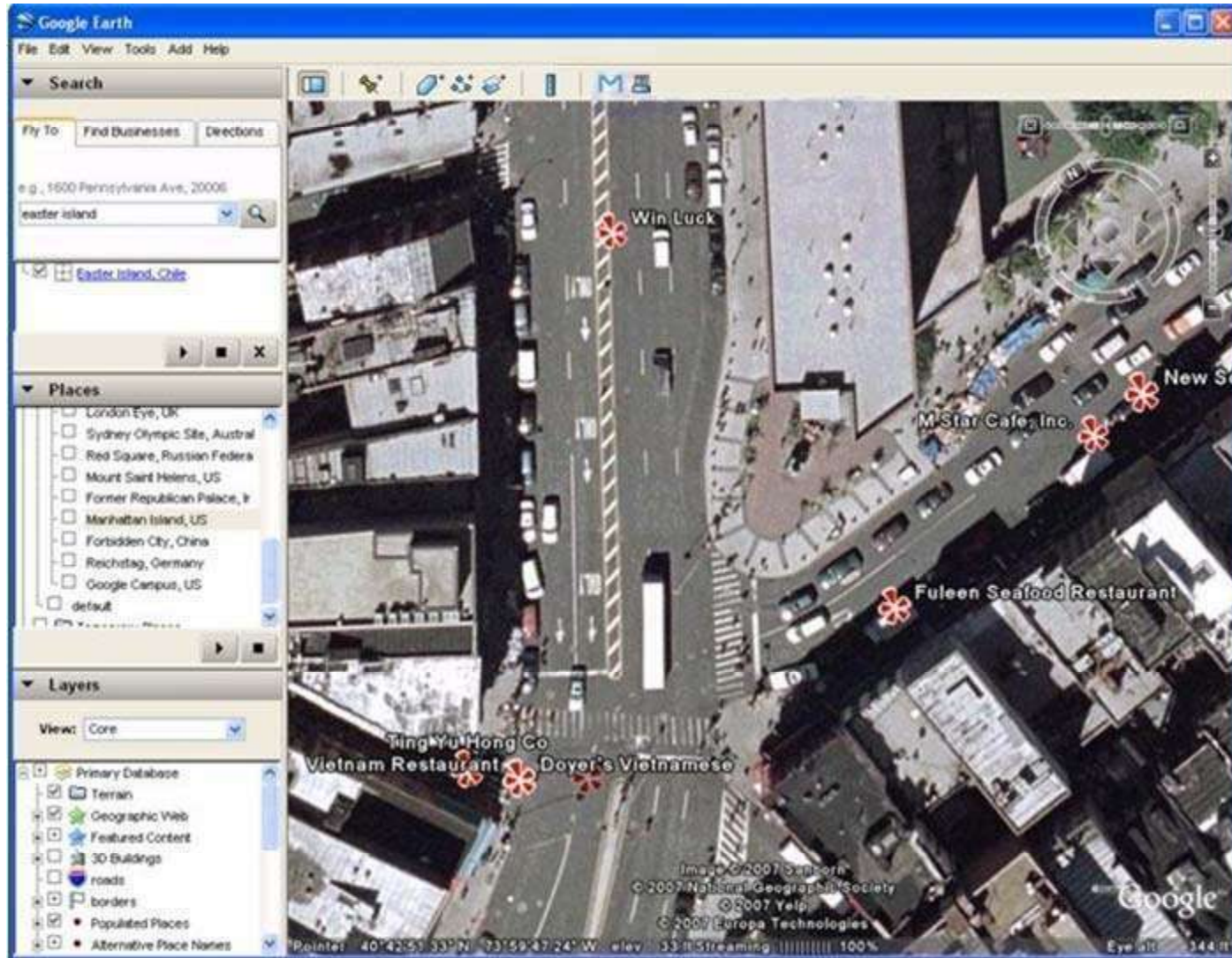
Valuable tool for Hackers



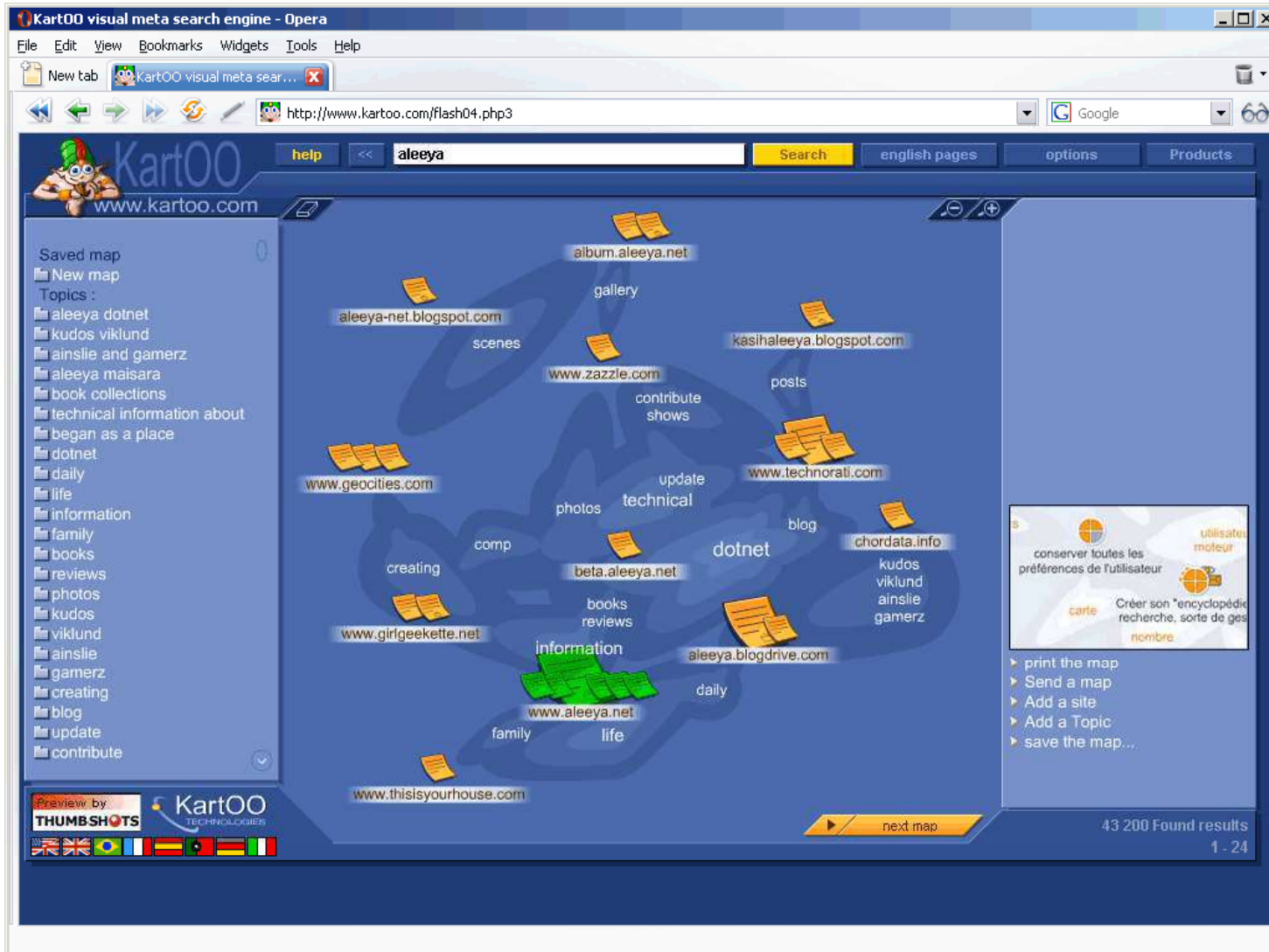
GoogleEarth (cont'd)



GoogleEarth (cont'd)



Search Engines



Dogpile (Meta Search Engine)



Dogpile is a meta search engine; it gets results from multiple search engines and directories and then combines them and presents to the user

Dogpile page provides code to add search tool to your website

It chases down the best results from Internet's top search engines, including Google, Yahoo! Search, MSN, Ask Jeeves, About, MIVA, LookSmart and others

