

# Email and Web Site Tracing

Jaqui Lynch

Mainline Information Systems

Email – [jaqui@circle4.com](mailto:jaqui@circle4.com)

HTCIA 6/28/05

<http://www.circle4.com/papers/htcia-email.pdf>

# Agenda

- IP Addresses and the Internic
- How is email delivered
- Obtaining Email Headers
- What are Email Headers?
- Understanding Reading Email Headers
- Tracing Email Headers
- Tracing Web URLs
- Reporting and ISP Information
- Final Warnings/Notes
- References
- Practical Examples

# CERT Statistics

• Year	1998	1999	2000	2001	2002	2003	2004
• Emails	41,871	34,612	56,365	118,907	204,841	542,754	717,863
• Calls	1,001	2,099	1280	1,417	880	934	795
• Vuln. Reports	262	419	1,090	2,437	4,129	3,784	3,780
• Incidents	3,734	9,859	21,756	52,658	82,094	137,529	
• Alerts Pub.	34	22	26	41	41	32	
• Security Notes	8	3	47	326	375	255	341

– Please note: Data taken from:

[http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)

# IP Addresses

- IPV4
  - 32 bit numbers listed as four octets
  - i.e. 198.041.000.052 written as 198.41.0.52
  - Classes
  - Domain
    - Hierarchy for name
    - i.e. system1.circle4.com
    - Domain is circle4.com
    - Hostname is system1
  - DNS (Domain Name server)
    - Maps IP addresses to names and vice versa
    - Connections are always done via IP address

# IP addresses and Classes

- Class A
  - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh
  - First bit 0; 7 network bits; 24 host bits
  - Initial byte: 0 - 127
  - 126 Class As exist (0 and 127 are reserved)
  - 16,777,214 hosts on each Class A
- Class B
  - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh
  - First two bits 10; 14 network bits; 16 host bits
  - Initial byte: 128 - 191
  - 16,384 Class Bs exist
  - 65,532 hosts on each Class B
- Class C
  - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh
  - First three bits 110; 21 network bits; 8 host bits
  - Initial byte: 192 - 223
  - 2,097,152 Class Cs exist
  - 254 hosts on each Class C
- Class D
  - 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm
  - First four bits 1110; 28 multicast address bits
  - Initial byte: 224 - 247
  - Class Ds are multicast addresses - see RFC 1112
- Class E
  - 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr
  - First four bits 1111; 28 reserved address bits
  - Initial byte: 248 - 255
  - Reserved for experimental use

# Reserved IP Addresses

- Class A
  - 0.0.0.0 to 0.255.255.255
  - 10.0.0.0 to 10.255.255.255 IANA
  - 127.0.0.0 to 127.255.255.255 Loopback
- Class B
  - 172.16.0.0 to 172.31.255.255 IANA
- Class C
  - 192.168.0.0 to 192.168.255.255 IANA
  - 192.0.2.0 to 192.0.2.255 Test Nets
- Class D
  - 224.0.0.0 to 239.255.255.255 Multicast
- Class E
  - 240.0.0.0 to 255.255.255.255 Multicast or Reserved
- Other
  - 169.254.0.0 to 169.254.255.255 IPV4 autoDHCP
- Bogus Addresses:
  - <http://www.cymru.com/Documents/bogon-list.html>
  - <http://www.faqs.org/qa/rfc618.html>

# IANA Reserved Addresses

- 192.168.0.0 – 192.168.255.255
- 172.16.0.0 – 172.31.255.255
- 10.0.0.0 – 10.255.255.255
- The above are non-routeable addresses that are reserved for internal use i.e. home or private networks
- If an address comes back to IANA it is forged so look at the next one
- 127.0.0.1 is the loopback port

# NICs



**whois.ripe.net**

**whois.arin.net**

**whois.apnic.net**

**whois.lacnic.net**

**whois.geektools.com**

**whois.nic.or.kr**

**From <http://www.apnic.net/info/faq/abuse/index.html>**

# How is Email Delivered

- MUA (mail user agent)
  - Client such as Outlook, Notes, Pegasus
- MTA (mail Transport Agent)
  - Server such as sendmail, MS Exchange, Postfix
- MUA passes message to MTA
- MTA does the following:
  - Logs the connection
  - Looks at envelope data and figures out path
  - If local (same server) it delivers it to the mailbox
  - Connects to receiving MTA and hands over message
  - MTAs may relay messages through other MTAs
- Causes of Multiple Hops
  - Firewalls, relaying

# Envelope Data

- Sender
  - Also called reverse path in RFC831
  - From: jaqui@circle4.com
- Recipient
  - Also called forward path in RFC 831
  - To: joe@smith.com
- Envelope Headers are derived from SMTP RCPT TO: and MAIL FROM: and can be forged
- Message Headers (Received From: ) can also be forged

# SMTP Protocol

- telnet mailserver1 25
- HELO mail.jaqui.com
  - This is me telling it my server name – a good server will pick up that I am lying and would record it as follows:
    - 250 mailserver1 Hello mail.jaqui.com [123.123.123.123], pleased to meet you
    - Note the server put my real IP address in [ ]
- MAIL FROM: jaqui@circle4.com
- RCPT TO: persontobug@smith.com
- DATA
- Type all the data in here and then end with a “.” on a line by itself
- QUIT

# SMTP Info

**HELO** identifies the sending machine; "HELO mail.bieberdorf.edu" should be read as "Hello, I'm mail.bieberdorf.edu". The sender can lie; nothing, in principle, prevents mail.bieberdorf.edu from saying "Hello, I'm frobozz.xyzzzy.gov" (HELO frobozz.xyzzzy.gov) or even "Hello, I'm a misconfigured computer" (HELO a misconfigured computer). However, in most circumstances, the receiver has some tools with which to discover this and find out the sending machine's real identity.

**MAIL FROM** initiates mail processing; it means "I have mail to deliver from so-and-so". The address given turns into the so-called "envelope From" (see Section Whatever); it need not be the same as the sender's own address! This apparent security hole is inevitable (after all, the receiving machine doesn't know anything about who has what username on the sending machine), and in certain circumstances it turns out to be a useful feature.

**RCPT TO** is dual to MAIL FROM; it specifies the intended recipient of the mail. One piece of mail can be sent to multiple recipients simply by including multiple RCPT TO commands (see the section on mail relaying, which explains how this feature is sometimes abused on insecure systems). The given address turns into the so-called "envelope To" (see Section Whatever); it actually determines who the mail will be delivered to, regardless of what the To: line in the message says.

**DATA** starts the actual mail entry. Everything entered after a DATA command is considered part of the message; there are no restrictions on its form. Lines at the beginning of the message (before the first blank line) that start with a single word and a colon are considered to be headers by most mail programs. A line consisting only of a period terminates the message.

**QUIT** terminates the connection.

SMTP is fully defined in RFC 821. Copies of the RFCs are widely available on the Web; this one is well worth reading, as it sheds much light on the intricacies of mail processing.

