TRACING EMAILS, EMAIL ACCOUNTS, AND IP ADDRESSES

SPECIAL AGENT SHEILA GORRIZ
Miami Electronic Crimes Task Force
United States Secret Service

IP (INTERNET PROTOCOL) ADDRESS

- Numeric string assigned by an ISP (INTERNET SERVICE PROVIDER) to a customer during an online session

- Example of an IP Address: 265.89.650.43

IP ADDRESS, continued

****IMPORTANT****

- An IP Address does not by itself identify a particular computer on the Internet

- An IP address does show that a computer, using the assigned IP Address, accessed the Internet

What service was utilized to commit the crime or suspect activity?

Internet Service (IS)

or

Internet Service Provider (ISP)

INTERNET SERVICE (IS)

- Company that provides their customer with free services (chat, email, search engine) on the Internet
- Registration is free and the identity of the user is rarely, and usually never, verified
- Examples: Yahoo, Hotmail, Google, Kazaa, Bearshare

- **A customer does not pay for the IS's services**
- **IS does not provide a customer with Internet access**

INTERNET SERVICE PROVIDER (ISP)

- The company provides a customer with Internet access
- The company provides the customer with additional services (chat, search engines, email)
- Examples: AOL, Earthlink, Bellsouth, Comcast

- **A customer PAYS the ISP for Internet access!**

Types of IP Addresses provided by the ISP.

DYNAMIC

or

STATIC

DIAL-UP SERVICE

- DIAL-UP is accessing the Internet by making a telephone call (dialing) to the ISP
- Customer will usually be assigned a different IP address for each Internet session; this is a dynamic IP address
- Example:
  - On 08/05/07 at 6:50 pm, the customer dials into the ISP for Internet access and is assigned IP address **657.12.412.6**
  - On 08/06/07 at 7:12 am, the customer dials into the ISP for Internet access and is assigned IP address **658.34.567.1**

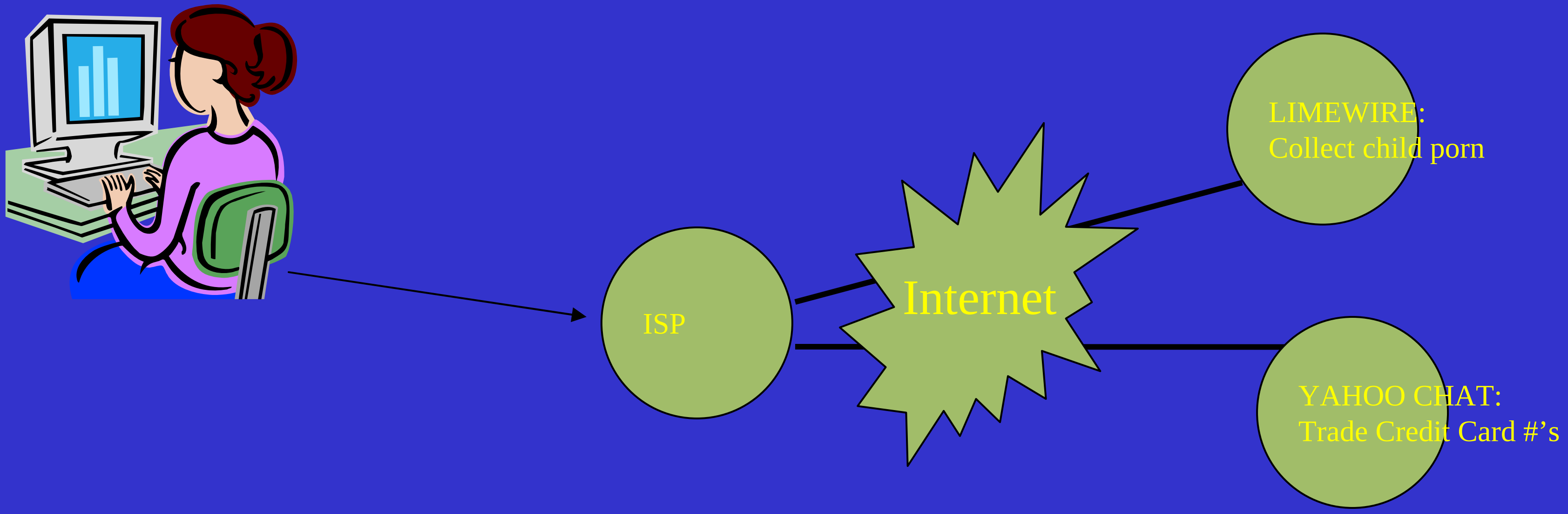
DIAL-UP, continued

- Ensure you request the ANI (AUTOMATIC NUMBER INFORMATION) from the ISP for the target IP address

- ANI is the phone number the customer used to access the ISP for internet service

- When you subpoena an IP Address, request the ISP provide you with the physical location of the DSL / Cable Modem

The Criminal Mind and Feeling Safe



ISP

Internet

LIMEWIRE:
Collect child porn

YAHOO CHAT:
Trade Credit Card #'s

Suspects accessing the Internet through ISP feel safe committing the crimes using programs and sites such as Limewire, Yahoo, and Photo Sharing Websites

IS REGISTRATION

- The suspect will usually provide a false name and other personal information
- However, a suspect will sometimes provide some helpful information
- Example:
  - A Suspect signs up for a Hotmail email account. He provides a fake name and date of birth, but does provide accurate information about his town and state of residence.

IS REGISTRATION, continued

- An IS usually requests an alternate email address from a user during registration.

- When a customer registers for service, changes their password, attempts to change a password, and accesses the services of the IS (for example, an email account), the IS records the time and IP address of the customer.

ISP REGISTRATION

- Customer must provide a credit card, name, phone number, billing address, and other personal information.
- For a DSL / Cable Modem, the customer must provide the physical location for access to the Internet.

