Part III: Reading Headers

- Some simple examples
  - direct delivery
  - webmail can be perfectly traceable
- How to cock it up
  - or why the industry promotes SPOC training
- Understanding the delivery path
  - no substitute for local knowledge
- Pre-loading
  - sometimes people don't want to be caught!

A Really Simple Example

```
Return-path: <dhogb@altavista.fr>
Delivery-date: Fri, 30 May 2003 04:56:33 +0100
Received: from 12-239-186-164.client.attbi.com
        ([12.239.186.164] helo=iinet.com ident=heg3q)
        by wisbech.cl.cam.ac.uk with smtp (Exim 3.092 #1)
        id 19Lb0K-00031X-00
        for Richard.Clayton@cl.cam.ac.uk; Fri, 30 May 2003 04:56:33 +0100
Message-ID: <515001c32646$55af9d68$b740316f@vdrsou3>
From: "Duncan Ho" <dhogb@altavista.fr>
To: Richard.Clayton@cl.cam.ac.uk
Subject: I want to see you again
Date: Fri, 30 May 2003 00:55:05 +0000

                NB: 164.186.239.12 is the Defense Intelligence Agency
                NB: iinet.com is a group of West Coast ISPs
                NB: altavista.fr may well have a user called dhogb
```


- Correct answer for this example (which was a “penis extension” spam) is to contact ATT to determine which of their customer accounts was using the IP address 12.239.186.164 last Thursday evening.

  OrgAbuseName: ATT Abuse
  OrgAbusePhone: +1-919-319-8130
  OrgAbuseEmail: abuse@att.net

- Potential cock-ups are:

  to believe the Return Path (trivial to forge)

  to reverse the IP address (or indeed to believe that the attbi.com name will necessarily be valid – as it happens, it is)

  to go and talk to iinet.com

  to go and talk to the owner of wisbech.cl.cam.ac.uk

  to look up Duncan Ho on Google (he’s a Hong Kong medic)

  to forget to tell ATT Abuse that the time is GMT

  to assume that wisbech.cl.cam.ac.uk has a working clock (so maybe you need to talk to them after all)

  to believe that the ATT customer consciously “sent” the spam

Can Webmail Be Traced ?

```
Return-Path: <abcdef@hotmail.com>
Received: from bay7-f65.bay7.hotmail.com (HELO hotmail.com) (64.4.11.65)
  by lilac.gradwell.net with SMTP; 12 May 2003 23:29:45 -0000
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
    Mon, 12 May 2003 16:29:44 -0700
Received: from 193.195.0.101 by by7fd.bay7.hotmail.msn.com with HTTP;
   Mon, 12 May 2003 23:29:43 GMT
X-Originating-IP: [193.195.0.101]
X-Originating-Email: [abcdef@hotmail.com]
From: ”Less than Anonymouse" <abcdef@hotmail.com>
To: richard@highwayman.com
Subject: You can’t catch me!
Date: Mon, 12 May 2003 23:29:43 +0000
Message-ID: <BAY7-F6507Hu2tYd2hi0000ada6@hotmail.com>
X-OriginalArrivalTime: 12 May 2003 23:29:44.0068 (UTC)
FILETIME=[5E510440:01C318DE]
```


- Correct answer for this example (a special test) is to contact Demon really quickly to determine how long they keep web cache logs.

  ```
  ******************************************************
  * ABUSE CONTACT: abuse@demon.net IN CASE OF
  * INTRUSIONS, ILLEGAL ACTIVITY, ATTACKS, SCANS,
  * PROBES, SPAM, ETC.
  ******************************************************
  ```

- Potential cock-ups are:

  failing to check this really did come from Hotmail
  but 64.4.11.65 is indeed them

  to think that the easy to pick out 193.195.0.101 is always going to be of significant assistance (it is “anchor-01.www-cache.demon.co.uk”)

- If you’re wondering how you’re *sure* that “www-cache” is a web cache
  then (a) use your common sense
  or (b) if it really matters, then ask Demon.

How to Cock It Up!

- An incorrect timestamp leads to the wrong person
  - check those clocks!
- An incorrect timezone leads to the wrong person
  - you have to learn to deal with -0500 (and BST)!
- Avoid typos (take care if you cannot cut & paste)
  - 224.xx.xx.xx is detectable, others will not be!
- and who owns 192.168.0.1 ?
  - it's in RFC1918 address space
    - 192.168/16
    - 172.16/12
    - 10/8

✶ Almost every time that the industry is consulted, this type of "war story" is trotted out…. One of the reasons that so much effort is put into SPOC training is to try and eliminate this type of issue.

A More Complex Example

```
Received: from pop3.demon.co.uk by rnc1.al.cl.cam.ac.uk with POP3
 id <"happyday.1052782215:10:06336:47".happyday@pop3.demon.co.uk>
 for <happyday@pop3.demon.co.uk> ; Tue, 13 May 2003 00:31:23 +0100
Return-Path: <abcdef@hotmail.com>
Received: from punt-1.mail.demon.net by mailstore
          for richard@happyday.demon.co.uk id 1052782215:10:06336:47;
          Mon, 12 May 2003 23:30:15 GMT
Received: from lilac.gradwell.net ([195.149.39.56]) by punt-1.mail.demon.net
           id aa1105516; 12 May 2003 23:29 GMT
Received: (qmail 41764 invoked by uid 800); 12 May 2003 23:29:45 -0000
Delivered-To: forwarding-richard@highwayman.com
X-Envelope-To: richard@highwayman.com
X-Forwarding-To: richard@highwayman.com
Received: (qmail 41758 invoked from network); 12 May 2003 23:29:45 -0000
Received: from bay7-f65.bay7.hotmail.com (HELO hotmail.com) (64.4.11.65)
  by lilac.gradwell.net with SMTP; 12 May 2003 23:29:45 -0000
```


✶ These are the real headers from the previous example (ie: not the sanitised ones for a pedagogic aid).