From <http://www.stopspam.org/email/headers.html>

# Email Log on MTA

## Sample Email Server Log Entry

Jun 23 15:37:46 www sendmail[4400]: j5NJbkcn004400: from=<jaqui@cmg.org>, size=0, class=0, nrcpts=3, proto=SMTP, daemon=MTA, relay=pcp08983787pcs.trnrsv01.nj.comcast.net [68.46.28.238]

Jun 23 15:37:48 www sendmail[4400]: j5NJbkcp004400: from=<jaqui@cmg.org>, size=69891, class=0, nrcpts=3, msgid=<008201c5782b\$0c76b440\$0200a8c0@JAQUILAPTOP>, proto=SMTP, daemon=MTA, relay=pcp08983787pcs.trnrsv01.nj.comcast.net [68.46.28.238]

# Obtaining Email Headers

- Instructions for most clients are at:
  - <http://www.spamcop.net/fom-serve/cache/19.html>
  - <http://www.haltabuse.org/help/headers/index.shtml>
  - [http://www.wiredkids.org/teens/personal\\_information\\_safety/email\\_safety/getheaders.html](http://www.wiredkids.org/teens/personal_information_safety/email_safety/getheaders.html)
- i.e. Netscape v7 mail
  - Click on view and then message source
- Info on Email Headers in general:
  - <http://www.stopspam.org/email/headers.html>
  - <http://tgos.org/newbie/xheader.html>
- Without these headers you have nothing

# Understanding Email Headers

- Standard Header:
  - Subject: test email
  - From: jaqui@circle4.com
  - Reply\_To: jaqui@circle4.com
  - Date: 08/08/2002 11.50am
  - To: jaqui@circle4.com
- All of the above can be faked and should be ignored for now

# Header Parameters

- Apparently-To:
- Bcc:
- Cc:
- Comments:
- Content-Transfer-Encoding:
- Content-Type:
- Date:
- Errors-To:
- From
- From:
- Message-Id:
- In-Reply-To:
- Newsgroups:
- Organization:
- Priority:
- Received:
- References:
- Reply-To:
- Sender:
- Subject:
- To:

# X-Headers

- X-Confirm-Reading-To:
- X-Distribution:
- X-Errors-To:
- X-Mailer:
- X-PMFLAGS:
- X-Priority:
- X-Sender:
- X-UIDL:

# Key Components to Review

- **Message-Id:** (also Message-id: or Message-ID:) The Message-Id is a more-or-less unique identifier assigned to each message, usually by the first mailserver it encounters. Conventionally, it is of the form "gibberish@bieberdorf.edu", where the "gibberish" part could be absolutely anything and the second part is the name of the machine that assigned the ID. Sometimes, but not often, the "gibberish" includes the sender's username. Any email in which the message ID is malformed (e.g., an empty string or no @ sign), or in which the site in the message ID isn't the real site of origin, is probably a forgery.
- i.e. 35BA4388F7518544922C06DD461062E23F768B@pa7-j.abc.com
- Can sometimes be used to tie this email to the correct Received From
- Can be faked
  - FROM <http://www.stopspam.org/email/headers.html>

# More key Components

- From: and To:
  - Ignore for now – these are usually forged, often by viruses or worms as well as spammers
- Received:
  - This is where the information you really need is
  - These can be forged
  - Once the header leaves the client the sender has no control over the future headers. Since headers are built bottom up it is normally the bottom ones that are faked.
- Date:
  - The date/time on either the computer sending the message or the mailserver
  - These are regularly not set correctly

# Received From:

- Includes:
- Name and ip of machine handing off the email
- Name and/or ip of machine receiving the email
- Mail version and unique identifier for receiving system for this piece of mail
- Date and time this happened
- Received: from circle4.com (d47-69-226-132.nap.wideopenwest.com [69.47.132.226]) by cmg.org (8.12.10/8.11.4) with ESMTP id i1IExB59000710; Wed, 18 Feb 2004 09:59:12 -0500 (EST)

# Notes

- Date: Thu, 08 Aug 2002 11:53:02 -0400
  - From: "Jaqui Lynch" <jaqui@circle4.com>
  - To: jaqui@circle4.com
  - Subject: Test email
  - Sender: "927222556,06/10/01,RDP5," <jaqui@zeus.jersey.net>
- 
- **Relationship between domain in From:**
    - From: "Jaqui Lynch" <jaqui@circle4.com>
  - **and IP in Received from:**
    - Received: from circle4.com (d47-69-226-132.nap.wideopenwest.com [69.47.132.226]) by cmg.org

# Full Headers

- Received: (qmail 73307 invoked from network); 18 Feb 2004 15:18:56 -0000
- Received: from cmg.org (209.66.0.64) by chanas.pair.com with SMTP; 18 Feb 2004 15:18:56 -0000
- Received: from circle4.com (d47-69-226-132.nap.wideopenwest.com [69.47.132.226]) by cmg.org (8.12.10/8.11.4) with ESMTP id i1IExB59000710; Wed, 18 Feb 2004 09:59:12 -0500 (EST)
- Message-ID: 4033825B.5040405@circle4.com
- Date: Wed, 18 Feb 2004 09:18:51 -0600
- From: Jaqui Lynch <jaqui@circle4.com>

# So where did that email come from?

- Received: from circle4.com (d47-69-226-132.nap.wideopenwest.com [69.47.132.226]) by cmg.org (8.12.10/8.11.4) with ESMTP id i1IExB59000710; Wed, 18 Feb 2004 09:59:12 -0500 (EST)
- Message-ID: 4033825B.5040405@circle4.com
- IP ADDRESS is:
- 69.47.132.226

# DNS Info

02/18/04 17:50:50 dns 69.47.132.226

nslookup 69.47.132.226

Canonical name:

d47-69-226-132.nap.wideopenwest.com

Addresses:

69.47.132.226

# IPBlock Info

02/18/04 17:53:54 IP block 69.47.128.0@whois.geektools.com

Trying 69.47.128.0 at ARIN

Trying 69.47.128 at ARIN

WideOpenWest LLC WIDEOPENWEST (NET-69-47-0-0-1)

69.47.0.0 - 69.47.191.255

WIDEOPENWEST ILL WOW-ILL-6-128 (NET-69-47-128-0-1)

69.47.128.0 - 69.47.159.255

# ARIN WHOIS database, last updated 2004-02-17 19:15

# Enter ? for additional hints on searching ARIN's WHOIS database.

**Drill down on NET-69-47-128-0-1**

# Whois Info 1/3

- 02/18/04 17:54:01 whois !NET-69-47-128-0-1@whois.arin.net
- whois -h whois.arin.net !net-69-47-128-0-1 ...
- CustName: WIDEOPENWEST ILL
- Address: 1674 FRONTENAC RD
- City: NAPERVILLE
- StateProv: IL
- PostalCode: 60563
- Country: US
- RegDate: 2004-02-12
- Updated: 2004-02-12

# Whois Info 2/3

NetRange: 69.47.128.0 - 69.47.159.255  
CIDR: 69.47.128.0/19  
NetName: WOW-ILL-6-128  
NetHandle: NET-69-47-128-0-1  
Parent: NET-69-47-0-0-1  
NetType: Reassigned  
Comment:  
RegDate: 2004-02-12  
Updated: 2004-02-12  
TechHandle: LW463-ARIN  
TechName: WALDEN, LAWRENCE D  
TechPhone: +1-630-536-3161  
TechEmail: dwalden@wideopenwest.com

# Whois Info 3/3

OrgAbuseHandle: ABUSE241-ARIN

OrgAbuseName: Abuse Department

OrgAbusePhone: +1-800-496-9669

OrgAbuseEmail: abuse@wideopenwest.com

OrgNOCHandle: NMC5-ARIN

OrgNOCName: Network Management Center

OrgNOCPhone: +1-800-496-9669

OrgNOCEmail: nmc@wideopenwest.com

# So who was I?

- A Wideopenwest user (IP 69.47.132.226)
- My email domain is circle4.com
- In this case I sent an email from myself to myself
- The email was relayed through an smtp server called cmg.org
- cmg.org passed the email to the final destination which was pair.com – so circle4.com is hosted at pair.com most likely so we do a dns lookup on circle4.com to check .....