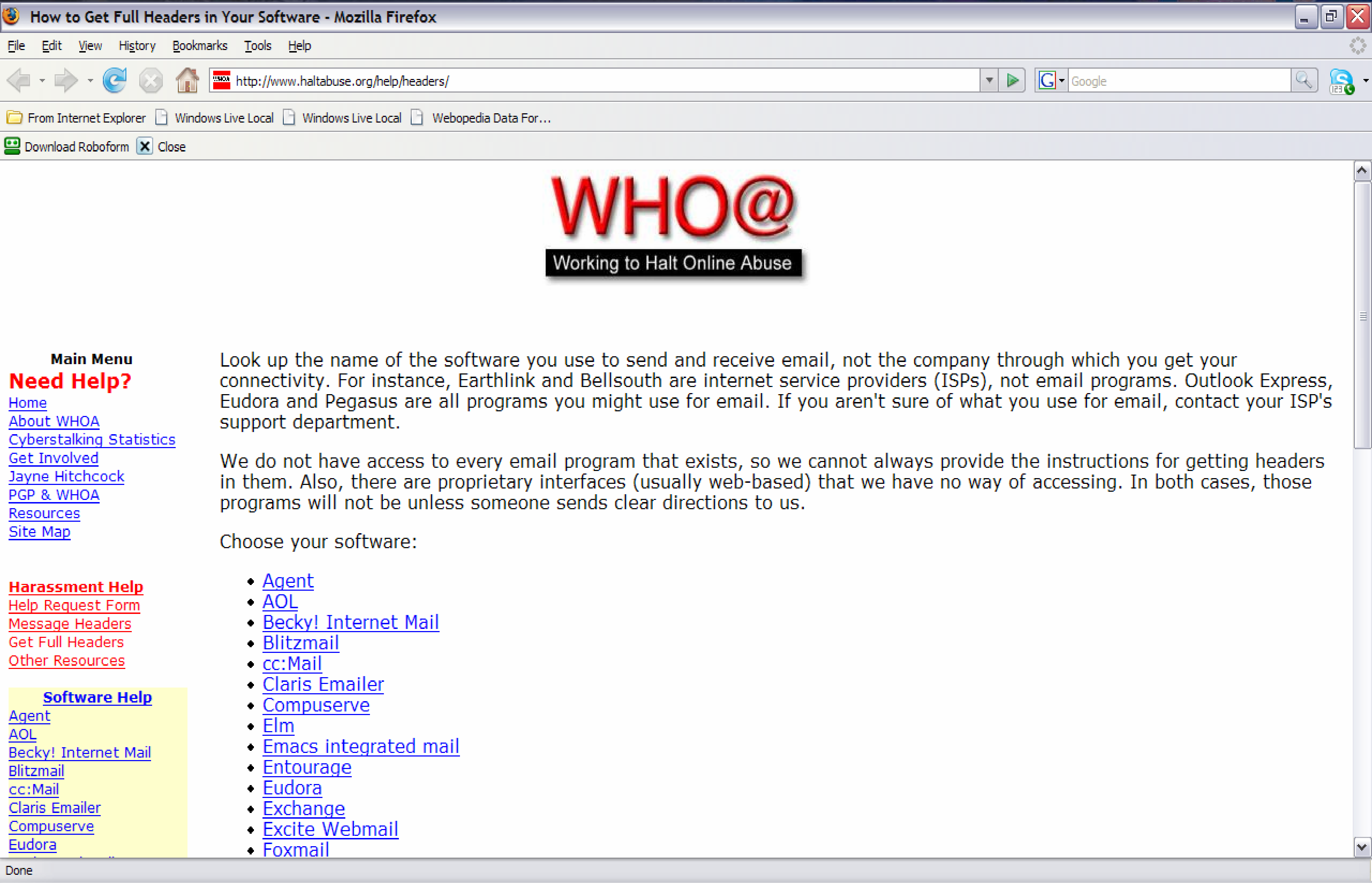
Please Note

- U.S. law does not require ISPs or SPs to retain any electronic data; what is the law on data retention in your country?
- Some providers purge their records every day, while some maintain a database for years
- The quicker you initiate the investigation, the better chance you have of recovering the information.

IP ADDRESS: EMAIL

- Email headers contain important information
  - Originating (sender’s) IP address
  - Date stamp
  - May even contain the sender’s full name

EMAIL HEADERS: HOW TO VIEW



Main Menu

Need Help?

- Home
- About WHOA
- Cyberstalking Statistics
- Get Involved
- Jayne Hitchcock
- PGP & WHOA
- Resources
- Site Map

Harassment Help

- Help Request Form
- Message Headers
- Get Full Headers
- Other Resources

Software Help

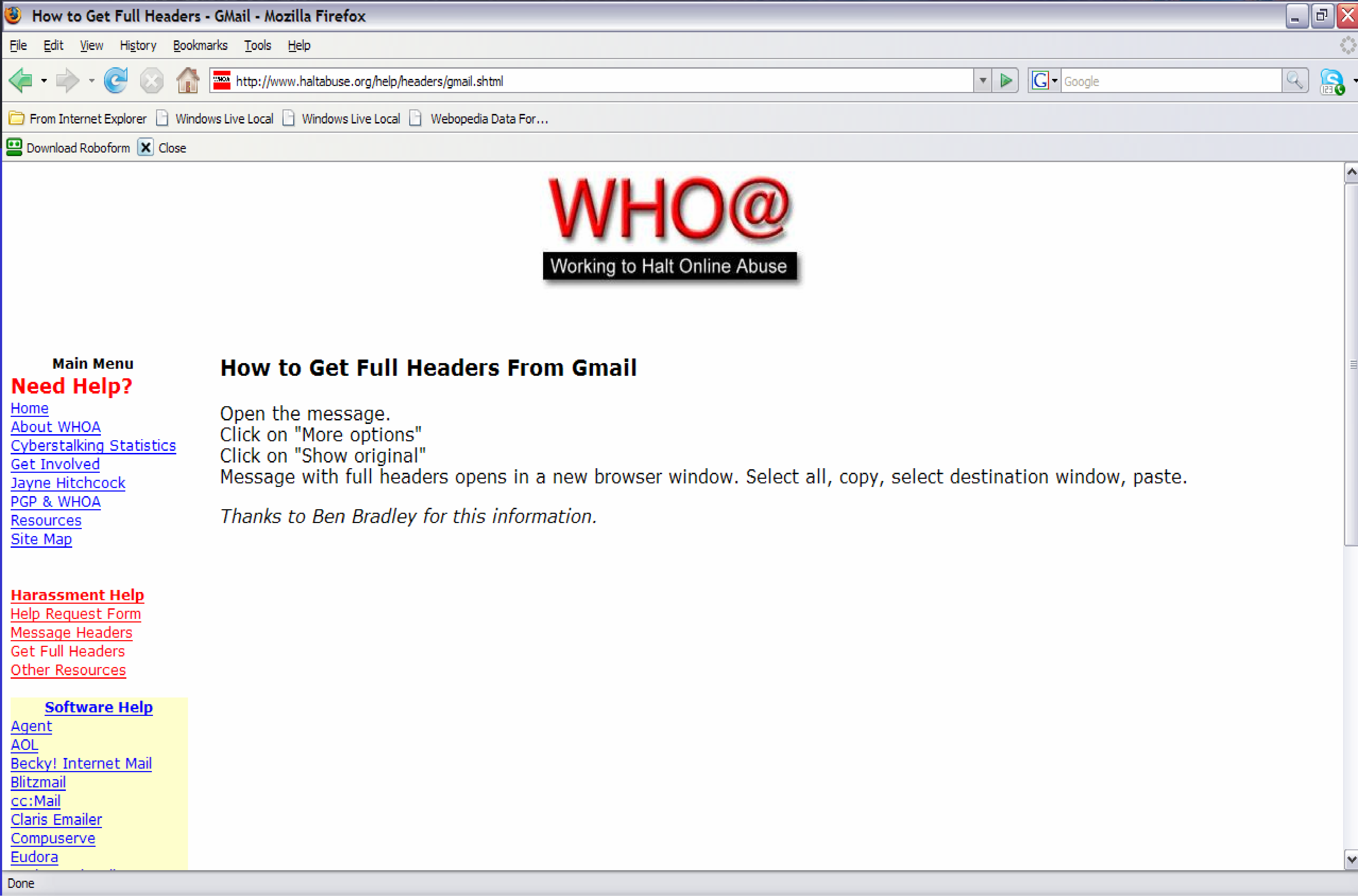
- Agent
- AOL
- Becky! Internet Mail
- Blitzmail
- cc:Mail
- Claris Emailer
- Compuserve
- Eudora

