Derive Intel from Emails

Dale Meredith
MCT/CEI/CEH/Security Dude
Owner: Wayne Technologies

:@dalemeredith :daledumbsITdown :daledumbsITdown
:dalemeredith www.daledumbsITdown.com

You've Got Mail = I've Got You!

Track:

When an email is read

If it's forwarded

Time spent reading

Links visited

Types of server used

OS the recipient is using

It's About the Header

```
Delivered-To: dale.meredith@gmail.com
Received: by 10.64.230.234 with SMTP id tb10csp3086933iec;
        Thu, 30 Apr 2015 07:14:50 -0700 (PDT)
X-Received: by 10.66.154.111 with SMTP id vn15mr8590499pab.108.1430403288686;
        Thu, 30 Apr 2015 07:14:48 -0700 (PDT)
Return-Path: <trc.1843@envfrm.rsys2.com>
Received: from om-thrifty.rsys3.com (om-thrifty.rsys3.com. [12.130.137.168])
        by mx.google.com with ESMTP id co1si3721858pad.63.2015.04.30.07.14.48
        for <dale.meredith@gmail.com>;
        Thu, 30 Apr 2015 07:14:48 -0700 (PDT)
Received-SPF: pass (google.com: domain of trc.1843@envfrm.rsys2.com designates 12.130.137.168 as permitted sender) client-ip=12.130.137.168;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of trc.1843@envfrm.rsys2.com designates 12.130.137.168 as permitted sender) smtp.mail=trc.1843@envfrm.rsys2.com;
       dkim=pass header.i=@email.thrifty.com;
       dmarc=pass (p=NONE dis=NONE) header.from=email.thrifty.com
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=thrifty; d=email.thrifty.com;
 h=MIME-Version:Content-Type:Content-Transfer-Encoding:Date:To:From:Reply-To:Subject:Feedback-ID:List-Unsubscribe:Message-ID;
i=thriftycarrental@email.thrifty.com;
 bh=qtw22FsUyXmGSoV2Mjp2Sib2LRs=;
 b=YnEKd5gKDeTgCnATBObseRFVZUnOQvREUN8Ou/b/0pVn/gHRaSnjoD9jSA2i/VaB57X0kKrb6+P7
   ZV4ovfMwstGUsewKmsAQqOPZ3aYEJHVaNzrM4z7N8YeuIS0YsYvkCs5u7n6P02pog5OL0djG6Pcg
   ccU7yMqJzYgV3pRAKI4=
DKIM-Signature: v=1; a=rsa-sha1; c=re
 h=MIME-Version:Content-Type:Content-Transfer-Encoding:Date:To:From:Reply-To:Subject:Feedback-ID:List-Unsubscribe:Message-ID;
 bh=qtw22FsUyXmGSoV2Mjp2Sib2LRs=;
 b=sGSEoxHmf0cLvIw1p5E7rxvx5Xtig40e9hTCZNQgznJszqbJaukBdQ9Fj59gEp98DXxTtcUnZ4fA
   INUa9cOZZsUhQW0KA5NktqZYLPE9oGNd7TiXoGQ1IgpAGngq85cLlnxAebsAySImx7g4v+RMPpcG
   vXg6qxxMiLEWQA9JtBk=
DomainKey-Signature: a=rsa-sha1; c=nofws; q=dns; s=thrifty; d=email.thrifty.com;
 b=FD1NQARjqKEWUoNKXgV6PijnBhgxL6Kze7kok7Y9knYU2pRbTjrYkc6Bf+E6wpE9B01dA9Bzjr+S
   nh0beQW9Qukim5z7jqURcgVoqM4GDvJohxjZQp0Fm2KMpswwmRAbWjbHnqsFVCa4ZXzuk8eu3YzC
```

Who the email went to

Date and time received

Where did it come from

Sender's IP address

Sender mail server

Original sender's email server's name

Authentication system used (sender)

Email Tracking Tools

- PoliteMail
- Email Lookup
- eMailTracker Pro
- DidTheyReadIt
- Read Notify
- WhoReadMe
- GetNotified
- G-Lock Analytics
- MSGTAG
- Trace Email

Demo

eMailTrackerPro

Up Next:
Examining WHOIS and DNS for Intel