# DNS Lookup on circle4.com

03/05/04 21:59:26 dns circle4.com

Mail for circle4.com is handled by chanas.pair.com

Canonical name: circle4.com

Addresses:

216.92.103.54

You could then go on to do an ipblock and a whois to confirm that pair is the ISP

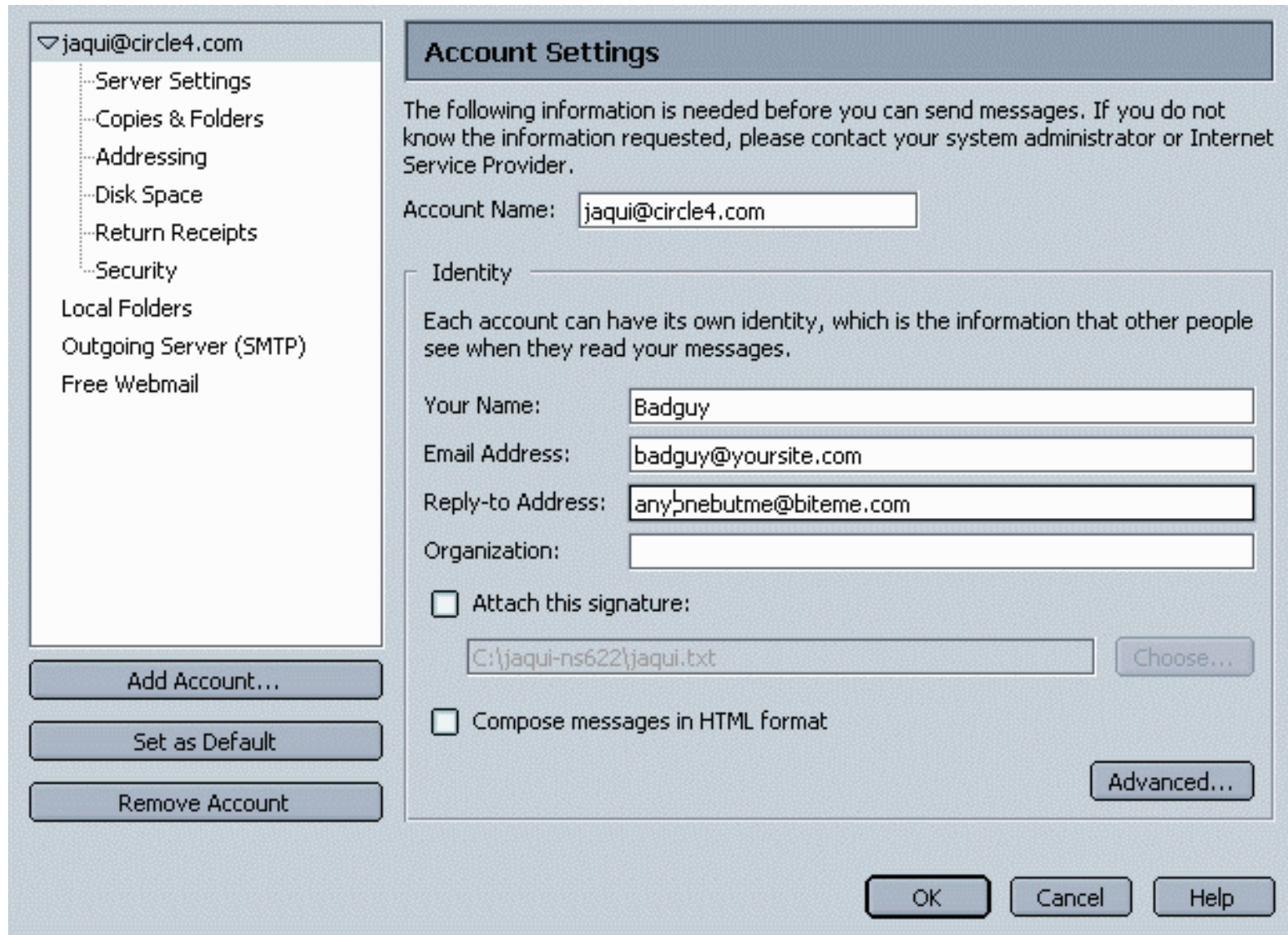
# Tips for reading email headers

- Start with the bottom Received from:
- Is it valid? Does it match the Message-Id line?
- Move up to the next one and keep doing so till you have a valid one
- I actually check every ip for whois and ip block – be persistent
- Often the From: is faked so I tend to ignore it
- Also follow the trail for the received froms – make sure they link to each other

# Forged Headers

- These occur when the connecting person tries to fake out who they are – a correctly configured mail server will pick this up and you will see something like:
- Received from: jaqui.org (circle4.com [69.47.132.226]) by mailserver.com
- Where I said I was jaqui.org the mail server checked my ip and found I was really circle4.com
- Sometimes they also add totally fake headers to try and confuse you so you may see multiple lines
- Also look for numbers in the ip address that are >255
- Watch for reserved addresses such as 10.\* or 192.\*

# How hard is it to fake the from and to?



# Steps to Trace an email

1. Analyze email headers to get the correct IP
2. Trace every ip from bottom to top and figure out the trail
3. DNS lookup – check for name if any
4. Set Sam Spade to use Geekttools initially
5. Ipblock with Sam Spade
6. Whois with Sam Spade
7. If the IP comes back to a legitimate ISP then go to their website to find their abuse email address
8. If it's a web site use Sam Spade to look at the website and if it looks safe then go there yourself – use view source to check the page source and see if there is anything useful there
9. Use [www.deja.com](http://www.deja.com) and google to search on the domain and/or email for info

# Interesting Headers

**Received: from mail.reallyfakedomain.com ([216.126.35.59])  
by mc5-f40.law1.hotmail.com with  
Microsoft SMTPSVC(5.0.2195.5600);  
Tue, 25 Feb 2003 05:25:30 -0800**

**Received: from vader (vader.pkint [192.168.0.2])by  
mail.reallyfakedomain.com (Postfix) with SMTP  
id E15751242AA7for <\*\*\*\*\*@hotmail.com>;  
Tue, 25 Feb 2003 05:36:35 -0700 (MST)**