Look up the name of the software you use to send and receive email, not the company through which you get your connectivity. For instance, Earthlink and Bellsouth are internet service providers (ISPs), not email programs. Outlook Express, Eudora and Pegasus are all programs you might use for email. If you aren't sure of what you use for email, contact your ISP's support department.

We do not have access to every email program that exists, so we cannot always provide the instructions for getting headers in them. Also, there are proprietary interfaces (usually web-based) that we have no way of accessing. In both cases, those programs will not be unless someone sends clear directions to us.

Choose your software:

- Agent
- AOL
- Becky! Internet Mail
- Blitzmail
- cc:Mail
- Claris Emailer
- Compuserve
- Elm
- Emacs integrated mail
- Entourage
- Eudora
- Exchange
- Excite Webmail
- Foxmail



How to Get Full Headers From Gmail

Open the message.
Click on "More options"
Click on "Show original"
Message with full headers opens in a new browser window. Select all, copy, select destination window, paste.

Thanks to Ben Bradley for this information.

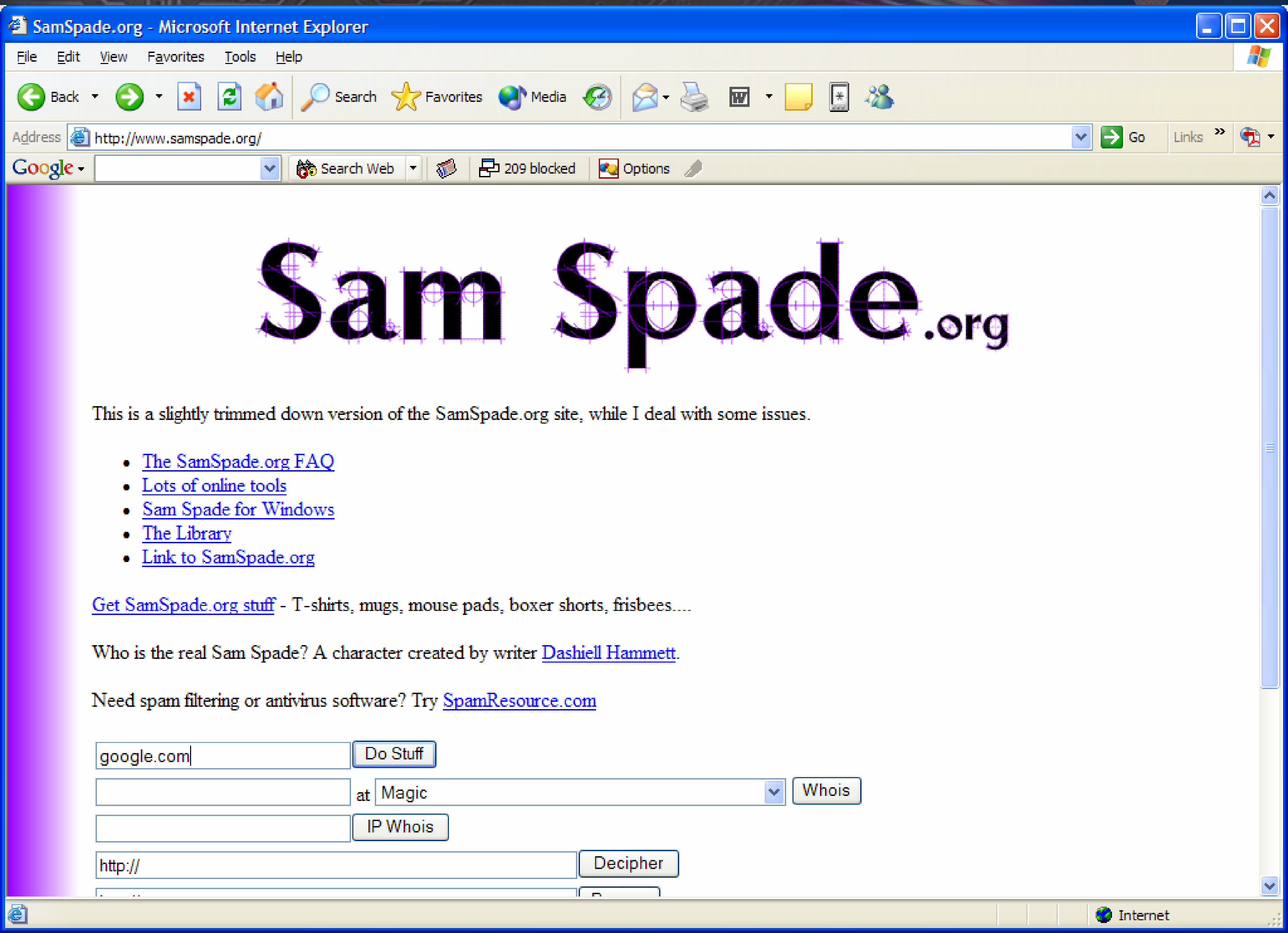
EXAMPLE HEADER

```
From - Mon Mar 19 08:17:17 2001
Return-Path: <wHargrove@newarkpd.state.de.us>
Received: from otma1.otm.state.de.us (votma1.state.de.us [167.21.1.115])
by copland.udel.edu (8.9.3/8.9.3) with ESMTP id NAA06271
for <sbunting@udel.edu>; Thu, 15 Mar 2001 13:10:40 -0500 (EST)
Received: from deljismail1.state.de.us (imail.deljis.state.de.us [172.20.66.11])
by otma1.otm.state.de.us (8.11.0/8.11.0) with ESMTP id f2FIA7t28739
for <sbunting@udel.edu>; Thu, 15 Mar 2001 13:10:07 -0500 (EST)
Received: from newarkpd.state.de.us [172.20.132.102] by deljismail1.state.de.us with ESMTP
(SMTPD32-5.05) id A8B32701AE; Thu, 15 Mar 2001 13:23:47 -0500
Received: by NEWARKPD with Internet Mail Service (5.5.1960.3)
id <FY66DSJT>; Thu, 15 Mar 2001 13:08:29 -0500
Message-ID: <777ED2AC6510D311BBB50000D11CB450167AAD@NEWARKPD>
From: William Hargrove <wHargrove@newarkpd.state.de.us>
To: "Steve Bunting (E-mail)" <sbunting@UDel.Edu>
Subject: good morning
Date: Thu, 15 Mar 2001 13:08:28 -0500
MIME-Version: 1.0
X-Mailer: Internet Mail Service (5.5.1960.3)
Content-Type: text/plain
X-Mozilla-Status: 8003
X-Mozilla-Status2: 00000000
```