dögpilē[®]

Dogpile (Meta Search Engine): Screen Shot

dögpile[®]

All the best search engines piled into one.

Google YAHOO! SEARCH Live Search Ask

Web Images Audio Video News Yellow Pages White Pages

[Go Fetch!](#) [Advanced Search Preferences](#)

Favorite Fetches: obama girl • flowers • valentine clipart • music lyrics • tattoo designs • vegas wedding
Joke of the Day • SearchSpy • Maps • Weather • Horoscope

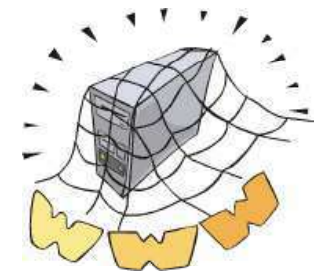
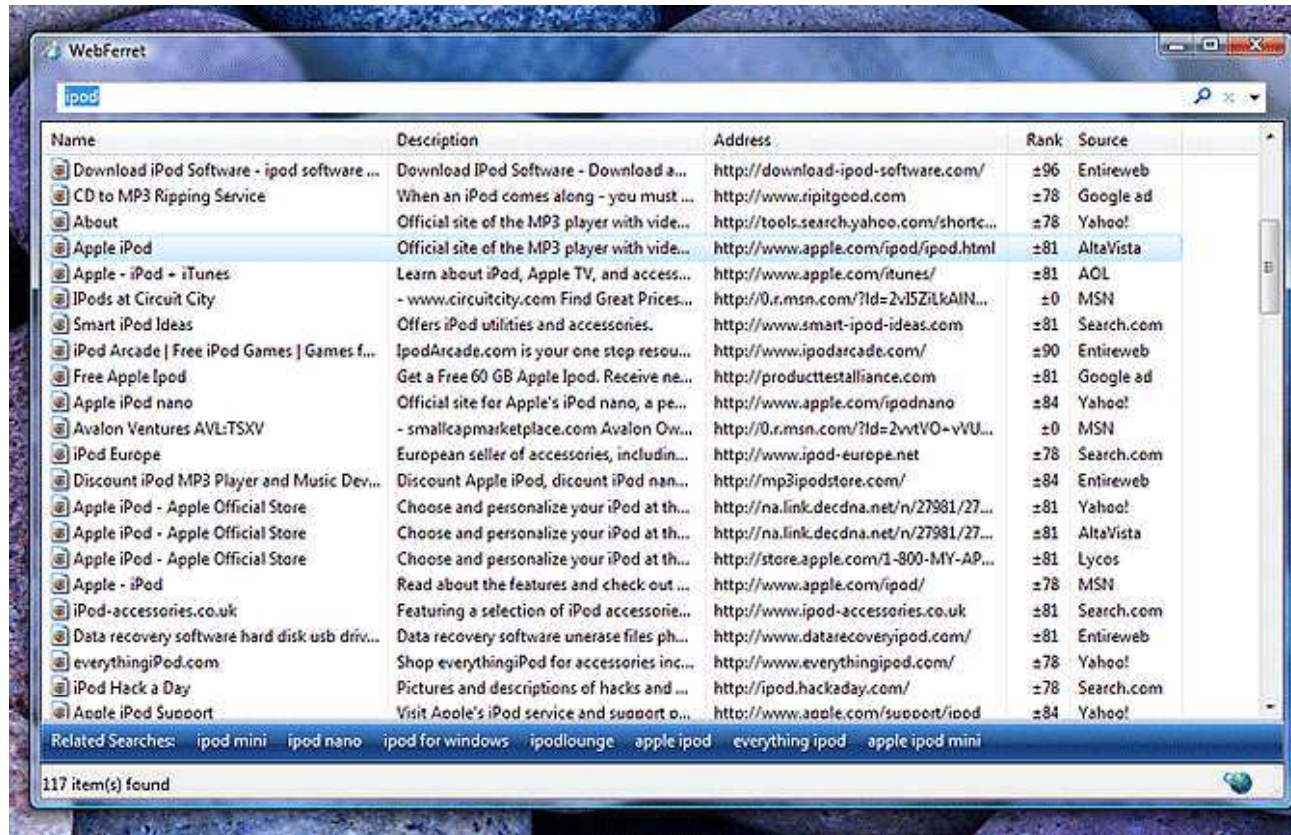
Opinions Wanted!
Help us improve Dogpile.
[Please answer some questions.](#)