**Received: by firewall(10.0.0.2)id 39999774.4453762;  
Nortel SMTP Gateway 3.2**

**X-Message-Info: dHZMQeBBv44IPE7o4B5bAg==**

**Message-Id: <20030225123635.E15751242AA7@mail.reallyfakedomain.com>**

**Return-Path: root@eroticmailers.com**

**X-OriginalArrivalTime: 25 Feb 2003 13:25:31.0075 (UTC)**

**FILETIME=[5E744930:01C2DCD1]**

**216.126.35.59 is really somewhere in broadriver.com**

# Interesting Headers

Received: (qmail 92224 invoked from network); 23 Jun 2005 19:34:38 -0000

Received: from sfmtx02.bankofamerica.com (HELO sfdmzmailmx02.bankofamerica.com) (171.159.64.79) by chanas.pair.com with SMTP; 23 Jun 2005 19:34:38 -0000

Received: from sfdmzmailmx03.bankofamerica.com ([171.182.72.79]) by sfdmzmailmx02.bankofamerica.com (8.12.11/8.12.11) with ESMTP id j5NJYOhD013653; Thu, 23 Jun 2005 19:34:28 GMT

Received: from memscmpl3. (casfodc07s889.bankofamerica.com [165.48.14.226]) by sfdmzmailmx03.bankofamerica.com (8.12.11/8.12.11) with SMTP id j5NJYCAG025527; Thu, 23 Jun 2005 19:34:24 GMT

Received: from memmta0201 (171.186.107.201) by memscmpl3. (Sigaba Gateway v3.6.1) with ESMTP id 197524549; Thu, 23 Jun 2005 12:34:24 -0700

Message-id:

<9BF1F3AB48FDC543BAAEA8B2D8122A8F04977293@ex2k.bankofamerica.com>

Above are all valid Bank IP addresses

# Steps to Trace a web site

1. Analyze Web URL to get the correct IP
2. For a website use the domain not the URL
  1. I.e. circle4.com not www.circle4.com
  2. Go back and check the URL later
3. Trace every ip from bottom to top and figure out the trail
4. DNS lookup – check for name if any
5. Set Sam Spade to use Geekttools initially
6. Ipblock with Sam Spade
7. Whois with Sam Spade
8. If the IP comes back to a legitimate ISP then go to their website to find their abuse email address
9. If it's a web site use Sam Spade to look at the website and if it looks safe then go there yourself – use view source to check the page source and see if there is anything useful there
10. Use www.deja.com and google to search on the domain and/or email for info

# www.circle4.com

DNS on circle4.com

06/23/05 18:52:02 dns circle4.com

Mail for circle4.com is handled by chanas.pair.com

Canonical name: circle4.com

Addresses:

216.92.103.54

DNS on www.circle4.com

06/23/05 18:52:51 dns www.circle4.com

Mail for www.circle4.com is handled by chanas.pair.com

Canonical name: circle4.com

Aliases:

www.circle4.com

Addresses:

216.92.103.54

In this case both the domain and url match for IP  
It is ok if they do not – trace both IPs then

# 216.92.103.54 IPBlock & Whois

06/23/05 18:54:20 IP block  
216.92.103.54@whois.geektools.com  
Trying 216.92.103.54 at ARIN  
Trying 216.92.103 at ARIN

OrgName: pair Networks  
OrgID: PAIR  
Address: 2403 Sidney St  
Address: Suite 510  
City: Pittsburgh  
StateProv: PA  
PostalCode: 15232  
Country: US

NetRange: 216.92.0.0 - 216.92.255.255  
CIDR: 216.92.0.0/16  
NetName: PAIRNET-BLK-3  
NetHandle: NET-216-92-0-0-1  
Parent: NET-216-0-0-0-0  
NetType: Direct Allocation  
NameServer: NS1.PAIR.COM  
NameServer: NS0.NS0.COM  
Comment: ADDRESSES WITHIN THIS BLOCK ARE  
NON-PORTABLE  
RegDate: 1998-09-25  
Updated: 2001-06-14

TechHandle: KM383-ARIN  
TechName: Martin, Kevin J.  
TechPhone: +1-412-381-7247  
TechEmail: sigma@pair.com

OrgAbuseHandle: ABUSE848-ARIN  
OrgAbuseName: Abuse Handling  
OrgAbusePhone: +1-412-381-7247  
OrgAbuseEmail: abuse@pair.com

OrgTechHandle: KM383-ARIN  
OrgTechName: Martin, Kevin J.  
OrgTechPhone: +1-412-381-7247  
OrgTechEmail: sigma@pair.com

# ARIN WHOIS database, last updated 2005-06-22 19:10  
# Enter ? for additional hints on searching ARIN's WHOIS  
database.

WHOIS shows the same (both at geektools)  
IPBlock on domain name also shows this

# Circle4.com Whois

Registrant:

Lynch, Jaqui

Circle4 Computer Consultants

5700 College Road

Lisle, IL 60532

US

Moral of the story!

Also do a whois on the domain name

Domain Name: CIRCLE4.COM

Administrative Contact, Technical Contact:

Lynch, Jaqui

jaqui@CIRCLE4.COM

Circle4 Computer Consultants

BK331

5700 College Road

Lisle, IL 60532

US

630-886-4440 fax: 253-736-9389

Record expires on 01-Aug-2008.

Record created on 02-Aug-1997.

Bulk whois optout: N

Database last updated on 23-Jun-2005 19:56:38 EDT.

Domain servers in listed order:

NS321.PAIR.COM

NS0000.NS0.COM           216.92.61.2

# Web Page

The screenshot shows a web browser window displaying the homepage of the Computer Measurement Group (CMG). The browser's address bar shows the URL <http://www.cmg.org/>. The website features a dark blue header with the CMG logo and navigation links: [International Conference](#), [Measure IT](#), [CMG Groups](#), [CMG National](#), [Members Only](#), [Links](#), and [Site Map](#). A vertical sidebar on the left contains a list of links: [CMG 2005](#), [Conference Admin](#), [National](#), [Past Conferences](#), [Groups](#), [About CMG](#), [Membership Info](#), [Publications](#), [Calendar of Events](#), [Members Only](#), [Links](#), and [Site Map](#). The main content area includes the CMG logo and tagline, "The Association of System Performance Professionals", followed by a paragraph describing the group's mission. Below this is a link to the [webmaster](#) and a footer with the date "Last Updated 05/12/05", copyright information "© 1995-2005 Computer Measurement Group, Inc.", and a link to the [Full copyright notice and disclaimer](#). On the right side, there are three light blue boxes: the top one promotes the [Subscribe to CMG's MeasureIT Newsletter!](#), the middle one contains links for [CMG2005 Registration Options](#) and [CMG Membership Information](#), and the bottom one features a search bar with the text "Search CMG's library of technical papers!" and a "Search!" button. At the bottom of the page, there is a navigation bar with links: [Home](#) | [Conference](#) | [Groups](#) | [National](#) | [Members](#) | [Links](#) | [Site Map](#), and a footer with the text "Computer Measurement Group". The browser's status bar at the bottom shows the URL <http://www.cmg.org/index.html> and the "Internet" icon.

