**[What Can You Find in an Email Header?](https://www.howtogeek.com/108205/htg-explains-what-can-you-find-in-an-email-header/)**

by [**Jason Faulkner**](https://www.howtogeek.com/author/jasonfaulkner/) on September 28th, 2016



Whenever you receive an email, there is a lot more to it than meets the eye. While you typically only pay attention to the from address, subject line and body of the message, there is lots more information available “under the hood” of each email which can provide you a wealth of additional information.

**Why Bother Looking at an Email Header?**

This is a very good question. For the most part, you really wouldn’t ever need to unless:

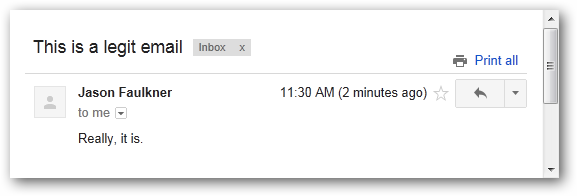
* You suspect an email is a phishing attempt or spoof
* You want to view routing information on the email’s path
* You are a curious geek

Regardless of your reasons, reading email headers is actually quite easy and can be very revealing.

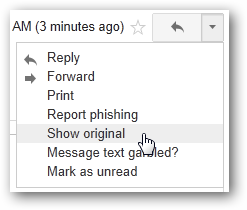
Article Note: For our screenshots and data, we will be using Gmail but virtually every other mail client should provide this same information as well.

**Viewing the Email Header**

In Gmail, view the email. For this example, we will use the email below.



Then click the arrow in the upper right corner and select Show original.



The resulting window will have the email header data in plain text.

*Note: In all the email header data I show below I have changed my Gmail address to show as*[*myemail@gmail.com*](mailto:myemail@gmail.com)*and my external email address to show as*[*jfaulkner@externalemail.com*](mailto:jfaulkner@externalemail.com)*and*[*jason@myemail.com*](mailto:jason@myemail.com)*as well as masked the IP address of my email servers.*

Delivered-To: myemail@gmail.com  
Received: by 10.60.14.3 with SMTP id l3csp18666oec;  
Tue, 6 Mar 2012 08:30:51 -0800 (PST)  
Received: by 10.68.125.129 with SMTP id mq1mr1963003pbb.21.1331051451044;  
Tue, 06 Mar 2012 08:30:51 -0800 (PST)  
Return-Path: <jfaulkner@externalemail.com>  
Received: from exprod7og119.obsmtp.com (exprod7og119.obsmtp.com. [64.18.2.16])  
by mx.google.com with SMTP id l7si25161491pbd.80.2012.03.06.08.30.49;  
Tue, 06 Mar 2012 08:30:50 -0800 (PST)  
Received-SPF: neutral (google.com: 64.18.2.16 is neither permitted nor denied by best guess record for domain of jfaulkner@externalemail.com) client-ip=64.18.2.16;  
Authentication-Results: mx.google.com; spf=neutral (google.com: 64.18.2.16 is neither permitted nor denied by best guess record for domain of jfaulkner@externalemail.com) smtp.mail=jfaulkner@externalemail.com  
Received: from mail.externalemail.com ([XXX.XXX.XXX.XXX]) (using TLSv1) by exprod7ob119.postini.com ([64.18.6.12]) with SMTP  
ID DSNKT1Y7uSEvyrMLco/atcAoN+95PMku3Y/9@postini.com; Tue, 06 Mar 2012 08:30:50 PST  
Received: from MYSERVER.myserver.local ([fe80::a805:c335:8c71:cdb3]) by  
MYSERVER.myserver.local ([fe80::a805:c335:8c71:cdb3%11]) with mapi; Tue, 6 Mar  
2012 11:30:48 -0500  
From: Jason Faulkner <jfaulkner@externalemail.com>  
To: “myemail@gmail.com” <myemail@gmail.com>  
Date: Tue, 6 Mar 2012 11:30:48 -0500  
Subject: This is a legit email  
Thread-Topic: This is a legit email  
Thread-Index: Acz7tnUyKZWWCcrUQ+++QVd6awhl+Q==  
Message-ID: <682A3A66C6EAC245B3B7B088EF360E15A2B30B10D5@MYSERVER.myserver.local>  
Accept-Language: en-US  
Content-Language: en-US  
X-MS-Has-Attach:  
X-MS-TNEF-Correlator:  
acceptlanguage: en-US  
Content-Type: multipart/alternative;  
boundary=”\_000\_682A3A66C6EAC245B3B7B088EF360E15A2B30B10D5HARDHAT2hardh\_”  
MIME-Version: 1.0