“WHO IS”

How to Look Up Information to Start the Process

- Utilize free websites to identify the ISP for the target IP Address
- This gives you the company or ISP where you will submit your requests
  - – Subpoena or Informal



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.

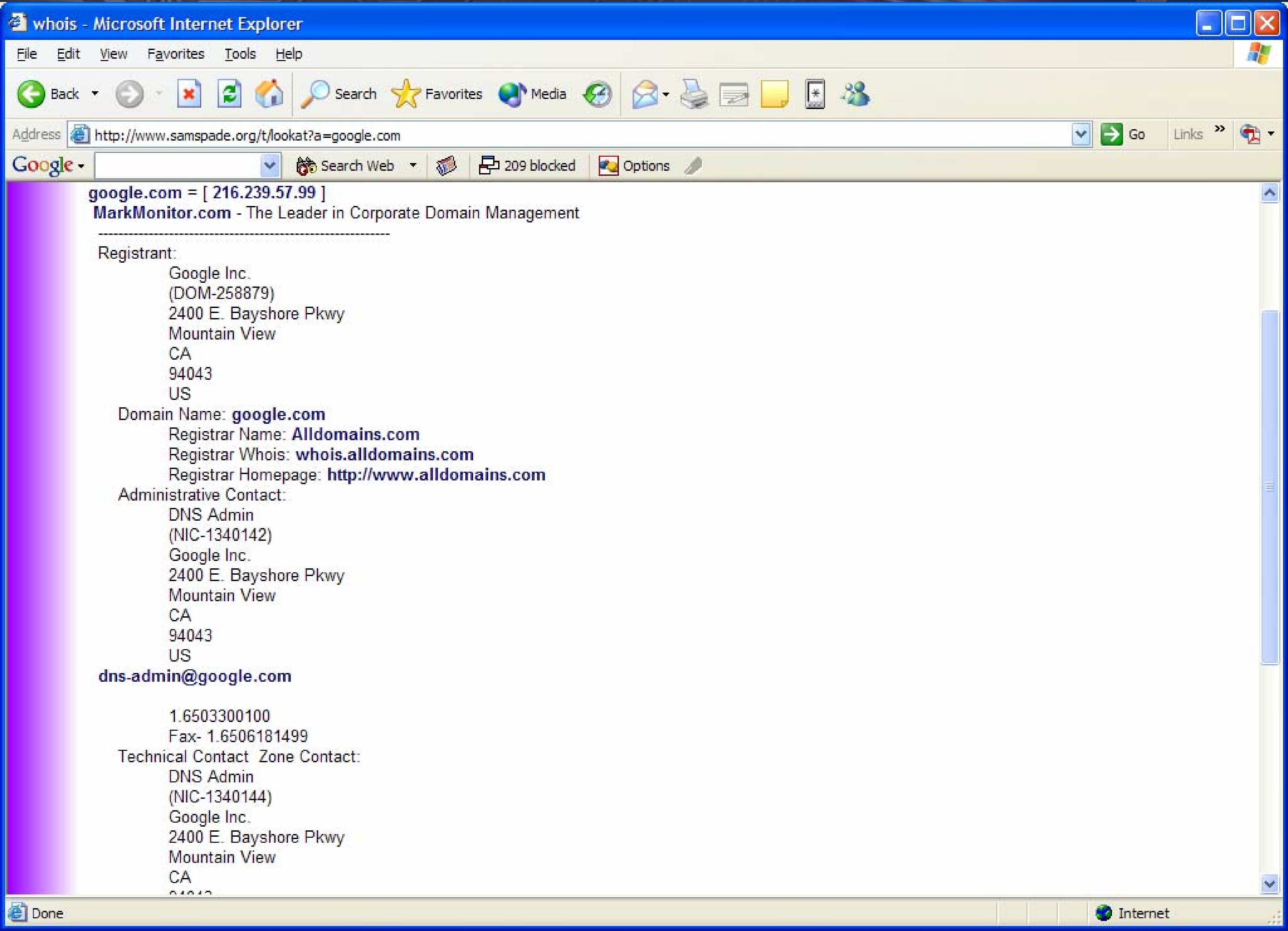
Need spam filtering or antivirus software? Try SpamResource.com

