

Email and Web Site Tracing

Jaqui Lynch
Mainline Information Systems
Email – jaqui.lynych@mainline.com
Session 1794
1.30pm 2/26/04



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 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>



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



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
- Received:
 - This is where the information you really need is
 - These can be forged
- 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 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)



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: (gmail 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: WIDOPENWEST 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
OrgNOCHandle: Network Management Center
OrgNOCHandle: +1-800-496-9669
OrgNOCHandle: 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



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.*



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. Ipbloc 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
 2. Go back and check the URL later



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 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>

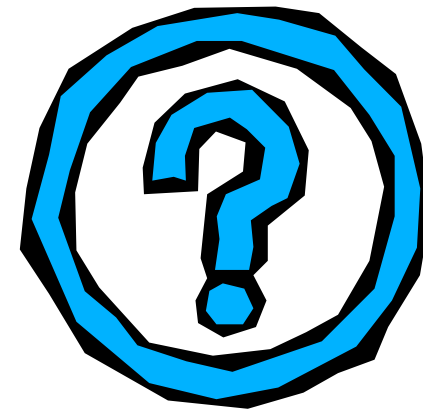


References

- 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???



Headers to Try #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]



Answers #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



Headers to Try #2

From ytU9Iea@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.yahoo.com with
QMQP; Tue, 30 Jul 2002 04:01:02 -0000
Message-ID: <Vyppq753NYU\$7DWsiiU\$PFMyp1BK@bfd9Lf5g>
From: "NORAH" <ytU9Iea@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
]



Answers #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



Headers to Try #3

From ootzzixxz@msn.com Wed, 10 Jul 2002 05:08:28 -0700
Received: from [211.62.172.8] by hotmail.com (3.2) with ESMTP id
MH0tMailBEF56E2B006A40043158D33EAC0811441; 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 " <ootzzixxz@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

]



Answers #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



Headers to Try #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 NNFP;
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 NNFP;
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]



Answers #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
87.15.78.89 also comes back as IANA
149.89.93.47 looks valid but does not flow on to the final destination
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



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