✶ From this it can be seen that the email arrived at Gradwell's system and was then rewritten from <richard@highwayman.com> to <richard@happyday.demon.co.uk> and delivered to Demon's mail system. It was then downloaded using POP3 by a machine claiming to be rnc1.al.cl.cam.ac.uk.

Who are the Good Guys?

```
Return-Path: <nehcnelle@yahoo.com>
Received: from lilac.gradwell.net ([195.149.39.56]) by punt-2.mail.demon.net
          id aa2116333; 1 Jun 2003 13:00 GMT
Received: (qmail 7551 invoked by uid 800); 1 Jun 2003 13:00:03 -0000
Delivered-To: forwarding-amikam@highwayman.com
X-Envelope-To: amikam@highwayman.com
X-Forwarding-To: amikam@highwayman.com
Received: (qmail 7526 invoked from network); 1 Jun 2003 13:00:02 -0000
Received: from terry.blackcatnetworks.co.uk (193.201.200.35)
  by lilac.gradwell.net with SMTP; 1 Jun 2003 13:00:02 -0000
Received: from [211.90.171.142] (helo=drgoodbody.net)
   by terry.blackcatnetworks.co.uk with smtp (Exim 3.35 #1
(Debian))
   id 19MSRL-0004mS-00; Sun, 01 Jun 2003 14:00:00 +0100
Subject: Arnold Quit smoking patch
From: nehcnelle@yahoo.com (Babette Dushane)
```


✶ This email reached Gradwell via terry.blackcatnetworks.com. This is because Gradwell has a secondary email arrangement with this machine.
http://support.gradwell.net/article.php?123

✶ There is in general no way of knowing of such arrangements (though in this case a Google search will find this URL). You just need to know it (or talk to Black Cat Networks – preferably just the once!)

✶ The real source is 211.90.171.142, which you can readily determine is operated by part of the Chinese government in LianYunGang city, JiangSu province (also known an Xinpu) … 1200km SE of Beijing

Intentional Obfuscation

```
Return-Path: <lyb31141oe5217m@yahoo.com>
Received: from dhcp024-209-221-239.cinci.rr.com ([24.209.221.239])
          by relay-1.mail.demon.net  id aa0122085; 28 May 2003 11:55 GMT
Received: from emirates.net.ae (24050 [102.30.207.28])
          by  caramail.com (8.12.1/8.12.1) with ESMTP id 2012
          for <richard@pillar.turnpike.com>; Wed, 28 May 2003 04:58:18 -0700
Received: from cgocable.ca ([66.14.61.133])
          by losbacas.com (8.9.3/8.9.3) with SMTP id 32243
          for <richard@pillar.turnpike.com>; Wed, 28 May 2003 04:58:13 -0700
Message-ID: <1092030025ulfkdugCsloodu1wxuqslnh1frp@telia.com>
From: Lara <lyb31141oe5217m@yahoo.com>
To: ulfkdugCsloodu1wxuqslnh1frp <richard@pillar.turnpike.com>
Date: Wed, 28 May 2003 04:58:08 -0700
Subject:  nHi my name is BrunoB t ulfkdugCsloodu1wxuqslnh1frp
```


✶ This email arrived from 24.209.221.239 which is the IP address of a customer of “Road Runner” probably based in Cincinnati, Ohio.

✶ Before that it is alleged to have come from
102.30.207.28
which is in IANA reserved space (ie not allocated)
which is quite a good clue that this line is fake

✶ A similar email (from my disappointingly large collection of “spam”) that was sent from a Mexican ADSL connection apparently “actually” comes from 54.225.245.23 which is owned by Merck & Co (a pharmaceutical research lab). Apart recognising a particular pattern of faked material, or getting lucky with unallocated blocks of address space, there’s no way to know for sure that these header lines are fake. Investigation at the next hop back (the Road Runner customer) is the only way to know whether there is an email system there which can be trusted to add valid “Received” lines or whether a “trojan” or other configuration weakness means that entirely fake material can be funnelled through the machine.

Review

- Read "Received:" headers from the top down
- Stop when you reach one you don't trust and/or fully understand
- Double check those timestamps and timezones

- Reporting "spam" is a good way of practising!

✶ Reading email headers is, in principle, entirely straightforward. However there are lots of little quirks and details that mean that it cannot be entirely automated.

✶ Even if you regularly rely on standard tools to process headers, you need to understand what's going on in order to ensure that you can step in when they are fooled.

✶ There's no substitute for understanding which machines you can trust and having copies of "normal" email to hand in order to be able to detect anomalies.

✶ For practice… try tracing (and reporting to abuse@ the source) some of the unsolicited email you received.