google.com Do Stuff

at Magic Whois

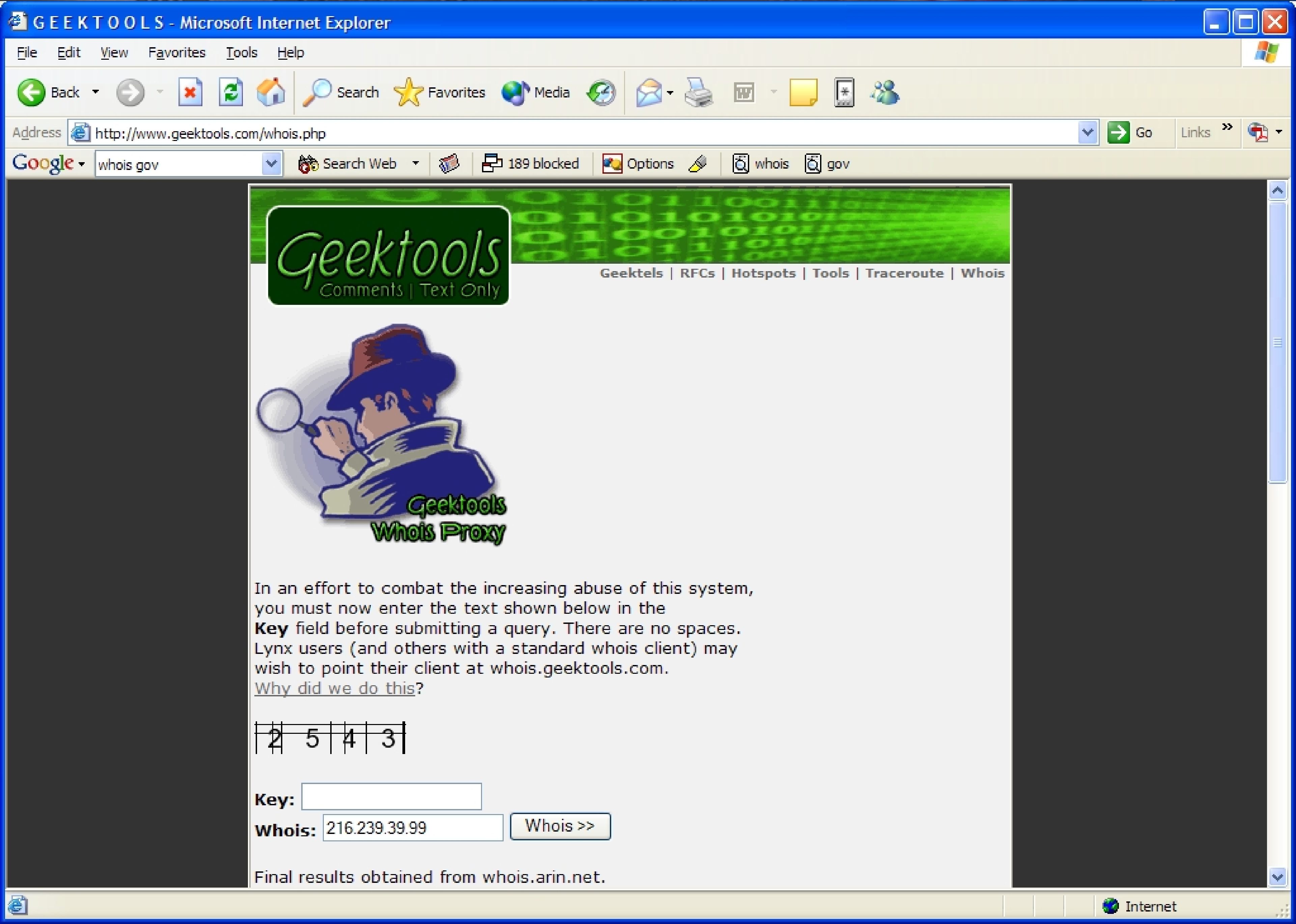
IP Whois

http:// Decipher



http://www.samspade.org/t/lookat?a=google.com

```
google.com = [ 216.239.57.99 ]
 MarkMonitor.com - The Leader in Corporate Domain Management
  ----------------------------------------------------------
  Registrant:
              Google Inc.
              (DOM-258879)
              2400 E. Bayshore Pkwy
              Mountain View
              CA
              94043
              US
      Domain Name: google.com
              Registrar Name: Alldomains.com
              Registrar Whois: whois.alldomains.com
              Registrar Homepage: http://www.alldomains.com
      Administrative Contact:
              DNS Admin
              (NIC-1340142)
              Google Inc.
              2400 E. Bayshore Pkwy
              Mountain View
              CA
              94043
              US
  dns-admin@google.com

              1.6503300100
              Fax- 1.6506181499
      Technical Contact, Zone Contact:
              DNS Admin
              (NIC-1340144)
              Google Inc.
              2400 E. Bayshore Pkwy
              Mountain View
              CA
```



