

Email and Web Site Tracing

Jaqui Lynch

Mainline Information Systems

Email – jaqui.lynch@mainline.com

<http://www.circle4.com/jaqui/papers/emailtrace.pdf>

Session 6830



Agenda

- Obtaining Email Headers
- Understanding & Reading Email Headers
- Tracing Email Headers and Web URLs
- Reporting and ISP Information
- References



Obtaining Email Headers

- Instructions for most clients are at:
 - <http://www.wiredkids.org/safety/e-mail/getheaders.html>
 - <http://www.haltabuse.org/help/headers/index.shtml>
- i.e. Netscape v6 mail
- Click on view and then message source
- Info on Email Headers in general:
 - <http://www.stopspam.org/email/headers/headers.html>
 - <http://tgos.org/newbie/xheader.html>

Understanding Email Headers

- Standard Header:
 - Subject: test email
 - From: peter@circle4.com
 - Reply_To: peter@circle4.com
 - Date: 08/08/2002 11.50am
 - To: jaqui@circle4.com

Full Headers 1/2

- 1. Received: from stats1.jersey.net (stats1.jersey.net [209.66.45.10]) by zeus.jersey.net (8.12.4/8.12.4) with SMTP id g78FovSo017202 for <jaqui@jersey.net>; Thu, 8 Aug 2002 11:50:58 -0400 (EDT)
- 2. Received: from zeus.jersey.net ([209.66.0.10]) by stats1.jersey.net (NAVGW 2.5.1.15) with SMTP id M2002080811503917513 for <jaqui@jersey.net>; Thu, 08 Aug 2002 11:50:39 -0400
- 3. Received: from jaqui by zeus.jersey.net with local (Exim 3.32 #1) id 17cpYw-0004TQ-00 for jaqui@jersey.net; Thu, 08 Aug 2002 11:50:58 -0400
- 4. Received: from siaar2aa.compuserve.com (siaar2aa.compuserve.com [149.174.40.137]) by zeus.jersey.net (8.12.4/8.12.4) with ESMTP id g78FovSo017173 for <jaqui@circle4.com>; Thu, 8 Aug 2002 11:50:57 -0400 (EDT)
- 5. Received: (from mailgate@localhost) by siaar2aa.compuserve.com (8.9.3/8.9.3/SUN-REL-1.3) id LAA21982 for jaqui@circle4.com; Thu, 8 Aug 2002 11:50:33 -0400 (EDT)
- 6. Received: from circle4.com (chi-tgn-goi-vty3.as.wcom.net [216.192.134.3]) by siaar2aa.compuserve.com (8.9.3/8.9.3/SUN-REL-1.3) with ESMTP id LAA21872 for <jaqui@circle4.com>; Thu, 8 Aug 2002 11:50:14 -0400 (EDT)
- 7. Message-ID: <3D5293DE.DC3025C6@circle4.com>



Full Headers 2/2

- Date: Thu, 08 Aug 2002 11:53:02 -0400
 - From: "Pete Nelson, Ph.D." <peter@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: "Pete Nelson, Ph.D." <peter@circle4.com>
 - and IP in Received from:
 - Received: from circle4.com (chi-tgn-goi-vty3.as.wcom.net [216.192.134.3])



So where did that email come from?

- Received: from circle4.com (chi-tgn-goi-vty3.as.wcom.net [216.192.134.3]) by siaar2aa.compuserve.com (8.9.3/8.9.3/SUN-REL-1.3) with ESMTP id LAA21872 for <jaqui@circle4.com>; Thu, 8 Aug 2002 11:50:14 -0400 (EDT)
- Message-ID: 3D5293DE.DC3025C6@circle4.com
- IP ADDRESS is:
- 216.192.134.3



Whois Info

- UUNET Technologies, Inc. (NET-UUNET-HIL-BLK4)
- 5000 Britton Rd.
- Hilliard, OH 43026
- US
- Netname: UUNET-HIL-BLK4
- Netblock: 216.192.0.0 - 216.193.127.255
- Maintainer: UU
- Coordinator:
- UUNET an MCI WorldCom Company (HC3-ORG-ARIN) hostmaster@wcom.net
- 614/723-8128



IP Block Info

- UUNET Technologies, Inc. (NET-UUNET-HIL-BLK4)
- 5000 Britton Rd.
- Hilliard, OH 43026
- US

- Netname: UUNET-HIL-BLK4
- Netblock: 216.192.0.0 - 216.193.127.255
- Maintainer: UU

- Coordinator:
- UUNET an MCI WorldCom Company (HC3-ORG-ARIN)
hostmaster@wcom.net
- 614/723-8128



So who was I?

- A compuserve user dialed into worldcom (which is really UUNET)
- Compuserve uses worldcom in some cases instead of its own dialin
- The email was relayed from Wcom to compuserve to the final destination – jersey.net so circle4.com is hosted at jersey.net most likely



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



Received From:

- Includes:
- Name and ip of machine handing off the email
- Name and 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 (chi-tgn-goi-vty3.as.wcom.net [216.192.134.3]) by siaar2aa.compuserve.com (8.9.3/8.9.3/SUN-REL-1.3) with ESMTP id LAA21872 for <jaqui@circle4.com>; Thu, 8 Aug 2002 11:50:14 -0400 (EDT)



Message-Id

- Unique identifier that stays with this piece of mail for life
- Can sometimes be used to tie this email to the correct Received From
- Can be faked

- Message-ID: 3D5293DE.DC3025C6@circle4.com

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 [123.123.123.123]) by mailserver.com

- Where I said I was jaqui.org but 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

Steps to Trace an email or web site

1. Analyze email headers or Web URL 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 crawl 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. For a website use the domain not the URL
 1. I.e. circle4.com not www.circle4.com

IANA Reserved Addresses

- 192.68.0.0 – 192.168.255.255
- 172.16.0.0 – 172.31.255.255
- 10.0.0.0 – 10.255.255.255

- If an address comes back to IANA it is most likely forged so look at the next one

NICs



whois.ripe.net
whois.apnic.net

whois.arin.net
whois.lacnic.net

whois.geektools.com

whois.nic.or.kr



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://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>



References

- Internet Fraud
 - <http://www1.ifccfbi.gov/index.asp>
- Obtaining and understanding email headers
 - <http://www.haltabuse.org/help/header.shtml>
 - <http://www.stopspam.org/email/headers/headers.html>
- Tracing sites
 - <http://combat.uxn.com/>
 - <http://www.network-tools.com/>
 - <http://www.geektools.com/>
 - <http://www.sampade.org/>
 - <http://www.sampade.org/ssw>
 - http://thetrainingco.com/technion_tracker.htm

Questions???



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 | ➤ 2. Across the Top |
| DNS | ➤ Select Tools and |
| WHOIS | then: |
| IPBLOCK | ➤ SMTP relay check |
| DIG | ➤ Crawl Website |
| TRACERBL | ➤ Browse Website |
| ABUSE | ➤ Parse Email Headers |