# Source

```
<!--
Rob Harrigan, February 25th 2003:
The top logo and navigation graphics are in their own table row and the white graphic with the small
left blue stripe
is used as the repeating background. The only absolutely defined column width is the column containing
the
CMG logo and left navigation. Everything to the right should wrap with the screen size.

* This is the new template for all pages.
** It will speed up load times, because the huge background gif's are not used.
***Be sure to change the following:
1. Title
2. Menu number in toggleMenu statement (see Body onLoad tag)
3. Include correct content file
4. Save this file with correct name (i.e. without _content)
-->
<HTML>
<HEAD>
<TITLE>Computer Measurement Group</TITLE>
<META NAME="description" CONTENT="worldwide non-profit organization that focuses on computer
performance evaluation and capacity management">
<META NAME="keywords" CONTENT="performance management, capacity planning, service level management,
modeling, accounting chargeback, software performance engineering, architectural technology
description, management, system software, operating systems, servers, network, internet,
infrastructure, storage systems, data store, databases, warehouses, data design, application
development, slm, sla, spe, architecture, paging, udb, z/os, management, performance, reporting, unix,
vsam, web, dasd, disk, san, sar, smf, open systems, os/390, response time, simulation, swapping,
storage, cpu, ecommerce, java, i/o, windows, workload, wlm, rmf, planning">
<META HTTP-EQUIV="CACHE-CONTROL" CONTENT="NO-CACHE">
<SCRIPT LANGUAGE="JavaScript"><!--
//script for navigation bar rollover
if (document.images)
    {
        img1nb = new Image();
        img1nb.src = "/pics/logo_home_b.gif";

        img2nb = new Image();
        img2nb.src = "/pics/top_conference.gif";

        img3nb = new Image();
        img3nb.src = "/pics/top_groups.gif";

        img4nb = new Image();
        img4nb.src = "/pics/top_national.gif";

        img5nb = new Image();
        img5nb.src = "/pics/top_members.gif";

        img6nb = new Image();
        img6nb.src = "/pics/top_links.gif";

        img7nb = new Image();
        img7nb.src = "/pics/top_sitemap.gif";

        img8nb = new Image();
        img8nb.src = "/pics/top_measure.gif";

    }
function img_nbon(imgName)
{
    if (document.images)
    {
```

Sometimes info such as name or number is in the comments

# Strange Web Links

- <http://1%30%38%35%338%31%32%39%32/>
  - These are %-encoded characters
  - Decoded this reads <http://1085381292/> - a decimal number
  - This is another way of writing 64.177.154.172
  - To convert the decimal number to a proper IP address go to:
    - <http://www.samspade.org> – type it in and click on do stuff

# Reporting and ISP Information

- Most ISPs have an email address of:
- Abuse@domain or postmaster@domain
- i.e. abuse@attbi.com
- It still pays to check on their web site though
- Other Useful Addresses:
- [http://add.yahoo.com/fast/help/us/clubs/cgi\\_abuse](http://add.yahoo.com/fast/help/us/clubs/cgi_abuse)
- <http://help.yahoo.com/help/us/mb/abuse/abuse-06.html>  
(subpoenas)
- <http://abuse.yahoo.com>
- <http://www.forensicsweb.com/downloads/cfid/isplist/isplist.htm> (how to contact ISPs legal departments)
- <http://mailabuse.org/rbl/notifyfaq.html>
- **Preservation Letters**
- **Ask them not to inform the person being investigated**

# Incident Reporting

- Gathering Evidence
  - Know the legal issues
- Who to contact and how
- abuse@ your site or the attack site
- FBI
- Local Computer Crime bureau
- Police
- Have an Emergency Response Team with a clear set of policies and procedures

# Gathering Evidence

- CHAIN OF CUSTODY
- Copies of all logs (signed and dated)
- Output from last and lastcomm commands
- Output from ls -al and other commands
- Output from lsof
- If email - copy of raw headers for the messages
- Username, phone number, etc
- Email address including mail node
  - See next slide

# References

- Internet Fraud
  - <http://www1.ifccfbi.gov/index.asp>
- Obtaining and understanding email headers
  - <http://www.spamcop.net/fom-serve/cache/19.html>
  - <http://www.haltabuse.org/help/header.shtml>
  - <http://www.stopspam.org/email/headers.html>

# Tracing sites

- <http://www.sampade.org/>
- <http://www.sampade.org/ssw>  
Click on downloads and it takes you to:  
<http://static.sampade.org/ssw/spade114.exe>
- <http://combat.uxn.com/>
- <http://www.network-tools.com/>
- <http://www.geektools.com/>
- <http://www1.dshield.org/ipinfo.php>
- <http://www.traceroute.org/>
- <http://www.networksolutions.com/cgi-bin/whois/whois>
- <http://www.ripe.net/perl/whois> Europe
- <http://www.apnic.net/apnic-bin/whois.pl> AP and Asia
- <http://whois.nic.or.kr/> Korea
- <http://www.arin.net/> N. & S. America
- <http://www.alldomains.com/alltlds.html> Domain extensions

# Configuring Sam Spade for Windows

1. Download, scan and install the program
2. Bring up Sam Spade
3. Edit, options, basics
  - Do NOT check the dhcp box
  - Code the dns server (nameserver) ip into the nameserver box
  - Let max simultaneous connections default to 100
  - Put a yahoo email address (or similar) into the email address
4. Advanced
  - Select enable relay checking
  - Do not select zone transfers or active probing
5. Mail
6. Put something generic for your name and email addresses

# Using Sam Spade for Windows

## 1. Down left side

DNS

WHOIS

IPBLOCK

DIG

TRACERBL

ABUSE

## • 2. Across the Top

- Select Tools and then:

- SMTP relay check
- Crawl Website
- Browse Website
- Parse Email Headers

Questions???



# Headers to Try

# Header #1

Received: from mc2-f22.law16.hotmail.com ([65.54.237.29]) by mc2-s2.law16.hotmail.com with Microsoft SMTPSVC(5.0.2195.4905); Tue, 30 Jul 2002 11:54:01 -0700  
Received: from siet.inet.edu.ar ([168.83.21.35]) by mc2-f22.law16.hotmail.com with Microsoft SMTPSVC(5.0.2195.4905); Tue, 30 Jul 2002 11:48:58 -0700  
Received: from [24.197.150.239] by siet.inet.edu.ar (Netscape Messaging Server 3.5) with SMTP id 333; Tue, 30 Jul 2002 15:38:08 -0300  
From: sabrina7475536@yahoo.com  
To: abc@hotmail.com,  
Date: Tue, 30 Jul 2002 14:42:20 -0400  
Subject: Hello an\_blue 100% FREE TEENS!  
MIME-Version: 1.0  
X-Mailer: Microsoft Outlook Express 6.00.2600.0000  
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000  
X-Precedence-Ref: 12  
Content-Type: text/html; charset=us-ascii  
Content-Transfer-Encoding: 7bit  
Message-ID: <20020730183639484.AAE302.333@[24.197.150.239]>  
Return-Path: sabrina7475536@yahoo.com  
X-OriginalArrivalTime: 30 Jul 2002 18:49:00.0594 (UTC) FILETIME=[C4AE5920:01C237F9]