Address http://www.geektools.com/whois.php

Google whois gov

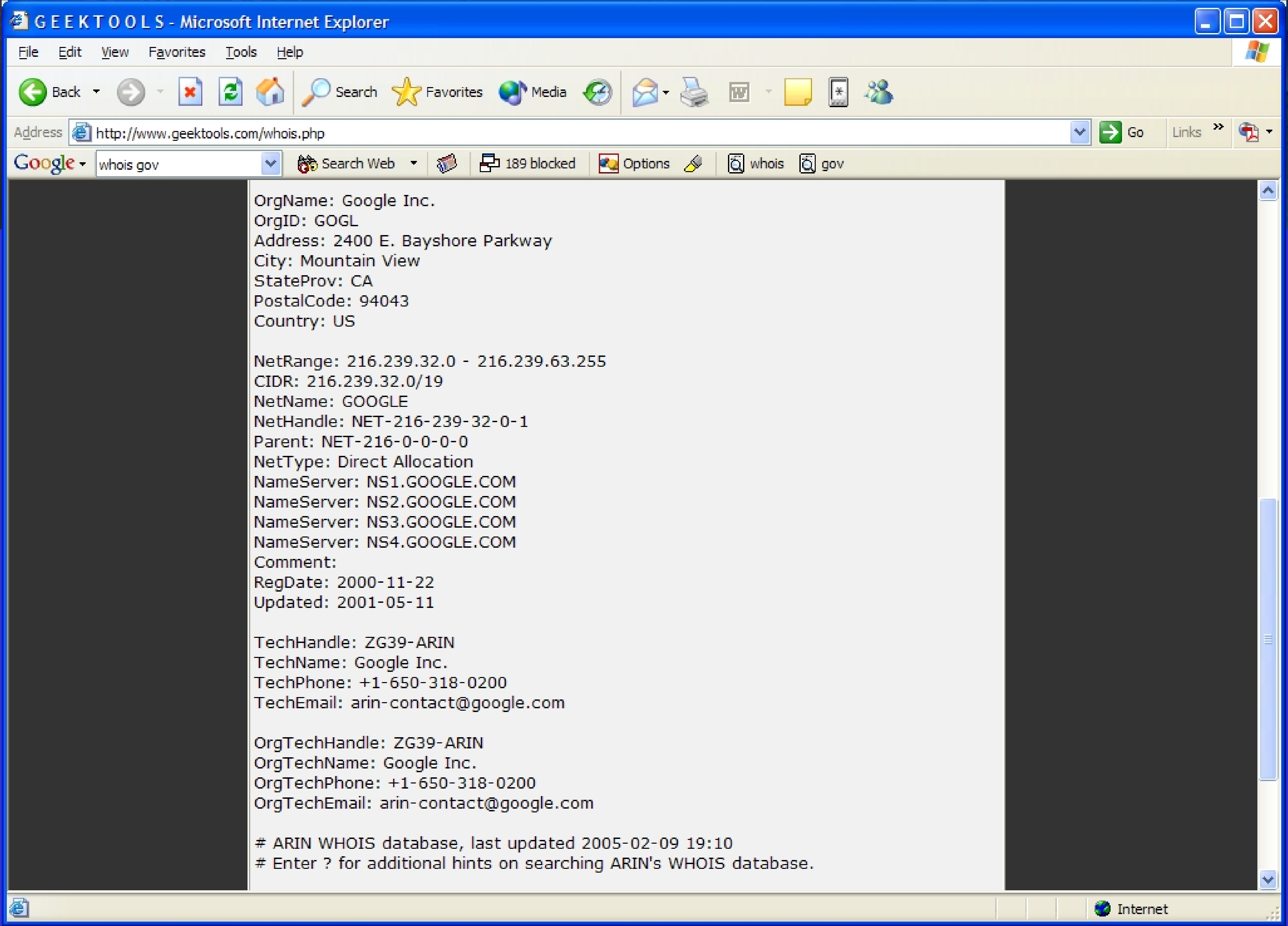
In an effort to combat the increasing abuse of this system, you must now enter the text shown below in the **Key** field before submitting a query. There are no spaces. Lynx users (and others with a standard whois client) may wish to point their client at whois.geektools.com. Why did we do this?

2 5 4 3

Key:

Whois: 216.239.39.99

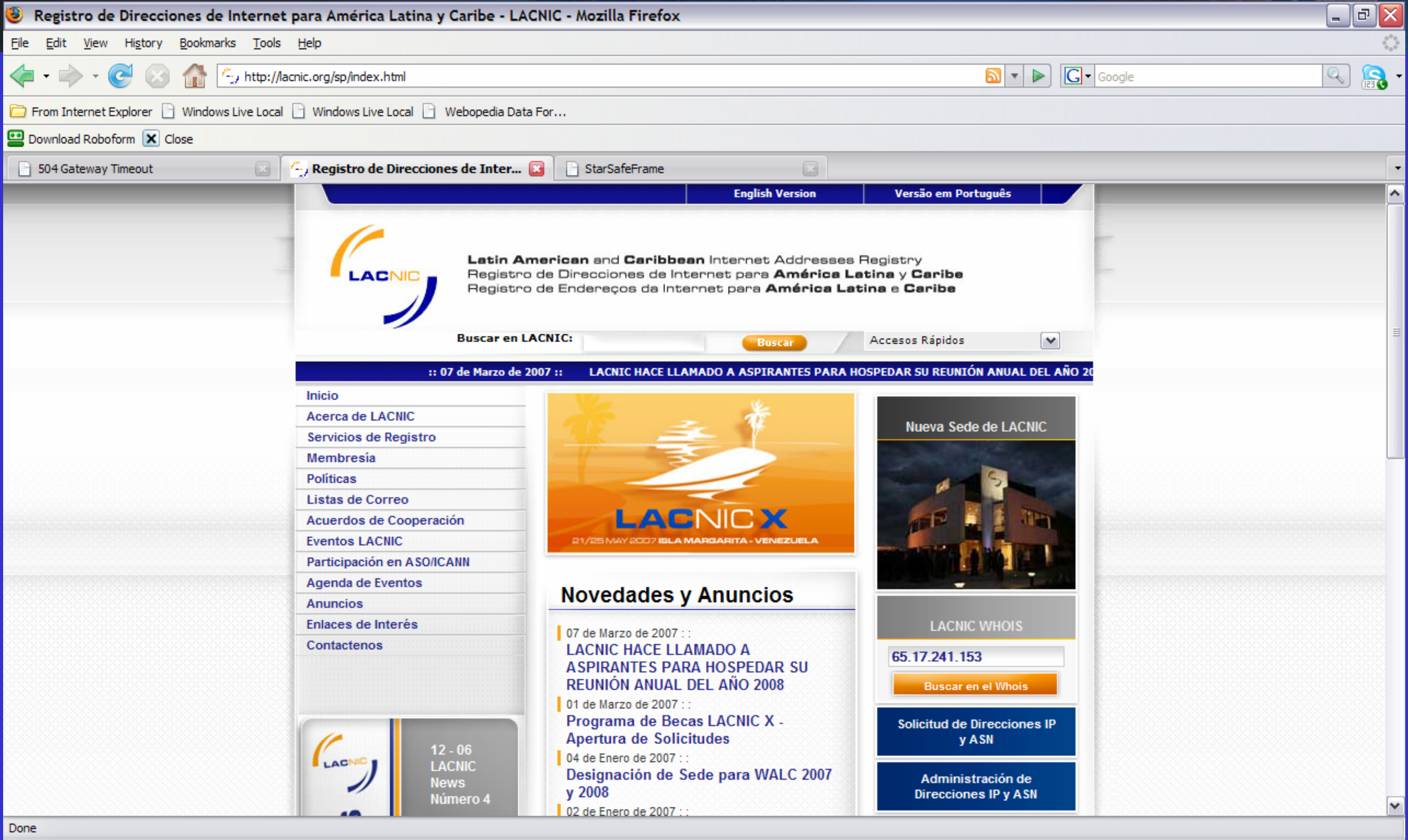
Final results obtained from whois.arin.net.