infospace [About](#) • [About Dogpile](#) • [Tools & Tips](#) • [Download Toolbar](#) • [Add Dogpile Search to Your Site](#) • [Privacy Policy](#) • [Terms of Use](#) • [Contact Us](#)

Tool: WebFerret

WebFerret searches the web quickly and thoroughly by instantly submitting the search query to multiple search engines

All results are displayed in a single concise window



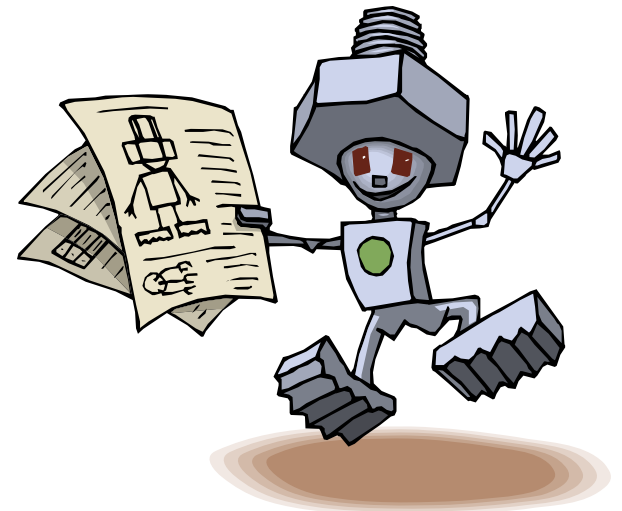
This page located at the root folder holds a list of directories and other resources on a site that the owner does not want to be indexed by search engines

All search engines comply to *robots.txt*

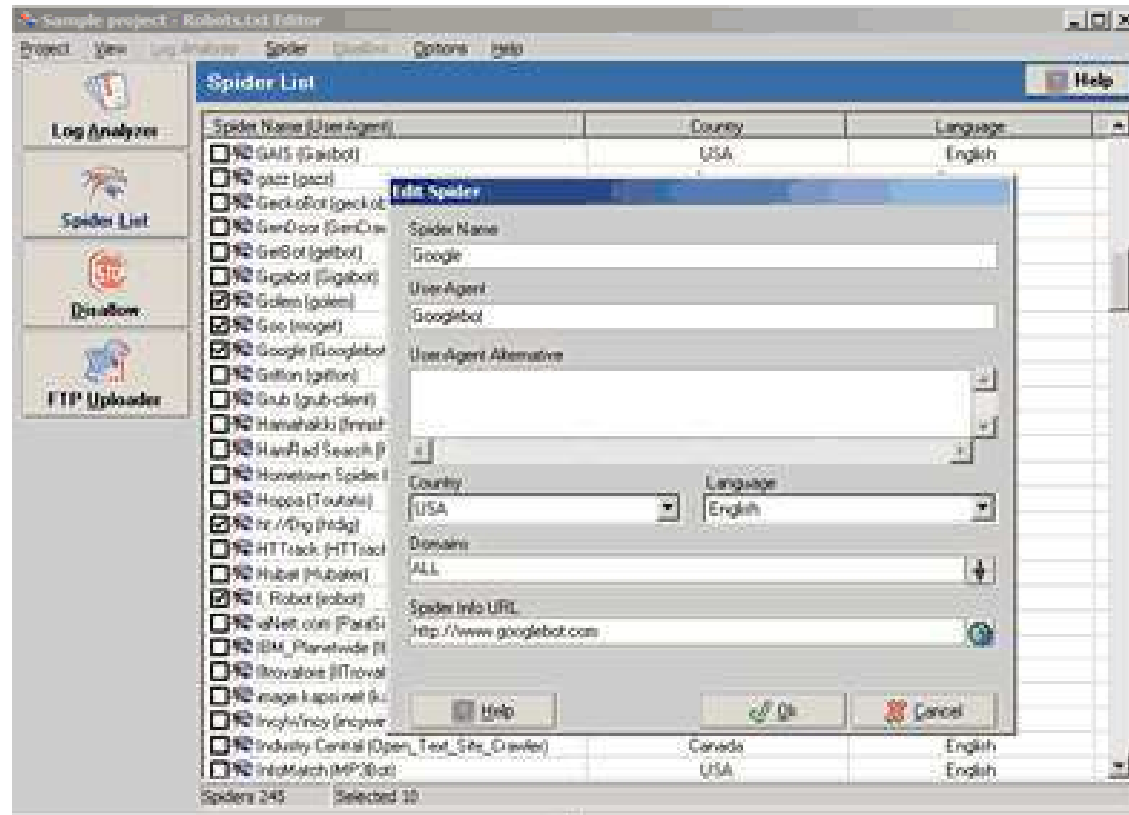
You might not want private data and sensitive areas of a site, such as script and binary locations indexed