# Answer #1

**1. Correct IP is 24.197.150.239**

**DNS is 24-197-150-239.charterga.net**

**IP Block shows the ISP is Charter Communications, 12405 Powerscourt**

**St. Louis, MO**

**For abuse try abuse@charterga.net but also the parent company at abuse@charter.net.**

**They also have a web form for reporting abuse at:**

**<http://abuse.charter.net/>**

**If from is correct then Mail-abuse@yahoo-inc.com, postmaster@yahoo.com,  
abuse@yahoo.com**

# Header #2

From ytUI9Iea@yahoo.com Tue, 30 Jul 2002 12:50:38 -0700  
Received: from [211.185.156.157] by hotmail.com (3.2) with ESMTP id  
MHotMailBF1037FF008E4136E820D3B99C9D0AAC49; Tue, 30 Jul 2002 12:49:04 -0700  
Received: from 175.247.114.183 ([175.247.114.183]) by m13.grp.snv.yahui.com with  
QMQP; Tue, 30 Jul 2002 04:01:02 -0000  
Message-ID: <Vyppq753NYU\$7DWsiiUU\$PFMyp1BK@bfD9Lf5g>  
From: "NORAH" <ytUI9Iea@yahoo.com>  
To: <abc@hotmail.com>  
Subject: Welcome To AdultClub. [Member: an\_ion]  
Date: Tue, 30 Jul 2002 12:53:50 -0580  
Content-Type: text/html; charset=us-ascii  
Content-Transfer-Encoding: 7bit  
X-Mailer: The Bat! (v1.52f) Business  
]

# Answer #2

**2. Correct IP is 211.185.156.157**

**DNS is nonexistent**

**Whois shows YONGDONG ELEMENTARY SCHOOL in Korea**

**For abuse try abuse@cnoe.or.kr and abuse@pubnet.ne.kr**

**If from is correct then Mail-abuse@yahoo-inc.com, postmaster@yahoo.com,  
abuse@yahoo.com**

**175.247.114.183 comes back as IANA which means  
it has not been assigned**

# Header #3

From ootxzzixxz@msn.com Wed, 10 Jul 2002 05:08:28 -0700  
Received: from [211.62.172.8] by hotmail.com (3.2) with ESMTP id  
MHotMailBEF56E2B006A40043158D33EAC0811441; Wed, 10 Jul 2002 05:06:35 -0700  
Received: from taco.rotis.com.tw ([203.39.24.194])  
by ns.sewon-ecs.co.kr (8.9.3/8.9.3) with SMTP id WAA13915;  
Wed, 10 Jul 2002 22:02:23 +0900  
Message-ID: <0000211d1090\$00000195\$00002f9c@taco.rotis.com.tw>  
To: <baby@ns.sewon-ecs.co.kr>  
From: "HOT SEX" <ootxzzixxz@msn.com>  
Subject: -->> Jennifer Lopez Orgy! 15797  
Date: Wed, 10 Jul 2002 08:05:25 -1900  
MIME-Version: 1.0  
Content-Type: text/html;  
charset="iso-8859-1"  
Content-Transfer-Encoding: quoted-printable  
X-mailer: Microsoft Outlook Express 5.00.2717.6778

]

# Answer #3

**3. IP is 203.39.24.194**

**No dns name**

**ISP and company are both Telstra**

**abuse@telstra.net**

**If from is valid you could try abuse@msn.com**

**211.62.172.8 is ns.sewon-ecs.co.kr so the flow is there**

**You can do an nslookup on the name to check this if the ip fails a lookup**

# Header #4

Received: from 209.149.145.250 ([209.16.245.179]) by mc2-f24.law16.hotmail.com with Microsoft SMTPSVC(5.0.2195.4905); Thu, 4 Jul 2002 04:01:37 -0700  
Received: from unknown (149.89.93.47) by rly-xr02.mx.aol.com with NNFMP; Jul, 04 2002 7:01:23 AM +1200  
Received: from 87.15.78.89 ([87.15.78.89]) by pet.vosn.net with local; Jul, 04 2002 5:54:19 AM +0600  
Received: from [118.189.136.119] by smtp-server1.cfl.rr.com with NNFMP; Jul, 04 2002 4:42:28 AM +0300  
From: druWendy <umhqtez@slo.net>  
To: Marisa  
Subject: FREE STREAMING PORNSTAR MOVIES!!! lind  
Sender: druWendy <umhqtez@slo.net>  
Mime-Version: 1.0  
Content-Type: text/html; charset="iso-8859-1"  
Date: Thu, 4 Jul 2002 07:01:34 -0400  
X-Mailer: Microsoft Outlook Express 5.00.2615.200  
Return-Path: umhqtez@slo.net  
Message-ID: <MC2-F24V7nUQtoWhFvs0014147e@mc2-f24.law16.hotmail.com>  
X-OriginalArrivalTime: 04 Jul 2002 11:01:37.0898 (UTC) FILETIME=[2B3104A0:01C2234A]

# Answer #4

**4. IP is 209.16.245.179**

**DNS is non existant**

**ISP is ITC Deltacom**

**Company is Smiths Machine Shop**

**abuse@deltacom.net**

**If from is valid then also send to abuse@slo.net**

**Notes:**

**118.189.136.119 comes back as IANA – no flow anyway**

**87.15.78.89 also comes back as IANA – no flow anyway**

**149.89.93.47 looks valid but does not flow on to the final destination  
resolves to Stuyvesant High School**

**The only line left reads:**

**209.149.145.250 ([209.16.245.179])**

**The correct ip is the one in brackets (209.16.245.179) and this  
is the address that hotmail received the email from**

# Header #5

From - Fri Mar 05 16:28:09 2004  
Return-Path: <americanairlines@info.aa.com>  
Delivered-To: pair-pair:com-jxxx@pair.COM  
X-Envelope-To: jxxx@pair.com  
Received: (qmail 84746 invoked from network);  
5 Mar 2004 20:52:45 -0000  
Received: from transit121.info.aa.com (64.73.138.121)  
by chanas.pair.com with SMTP; 5 Mar 2004 20:52:45 -0000  
To: jxxx@pair.COM  
Message-Id: <20040305145244.D157.90540-40492@info.aa.com>  
Date: Fri, 05 Mar 2004 14:52:44 -0600 (CST)  
From: American Airlines <americanairlines@info.aa.com>  
Subject: 2004 AAdvantage Upgrade Changes

# Answer #5

Correct ip is 64.73.138.121

This resolves to Berbee Information Netowrks  
abuse@binc.net and abuse@berbee.com

It looks like aa.com is partially hosted at Berbee networks in Wisconsin

# Header #6

From - Thu Mar 04 11:48:18 2004  
Return-Path: <juice3322@juno.com>  
Delivered-To: pair-pair:com-jxxx@pair.com  
X-Envelope-To: jxxx@pair.com  
Received: (qmail 12397 invoked from network); 4 Mar 2004 16:41:09 -0000  
Received: from pcp261776pcs.howard01.md.comcast.net (HELO Bob) (68.55.249.52)  
by chanas.pair.com with SMTP; 4 Mar 2004 16:41:09 -0000  
Date: Thu, 04 Mar 2004 11:41:00 -0500  
To: jxxx@pair.com  
Subject: Notify about your e-mail account utilization.  
From: staff@pair.com  
Message-ID: <yildxwxtitaqqvgbqbu@pair.com>