G E E K T O O L S - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://www.geektools.com/whois.php
Go
Links
Google whois gov
Search Web
189 blocked
Options
whois
gov
Internet

```
OrgName: Google Inc.
OrgID: GOGL
Address: 2400 E. Bayshore Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US

NetRange: 216.239.32.0 - 216.239.63.255
CIDR: 216.239.32.0/19
NetName: GOOGLE
NetHandle: NET-216-239-32-0-1
Parent: NET-216-0-0-0-0
NetType: Direct Allocation
NameServer: NS1.GOOGLE.COM
NameServer: NS2.GOOGLE.COM
NameServer: NS3.GOOGLE.COM
NameServer: NS4.GOOGLE.COM
Comment:
RegDate: 2000-11-22
Updated: 2001-05-11

TechHandle: ZG39-ARIN
TechName: Google Inc.
TechPhone: +1-650-318-0200
TechEmail: arin-contact@google.com

OrgTechHandle: ZG39-ARIN
OrgTechName: Google Inc.
OrgTechPhone: +1-650-318-0200
OrgTechEmail: arin-contact@google.com

# ARIN WHOIS database, last updated 2005-02-09 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

LACNIC.org



Latin American and Caribbean Internet Addresses Registry
Registro de Direcciones de Internet para América Latina y Caribe
Registro de Endereços da Internet para América Latina e Caribe

:: 07 de Marzo de 2007 :: LACNIC HACE LLAMADO A ASPIRANTES PARA HOSPEDAR SU REUNIÓN ANUAL DEL AÑO 20

65.17.241.153

Novedades y Anuncios

07 de Marzo de 2007 : :
LACNIC HACE LLAMADO A ASPIRANTES PARA HOSPEDAR SU REUNIÓN ANUAL DEL AÑO 2008

01 de Marzo de 2007 : :
Programa de Becas LACNIC X - Apertura de Solicitudes

04 de Enero de 2007 : :
Designación de Sede para WALC 2007 y 2008

02 de Enero de 2007 : :

GOING ONLINE FOR EXAMPLES

- LACNIC 72.37.160.24
- ARIN 205.149.192.0
- Samspade.org
- www.yahoo.com

$$ MONEY $$

- An IP Address equals Internet access; Internet access means SOMEBODY, SOMEWHERE IS PAYING FOR THE INTERNET ACCESS

- Subpoena the ISP for all customer and billing information, including ANI or physical location of the modem, for the target IP Address.
- You must include the date stamp for your target IP address in your subpoena.

$$ MORE MONEY $$

- Some ISPs record the MAC address (identification number of the modem card for the computer) during an Internet session

- This is good forensic evidence; give this information to your forensic examiner

- ISP may also provide telecommunications service for the customer

PHYSICAL LOCATION

IDENTIFY THE PHYSICAL LOCATION OF THE ANI OR DSL / MODEM LOCATION

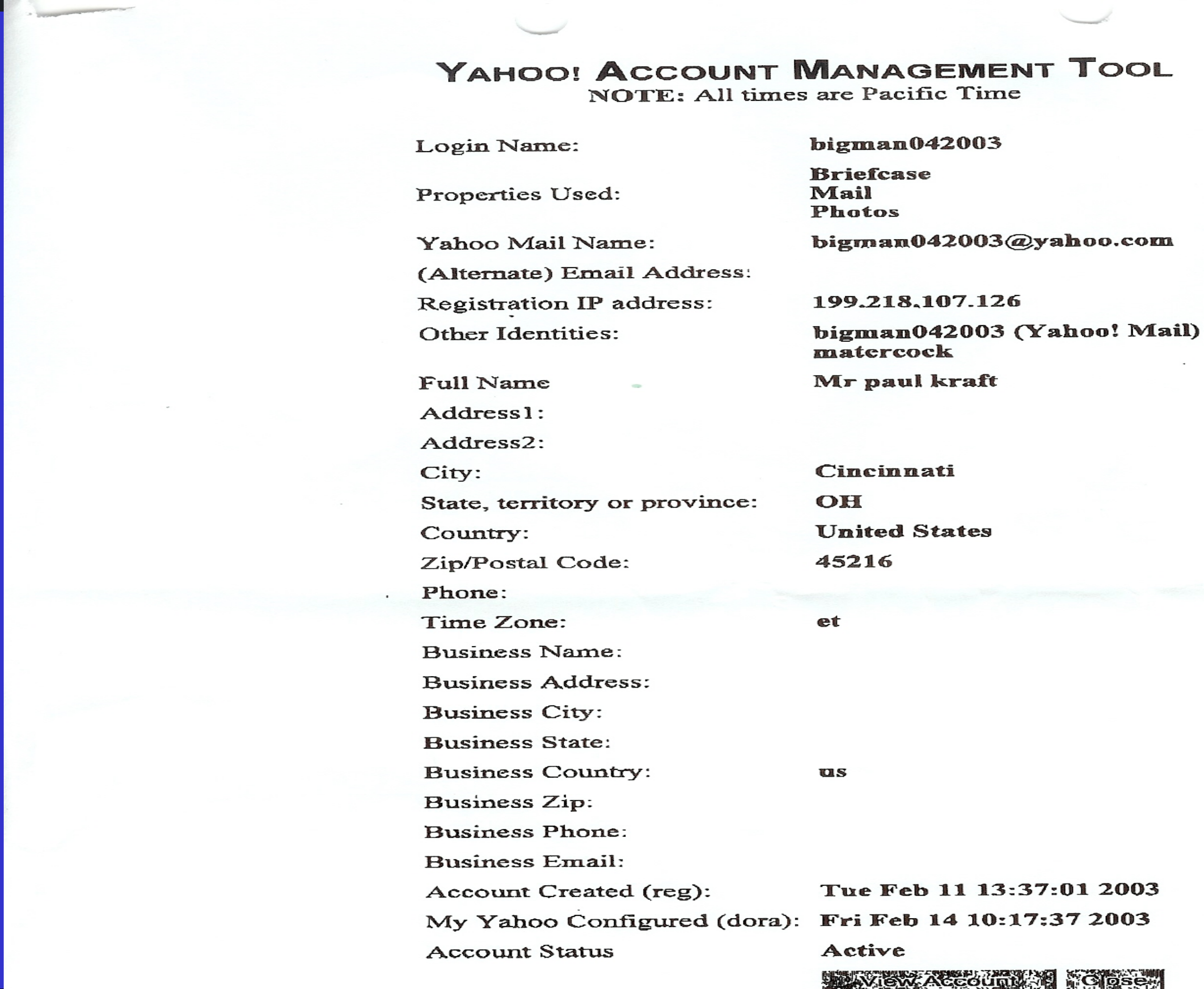
TRACKING WITHOUT AN IP ADDRESS

TRACKING BY USERNAME OR EMAIL ADDRESS

TRACKING EMAIL ADDRESS OR USERNAME

- Determine which IS has issued the email account or username
- Subpoena all customer information, but focus on IP log for registration, IP log for password change, and IP log for access to the account
- An alternate email address can also be used to track individual

YAHOO ACCOUNT MANAGEMENT TOOL

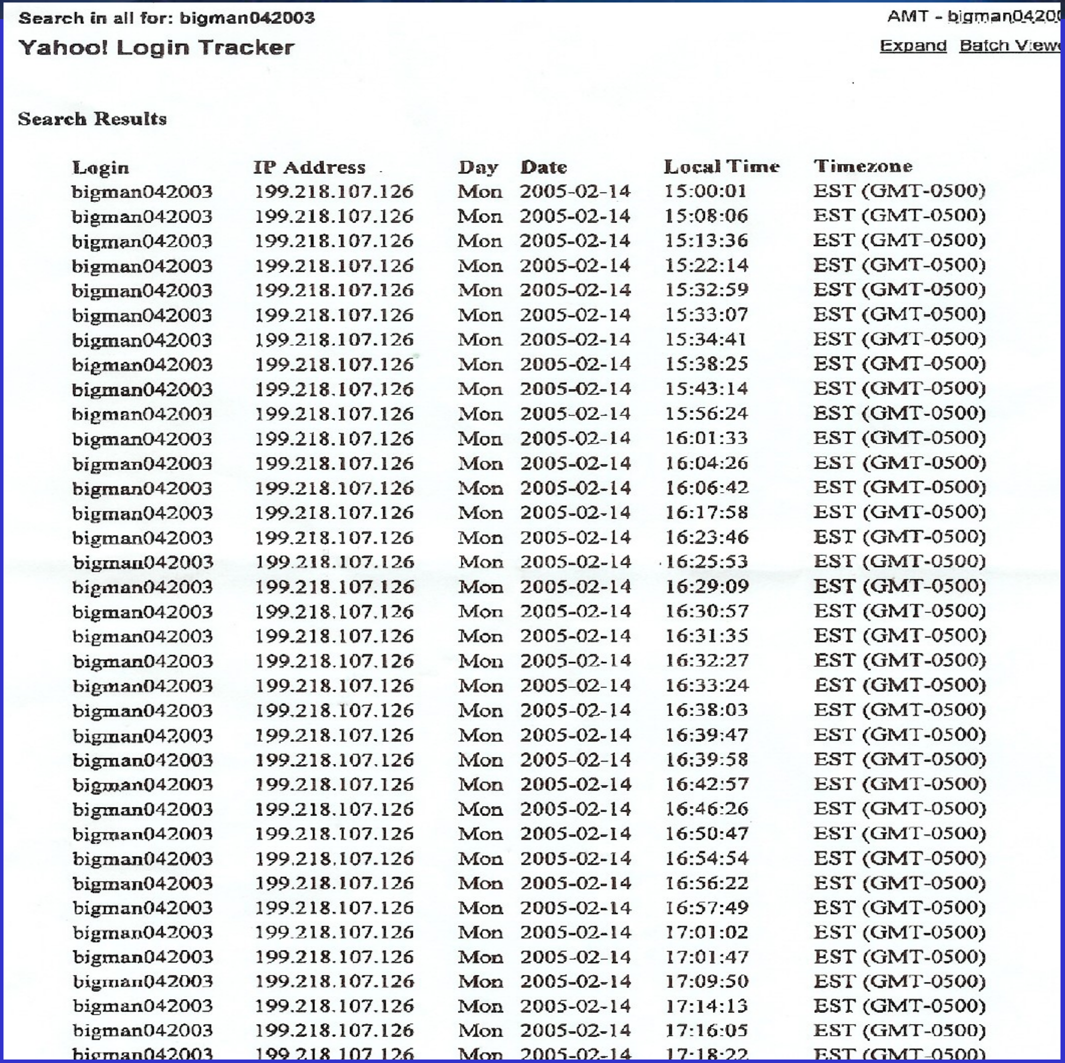


YAHOO! ACCOUNT MANAGEMENT TOOL

NOTE: All times are Pacific Time

Login Name:	bigman042003
Properties Used:	Briefcase Mail Photos
Yahoo Mail Name:	bigman042003@yahoo.com
(Alternate) Email Address:	
Registration IP address:	199.218.107.126
Other Identities:	bigman042003 (Yahoo! Mail) matercock
Full Name	Mr paul kraft
Address1:	
Address2:	
City:	Cincinnati
State, territory or province:	OH
Country:	United States
Zip/Postal Code:	45216
Phone:	
Time Zone:	et
Business Name:	