◉ Robots.txt file

```
User-agent: *  
Disallow: /cgi-bin  
Disallow: /cgi-perl  
Disallow: /cgi-store
```



robots.txt: Screenshot



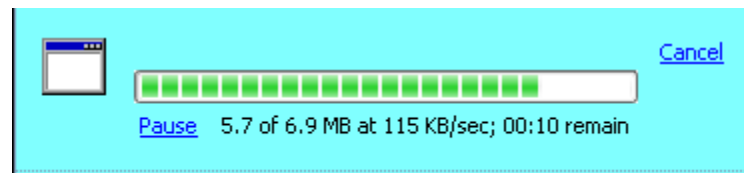
Tool: WTR - Web The Ripper

WTR - Web The Ripper 2 allows to select and download files that are linked from a specified web page

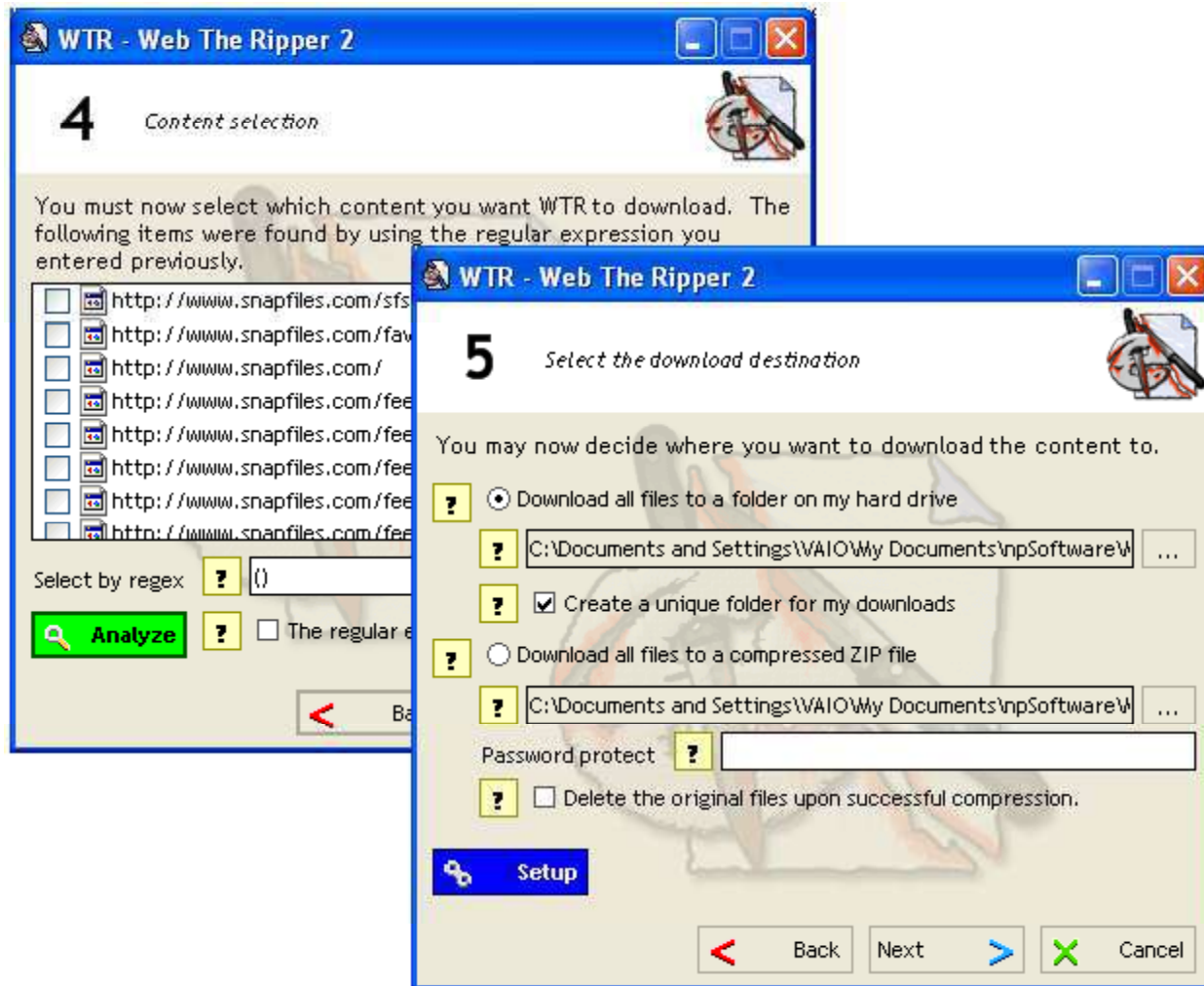
It analyzes input URL and then displays a list of all downloadable files (images, html, programs, mp3 etc.) allowing to select all or individual files