# Answer #6

Correct ip I 68.55.249.52

Lookup shows it is Comcast most likely in altimore

abuse@comcast.net

# Header #7

- X-Apparently-To: \*\*\*\*\*@yahoo.com via 66.218.78.102; Tue, 24 Feb 2004 12:54:48 -0800
- X-YahooFilteredBulk: 216.176.54.8
- Return-Path: <newsletter@execs-direct.com>
- Received: from 216.176.54.8 (EHLO m8.execs-direct.com) (216.176.54.8) by mta270.mail.scd.yahoo.com with SMTP; Tue, 24 Feb 2004 12:54:45 -0800
- Received: from execs-direct.com (localhost.localdomain [127.0.0.1]) by m8.execs-direct.com (Postfix) with SMTP id 9A87A305AB8D for <\*\*\*\*\*@yahoo.com>; Tue, 24 Feb 2004 12:45:11 -0800 (PST)
- Date: Tue, 24 Feb 2004 12:45:11 -0800
- From: "JobSeeker Weekly" <newsletter@execs-direct.com>
- Subject: Has The Job Market Put You In Debt?
- To: \*\*\*\*\*@yahoo.com
- Content-Transfer-Encoding: 7bit
- Content-Type: text/html; charset=us-ascii
- X-CIDL: 5119944A
- X-MIDL: 1671
- Message-Id: <20040224204511.9A87A305AB8D@m8.execs-direct.com>
- Content-Length: 3433

# Answer #7

Correct ip is 216.176.54.8

This resolves to m8-execs-direct.com

IPblock shows the ISP as fusepoint Managed services

Abuse@roundheaven.com

The received from that is 127.0.0.1 is the loopback port – my best guess is that m8-execs-direct.com is a Linux machine running postfix as a mail server and that the person who sent the email was logged onto that machine at the time

# Header #8

- MIME-Version: 1.0
- Received: from mc11-f37.hotmail.com ([65.54.167.44]) by mc11-s6.hotmail.com with Microsoft SMTPSVC(5.0.2195.6824); Sat, 28 Feb 2004 22:49:38 -0800
- Received: from phigyreey ([211.58.35.150]) by mc11-f37.hotmail.com with Microsoft SMTPSVC(5.0.2195.6824); Sat, 28 Feb 2004 22:49:37 -0800
- X-Message-Info: oem3jKoZKwpLBvs+2NgNECoR49jATTDGH3n6EFo43mk=
- Return-Path: jo8746278216skf2@yahoo.com
- Message-ID: <MC11-F37RUALA0DGUMn000246c2@mc11-f37.hotmail.com>
- X-OriginalArrivalTime: 29 Feb 2004 06:49:37.0882 (UTC)  
FILETIME=[32E06BA0:01C3FE90]

# Answer #8

211.58.35.150 is correct ip

This comes back to Hananet

abuse@hanaro.com

# Header #9

- MIME-Version: 1.0
- Received: from mc3-f29.hotmail.com ([64.4.50.165]) by mc3-s7.hotmail.com with Microsoft SMTPSVC(5.0.2195.6824); Sat, 28 Feb 2004 10:27:00 -0800
- Received: from phwaswqdxh ([198.248.38.98]) by mc3-f29.hotmail.com with Microsoft SMTPSVC(5.0.2195.6824); Sat, 28 Feb 2004 10:27:00 -0800
- X-Message-Info: RTtBqkld0RTxCGWbm9S/Lre/7ag8UB0Ta9VWI0nK05Q=
- Return-Path: oiqwaqdtgv@yahoo.com
- Message-ID: <MC3-F29JtXZe90ST6qK0000fa8f@mc3-f29.hotmail.com>
- X-OriginalArrivalTime: 28 Feb 2004 18:27:00.0249 (UTC)  
FILETIME=[74753090:01C3FE28]

# Answer #9

Correct ip is 198.248.38.98

This comes back to the Kansas research and Education Network

abuse@kanren.net

# Header #10

- MIME-Version: 1.0
- Received: from mc2-f36.hotmail.com ([65.54.190.43]) by mc2-s18.hotmail.com with Microsoft SMTPSVC(5.0.2195.6824); Tue, 2 Mar 2004 01:12:04 -0800
- Received: from mail.up.victorysoftwareproductions.com ([216.55.161.46]) by mc2-f36.hotmail.com with Microsoft SMTPSVC(5.0.2195.6824); Tue, 2 Mar 2004 01:11:54 -0800
- X-Message-Info: egX6NjsTjZFzxSrLNHFU6kGtAt/GAYyqRi5RvYoP/TE=
- Return-Path: dog79@enough.innovativesoftwaregroup.com
- Message-ID: <MC2-F36jG1JBUnqwO8l000b2e1d@mc2-f36.hotmail.com>
- X-OriginalArrivalTime: 02 Mar 2004 09:11:54.0594 (UTC)  
FILETIME=[67FACC20:01C40036]

# Answer #10

Correct ip is 216.55.161.46

This is in the dedicated.absac.net domain which is  
Abacus America Inc in San Diego

abuse@aplus.net

abuse@abac.net

# Header #11

- Received: from mc2-f23.hotmail.com ([65.54.190.30]) by mc2-s19.hotmail.com with Microsoft SMTPSVC(5.0.2195.6824); Thu, 4 Mar 2004 10:52:48 -0800
- Received: from tgateway9vpy.dextrastuff.org ([65.125.235.130]) by mc2-f23.hotmail.com with Microsoft SMTPSVC(5.0.2195.6824); Thu, 4 Mar 2004 10:52:09 -0800
- X-Message-Info: HQblehuYceTG3IK8qEopaSb6G+leUX+kqmatyjOSEH4=
- Message-Id: <805611098547526.ZM65076@gateway40>
- References: <502141354054500.GS47869@mail-o>
- Return-Path: StefanWeller352@dextrastuff.org
- X-MimeOLE: Produced By Microsoft Exchange V6.0.6375.0
- X-OriginalArrivalTime: 04 Mar 2004 18:52:09.0181 (UTC)  
FILETIME=[CBEAB0D0:01C40219

# Answer #11

Correct IP is 65.125.235.130

This comes back with Qwest as the ISP

Domain is ezzi.net in great River NY

abuse@ezzi.net

# Header #12

- From blaster20202003@yahoo.com Wed, 10 Jul 2002 00:17:07 -0700
- Received: from [63.218.225.155] by hotmail.com (3.2) with ESMTP id MHotMailBEF529340083400431953FDAE19B0FBE62; Wed, 10 Jul 2002 00:16:58 -0700
- From: blaster20202003@yahoo.com
- Subject: \*\*\*\*\* , thank you your key code : adv
- Received: from thezs.com by A7JA4A6XVBRX9.thezs.com with SMTP for \*\*\*\*\*@hotmail.com; Wed, 10 Jul 2002 03:17:40 -0500
- Date: Wed, 10 Jul 2002 03:17:40 -0500
- Message-Id: <08618E66159O5AMG.515Q7Y5G8H.blaster20202003@yahoo.com>
- X-Priority: 3
- X-Mailer: fabvac2020 V2.2
- Content-Transfer-Encoding: Quoted-Printable