 When you read an email header, the data is in reverse chronological order, meaning the info at the top is the most recent event. Therefor if you want to trace the email from sender to recipient, start at the bottom. Examining the headers of this email we can see several things.

Here we see information generated by the sending client. In this case, the email was sent from Outlook so this is the metadata Outlook adds.

From: Jason Faulkner <jfaulkner@externalemail.com>  
To: “myemail@gmail.com” <myemail@gmail.com>  
Date: Tue, 6 Mar 2012 11:30:48 -0500  
Subject: This is a legit email  
Thread-Topic: This is a legit email  
Thread-Index: Acz7tnUyKZWWCcrUQ+++QVd6awhl+Q==  
Message-ID: <682A3A66C6EAC245B3B7B088EF360E15A2B30B10D5@MYSERVER.myserver.local>  
Accept-Language: en-US  
Content-Language: en-US  
X-MS-Has-Attach:  
X-MS-TNEF-Correlator:  
acceptlanguage: en-US  
Content-Type: multipart/alternative;  
boundary=”\_000\_682A3A66C6EAC245B3B7B088EF360E15A2B30B10D5HARDHAT2hardh\_”  
MIME-Version: 1.0

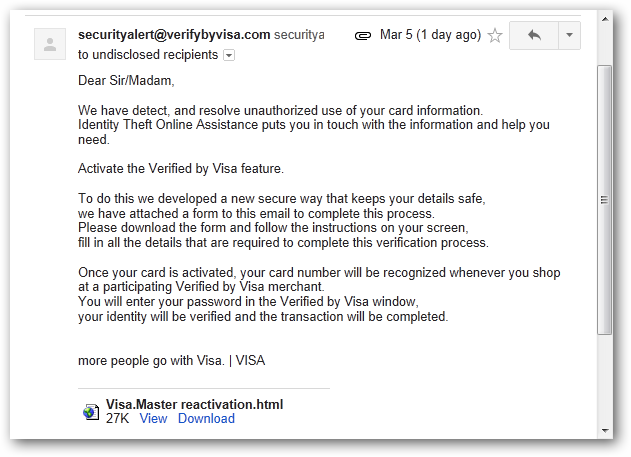
The next part traces the path the email takes from the sending server to the destination server. Keep in mind these steps (or hops) are listed in reverse chronological order. We have placed the respective number next to each hop to illustrate the order. Note that each hop shows detail about the IP address and respective reverse DNS name.

Delivered-To: myemail@gmail.com  
**[6]** Received: by 10.60.14.3 with SMTP id l3csp18666oec;  
Tue, 6 Mar 2012 08:30:51 -0800 (PST)  
**[5]** Received: by 10.68.125.129 with SMTP id mq1mr1963003pbb.21.1331051451044;  
Tue, 06 Mar 2012 08:30:51 -0800 (PST)  
Return-Path: <jfaulkner@externalemail.com>  
**[4]** Received: from exprod7og119.obsmtp.com (exprod7og119.obsmtp.com. [64.18.2.16])  
by mx.google.com with SMTP id l7si25161491pbd.80.2012.03.06.08.30.49;  
Tue, 06 Mar 2012 08:30:50 -0800 (PST)  
**[3]** Received-SPF: neutral (google.com: 64.18.2.16 is neither permitted nor denied by best guess record for domain of jfaulkner@externalemail.com) client-ip=64.18.2.16;  
Authentication-Results: mx.google.com; spf=neutral (google.com: 64.18.2.16 is neither permitted nor denied by best guess record for domain of jfaulkner@externalemail.com) smtp.mail=jfaulkner@externalemail.com  
**[2]** Received: from mail.externalemail.com ([XXX.XXX.XXX.XXX]) (using TLSv1) by exprod7ob119.postini.com ([64.18.6.12]) with SMTP  
ID DSNKT1Y7uSEvyrMLco/atcAoN+95PMku3Y/9@postini.com; Tue, 06 Mar 2012 08:30:50 PST  
**[1]** Received: from MYSERVER.myserver.local ([fe80::a805:c335:8c71:cdb3]) by  
MYSERVER.myserver.local ([fe80::a805:c335:8c71:cdb3%11]) with mapi; Tue, 6 Mar  
2012 11:30:48 -0500