The files are downloaded to a folder of choice and the program can also be configured to automatically launch anti-virus scanner

In addition, you can specify an extension filter to limit downloads to the specified file types



WTR - Web The Ripper: Screenshot

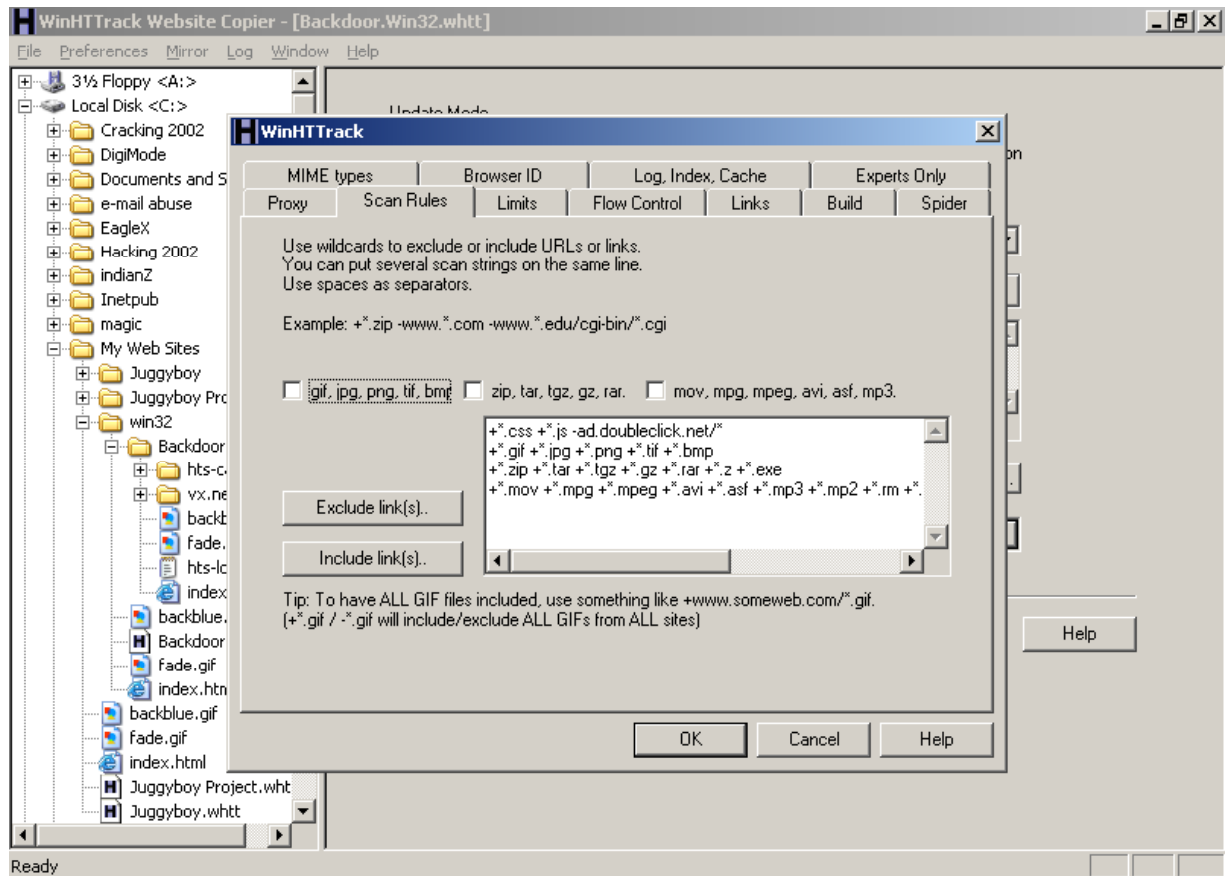
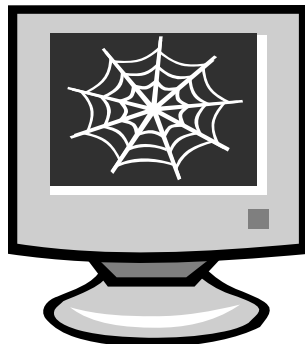




This tool mirrors an entire website to the desktop

You can footprint the contents of an entire website locally rather than visiting the individual pages