# Answer #12

The thezs.com received from is invalid – there is no flow and no IP recorded  
Thezs.com resolves to 66.253.50.92 which reverses to ctf127.com

Correct ip is 63.218.225.155  
155.255.218.63.nsiq.com

This traces back to CAIS Internet in McClean, VA

abuse@cais.net and abuse@cais.com

CAIS got bought by Ardent so you could also send email to abuse@ardentcomm.com

# Header #13

- From ooinsxnxjllixxnz@msn.com Sun, 07 Jul 2002 07:10:59 -0700
- Received: from [211.220.194.201] by hotmail.com (3.2) with ESMTP id MHotMailBEF196A3004D4136E816D3DCC2C905702; Sun, 07 Jul 2002 07:10:27 -0700
- Received: from peso.ozzo.com.tw ([211.167.231.66])
- by letsgo (8.9.3/8.9.3) with SMTP id XAA00558;
- Sun, 7 Jul 2002 23:45:11 +0900
- Message-ID: <000030892037\$00004fb2\$00005239@peso.ozzo.com.tw>
- To: <sluts@letsgo>
- From: " SHAKIRA " <ooinsxnxjllixxnz@msn.com>
- Subject: >>SHAKIRA AND BRITNEY HARDCORE<< 8617
- Date: Sun, 07 Jul 2002 10:09:03 -1900
- MIME-Version: 1.0
- Content-Type: text/html;
- charset="iso-8859-1"
- Content-Transfer-Encoding: quoted-printable
- X-mailer: Microsoft Outlook Express 5.00.2717.6706
- received: from Kang ([211.33.122.71])by peso.ozzo.com.tw (2.15.0/8.8.1) with SMTP id j56PSB4G21294;Fri, 05 Jul 2002 12:11:32 +0800

# Answer #13

Correct ip is 211.220.194.201

This comes back to Kernet or Korea Telecom

abuse@kernet.net

The bottom two received froms are invalid

211.167.231.66 comes back to 66-231.e-tele-net.cn but there is no flow

211.33.122.71 comes back to Thrunet in Korea – there is no flow and it is below all the other header information

# Header #14

Received: from mc2-f14.law16.hotmail.com ([65.54.237.21]) by mc2-s7.law16.hotmail.com with Microsoft SMTPSVC(5.0.2195.4905); Tue, 30 Jul 2002 14:18:06 -0700  
Received: from 200.161.16.159 ([200.161.16.159]) by mc2-f14.law16.hotmail.com with Microsoft SMTPSVC(5.0.2195.4905); Tue, 30 Jul 2002 12:43:18 -0700  
From: "brooke236" <merryl@tumharemail.com>  
Reply-To: "brooke236" <merryl@tumharemail.com>  
Date: Tue, 23 Jan 2001 23:18:55 -0800  
Subject: I n c r e a s i n g      S e x u a l  
MIME-Version: 1.0  
X-Mailer: Microsoft Outlook Express 6.00.2600.0000  
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000  
X-Precedence-Ref: 12340  
Content-Type: text/html; charset=us-ascii  
Content-Transfer-Encoding: 7bit  
Bcc:  
Return-Path: merryl@tumharemail.com  
Message-ID: <MC2-F14zaR6xE2XKc8100042633@mc2-f14.law16.hotmail.com>  
X-OriginalArrivalTime: 30 Jul 2002 19:43:20.0544 (UTC) FILETIME=[5BC33E00:01C23801]

# Answer #14

Correct IP is 200.161.16.159

DNS is 200-161-16-159.mgnet.com.br

Drilling down and finally using whois.registro.br we find the following:

TELECOMUNICACÕES DE SAO PAULO S/A - TELESP

Paulo Arthur Juliano

Av. Paulista, 2300, 19º andar

01310-300 - Sao Paulo - SP

Email addresses are: security@TELESP.NET.BR and mail-abuse@nic.br

If from is correct then abuse@tumharemail.com

Be aware that it initially tells you to use whois.lacnic.net which tells you it is in Brazil

And is owned by whois.registro.br

Geektools correctly resolves all the way through

# Header #15

From - Sat Mar 22 13:53:30 2003

Received: from stats1.xxxxx.com (stats1.xxxxx.com [209.66.45.10])

by zeus.xxxxx.com (8.12.8/8.12.4) with SMTP id h2MJtVFG017064

for <XXXXXX@xxxxx.com>; Sat, 22 Mar 2003 14:55:31 -0500 (EST)

Received: from zeus.xxxxx.com ([209.66.0.10])

by stats1.xxxxx.com (NAVGW 2.5.1.15) with SMTP id M2003032214513531522

for <XXXXXX@xxxxx.com>; Sat, 22 Mar 2003 14:51:35 -0500

Received: from XXXXXX by zeus.xxxxx.com with local (Exim 3.32 #1)

id 18wp5S-0004R9-00 for XXXXXX@xxxxx.com; Sat, 22 Mar 2003 14:55:26 -0500

Received: from 209.66.0.11 (CacheFlowServer@[202.184.78.12])

by zeus.xxxxx.com (8.12.8/8.12.4) with SMTP id h2MJtMFG017013

for <XXXXXX@xxxxx.com>; Sat, 22 Mar 2003 14:55:24 -0500 (EST)

Received: from sb7j.n.y42b4 [70.249.144.47] by 209.66.0.11 with ESMTP id XEGZUFVBT;  
Sat, 22 Mar 03 14:37:34 +0400

Received: from 093oiq [89.157.144.129] by 70.249.144.47 with ESMTP id PQZTEMZ; Sat,  
22 Mar 03 14:35:34 +0400

Message-ID: <1kse3-y-4\$f-k\$0d\$qb6-77n39shtb6@3wfzq7>

From: "" <bj34@pow.com.br>

To: XXXXXX@xxxxx.com

Subject: hi knq

Date: Sat, 22 Mar 03 14:35:34 GMT

# Answer #15

- Correct IP is 202.184.78.12 which does not resolve to a dns name
- Seems to be owned by: JARING-SAPURAUK, Sapura Holdings Sdn Bhd, Jalan Enggang, Ulu Kelang, 54200 Kuala Lumpur
- Email is sysadm@sapura.com.my
- Could also try abuse@jaring.my which I think is the ISP or holding company.
- If the from is correct then you could also use abuse@pow.com.br
- Pow.com.br resolves to 200.250.82.1 which is in Rio Janeiro. The abuse addy for that ip is abuse@embratel.com.br and also mail-abuse@nic.br
- Other addresses:
  - 89.157.144.129 IANA
  - 70.249.144.47 can't find owner
  - 209.66.0.11 smtp.jersey.net
  - Finally get to 202.184.78.12

# URLs to trace

- Go look at these using Sam Spade
- Browse as well to check the source
- [www.msn.com](http://www.msn.com)
- [www.whitehouse.gov](http://www.whitehouse.gov)
- [www.whitehouse.com](http://www.whitehouse.com)
- [www.whitehouse.net](http://www.whitehouse.net)
- [www.midwesthtcia.org](http://www.midwesthtcia.org)
- [www.disney.com](http://www.disney.com)
- [www.yahoo.com](http://www.yahoo.com)