Business Address:	
Business City:	
Business State:	
Business Country:	us
Business Zip:	
Business Phone:	
Business Email:	
Account Created (reg):	Tue Feb 11 13:37:01 2003
My Yahoo Configured (dora):	Fri Feb 14 10:17:37 2003
Account Status	Active

IP LOG



Search in all for: bigman042003

AMT - bigman04200

Yahoo! Login Tracker

Expand Batch Viewe

Search Results

Login	IP Address	Day	Date	Local Time	Timezone
bigman042003	199.218.107.126	Mon	2005-02-14	15:00:01	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	15:08:06	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	15:13:36	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	15:22:14	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	15:32:59	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	15:33:07	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	15:34:41	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	15:38:25	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	15:43:14	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	15:56:24	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:01:33	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:04:26	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:06:42	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:17:58	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:23:46	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:25:53	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:29:09	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:30:57	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:31:35	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:32:27	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:33:24	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:38:03	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:39:47	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:39:58	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:42:57	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:46:26	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:50:47	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:54:54	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:56:22	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	16:57:49	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	17:01:02	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	17:01:47	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	17:09:50	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	17:14:13	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	17:16:05	EST (GMT-0500)
bigman042003	199.218.107.126	Mon	2005-02-14	17:18:22	EST (GMT-0500)

IMPORTANT FACTS

- Law Enforcement is better off having a suspect use Internet communication than a phone number, because pre-paid phones and other phone services have made conducting criminal activity almost untraceable.

- In most investigations, and especially in fugitive cases, the biggest problem is locating the suspect. An email address or Internet communication can be tracked to a PHYSICAL LOCATION.

IMPORTANT FACTS, continued

- When a criminal act has occurred using an email address, ANY COMPUTER accessing that email might contain potential evidence. These computers are subject to seizure and forensic examination.

Questions ???

Agent Sheila Gorriz
US Secret Service
Miami Field Office

Sheila.Gorriz@usss.dhs.gov