Valuable footprinting tool



Tool: Reamweaver

Reamweaver lets the user automatically "funhouse-mirror" anyone's website

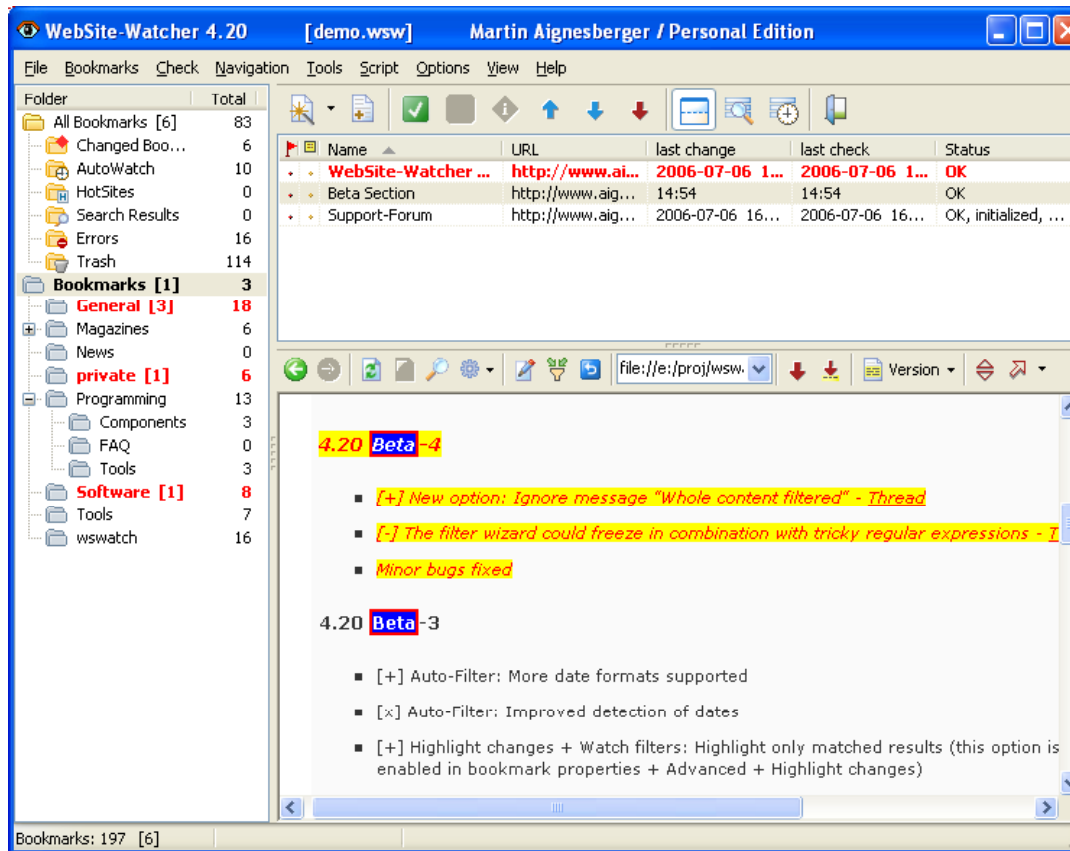
When a visitor visits a page on your Reamweaver site, Reamweaver gets the page from the target domain, changes the words as you specify, and stores the result (along with images, etc.)



Tool: Website Watcher

Website watchers can be used to get updates on the website

Can be used for competitive advantages



Website Watcher: Screenshot 1

The screenshot shows the Website-Watcher application window. On the left is a folder tree with columns for 'Folder' and 'Total'. The main area contains a table of monitored websites with columns for 'Name', 'URL', 'last check', and 'Status'. The bottom right pane shows a log of updates, including a section for '3.31 Beta -2' with a list of changes.

Folder	Total
Bookmarks	0
All Bookmarks [5]	80
Changed Book...	5
HotSites	0
AutoWatch	10
Disabled Bookm...	12
Errors	16
Trash	0
General [3]	18
Magazines	6
News	0
private [1]	6
Programming	13
Components	3
FAQ	0
Tools	3
Software [1]	8
Tools	7
swatch	16

Name	URL	last check	Status
WebSite-Watcher (PAD)	http://aignes.net/pad/...	28-Nov-2001 - ...	OK
FTP-Uploader	http://www.ftp-uploader.de...	28-Nov-2001 - 07:59	OK
NetCaptor	http://www.netcaptor.com/	28-Nov-2001 - 08:01	OK
Opera - the fastest browser ...	http://www.opera.com/	28-Nov-2001 - 08:01	OK
PADGen	http://www.asp-shareware...	28-Nov-2001 - 08:01	OK
The Bat	http://www.rtlabs.com/the...	28-Nov-2001 - 08:03	OK
WebSite-Watcher BETA	http://aignes.net/beta.htm	28-Nov-2001 - 12:33	OK
WinRAR	http://www.rarsoft.com/wel...	28-Nov-2001 - 08:02	OK

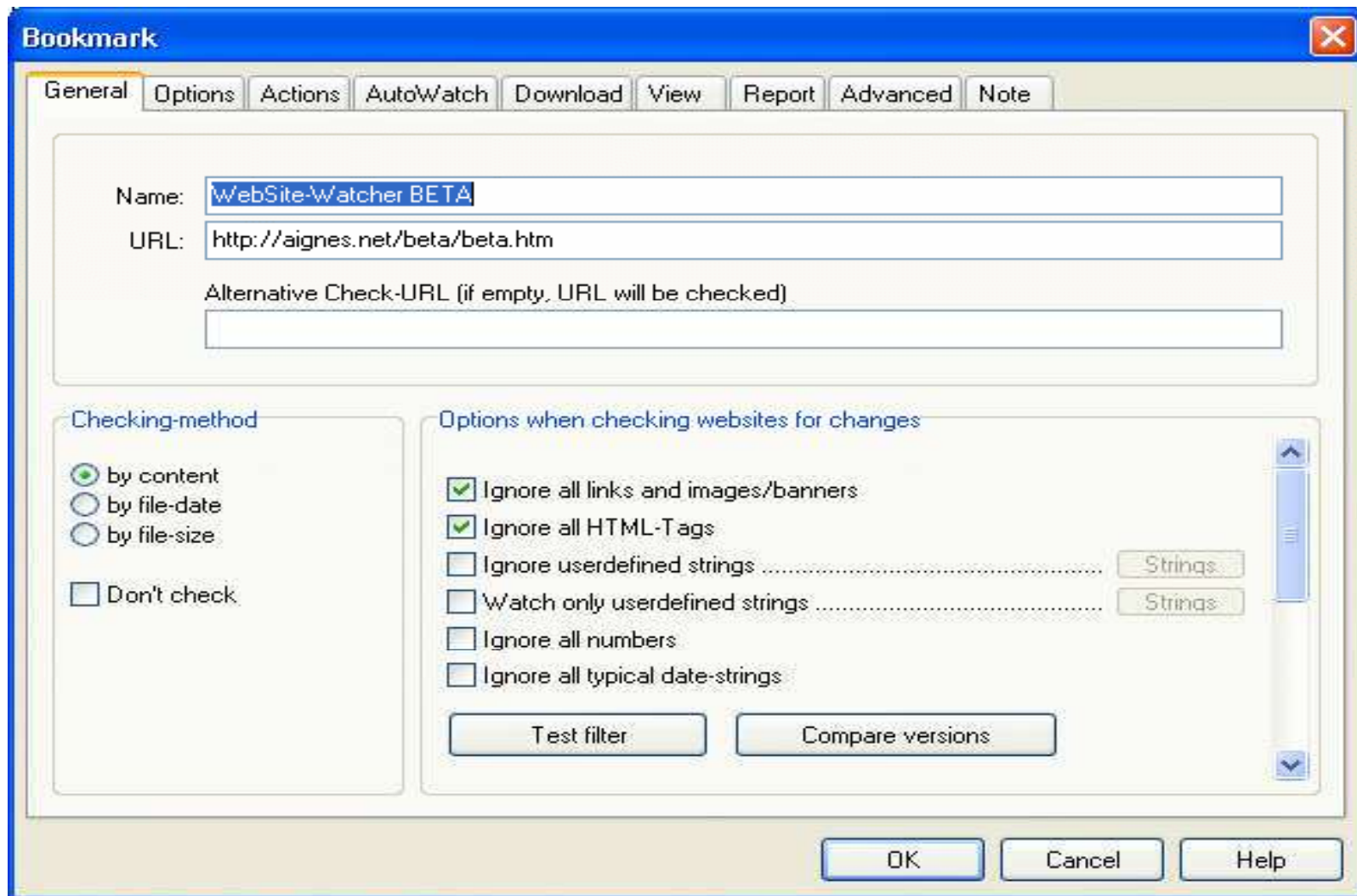
setting "use default path" was enabled

- [-] bugfix: button "Test filter" in dialog "ignore userdefined strings" didn't work properly, if there were more than one regular expressions entered
- [-] minor bugs fixed

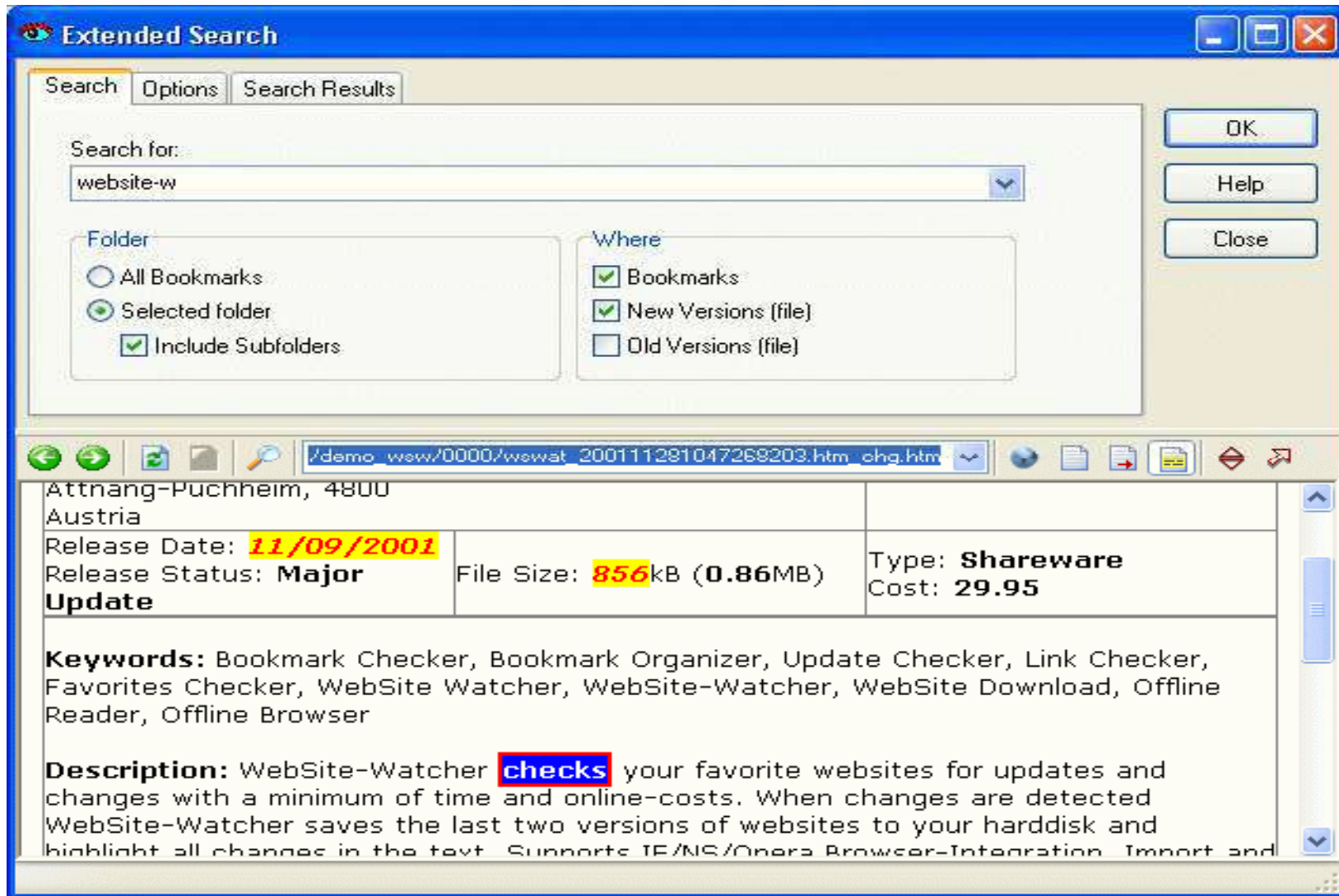
3.31 Beta -2

- [+] Bookmark properties / new check option: max. one update per week
- [+] Bookmark properties / new AutoWatch option: max. one update per week
- [+] New report fields: <!--wsw_note--> and <!--wsw_note_format-->
- [-] relative links were not converted correctly to

Website Watcher: Screenshot 2



Website Watcher: Screenshot 3



How to Fake Websites

Steps to Create Fake Login Pages

1

- Open any form building website (www.xyz.com) and sign up

2

- Login with newly registered account

3

- Click → Create First Form

4

- Delete all pre-defined entries and just leave 'First Name'

5

- Click → First Name and Click → Power Tool Option

6

- Double click → PasswordBox

7

- Click the newly form password entry to rename it as 'Password'

8

- Click → Properties Option

How to Create Fake Login Pages (cont'd)

9

- Give any title to the form

10

- Put any link, say <http://www.google.com> in Thank You URL

11

- Click → Save and click → Source Option

12

- Two Options: Option 1 & Option 2 are visible, copy the full code of 'Option 2'

13

- Open notepad and write the 'Option 2' code

14

- Save the notepad file as index.html

15

- Host this 'index.html' on Internet by using FREE hosting provider service

16

- Login in your hosting account and open 'File Manager'

17

- Upload index.html

Faking Websites using Man-in-the-Middle Phishing Kit

This kit enables hackers to sit between prospective marks and legitimate businesses

Using Universal Man-in-the-Middle Phishing Kit, an attack can be launched to import pages from any target website

Malicious users can use this kit to do phishing attacks

It can intercept any type of credentials submitted to a target site

Faking Websites using Man-in-the-Middle Phishing Kit (cont'd)

Fraudsters use Universal Man-in-the-Middle Phishing Kit to create a fake URL via a simple and user-friendly online interface

This fake URL communicates with the legitimate website of the targeted organization in real-time

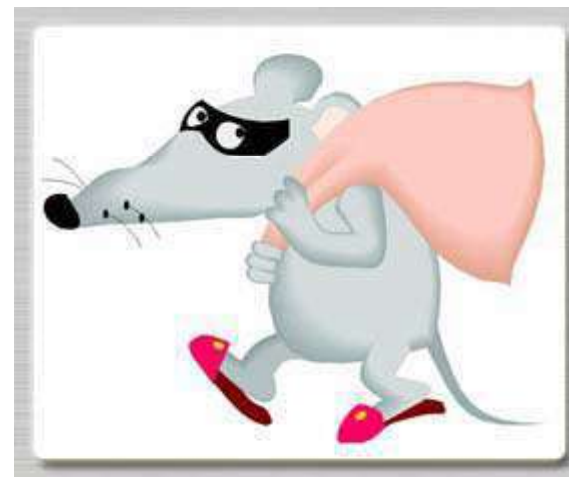
The target victim receives a phishing email and when clicking on the link s/he is directed to the fake URL



Benefits to Fraudster

Using Universal Man-in-the-Middle Phishing Kit, attackers can launch attack to import WebPages from any target website

This kit can launch attacks, which can intercept any type of credentials submitted to the site after the victim has logged into the account



Steps to Perform Footprinting

- 1 • Find companies' external and internal URLs
- 2 • Perform whois lookup for personal details
- 3 • Extract DNS information
- 4 • Mirror the entire website and look up names
- 5 • Extract archives of the website
- 6 • Google search for company's news and press releases
- 7 • Use people search for personal information of employees
- 8 • Find the physical location of the web server using the tool "NeoTracer"
- 9 • Analyze company's infrastructure details from job postings
- 10 • Track the email using "readnotify.com"

What Happened Next

Mason footprints Xmach Inc and gets some critical information which helps him in his assault on the notebook manufacturer.

The following is a partial list of information that Mason gathered :

- Domains and Sub Domains
- IP address and address range
- Contact Details of some employees including the Network Administrator; it included telephone number, email id, and address
- Current Technologies
- DNS information
- Firewalls

Mason now has enough information to bring down the network of Xmach Inc

Information gathering phase can be categorized broadly into seven phases

Footprinting renders a unique security profile of a target system

Whois and ARIN can reveal public information of a domain that can be leveraged further

Traceroute and mail tracking can be used to the target specific IP and later for IP spoofing

Nslookup can reveal specific users and zone transfers can compromise DNS security

Copyright 1998 Randy Glasbergen. www.glasbergen.com



“I’m paid \$4,000,000 a year. You’re paid \$40,000. The only difference is a few zeros. Everyone knows that zero equals nothing. So what’s the problem?”

© 2000 Randy Glasbergen.
www.glasbergen.com



**"Information security is becoming a big problem here.
Do you still have my Captain Crunch decoder ring, Ma?"**