While this is pretty mundane for a legitimate email, this information can be quite telling when it comes to examining spam or phishing emails.

**Examining a Phishing Email – Example 1**

For our first phishing example, we will examine an email which is an obvious phishing attempt. In this case we could identify this message as a fraud simply by the visual indicators but for practice we will take a look at the warning signs within the headers.



Delivered-To: myemail@gmail.com  
Received: by 10.60.14.3 with SMTP id l3csp12958oec;  
Mon, 5 Mar 2012 23:11:29 -0800 (PST)  
Received: by 10.236.46.164 with SMTP id r24mr7411623yhb.101.1331017888982;  
Mon, 05 Mar 2012 23:11:28 -0800 (PST)  
Return-Path: <securityalert@verifybyvisa.com>  
Received: from ms.externalemail.com (ms.externalemail.com. [XXX.XXX.XXX.XXX])  
by mx.google.com with ESMTP id t19si8451178ani.110.2012.03.05.23.11.28;  
Mon, 05 Mar 2012 23:11:28 -0800 (PST)  
Received-SPF: fail (google.com: domain of securityalert@verifybyvisa.com does not designate XXX.XXX.XXX.XXX as permitted sender) client-ip=XXX.XXX.XXX.XXX;  
Authentication-Results: mx.google.com; spf=hardfail (google.com: domain of securityalert@verifybyvisa.com does not designate XXX.XXX.XXX.XXX as permitted sender) smtp.mail=securityalert@verifybyvisa.com  
Received: with MailEnable Postoffice Connector; Tue, 6 Mar 2012 02:11:20 -0500  
Received: from mail.lovingtour.com ([211.166.9.218]) by ms.externalemail.com with MailEnable ESMTP; Tue, 6 Mar 2012 02:11:10 -0500  
Received: from User ([118.142.76.58])  
by mail.lovingtour.com  
; Mon, 5 Mar 2012 21:38:11 +0800  
Message-ID: <6DCB4366-3518-4C6C-B66A-F541F32A4C4C@mail.lovingtour.com>  
Reply-To: <securityalert@verifybyvisa.com>  
From: “securityalert@verifybyvisa.com”<securityalert@verifybyvisa.com>  
Subject: Notice  
Date: Mon, 5 Mar 2012 21:20:57 +0800  
MIME-Version: 1.0  
Content-Type: multipart/mixed;  
boundary=”—-=\_NextPart\_000\_0055\_01C2A9A6.1C1757C0″  
X-Priority: 3  
X-MSMail-Priority: Normal  
X-Mailer: Microsoft Outlook Express 6.00.2600.0000  
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000  
X-ME-Bayesian: 0.000000

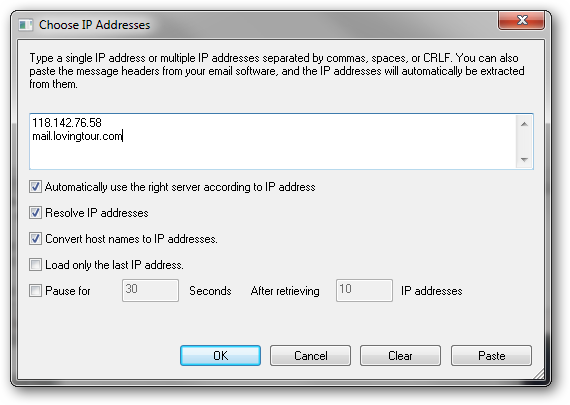
The first red flag is in the client information area. Notice here the metadata added references Outlook Express. It is unlikely that Visa is so far behind the times that they have someone manually sending emails using a 12 year old email client.

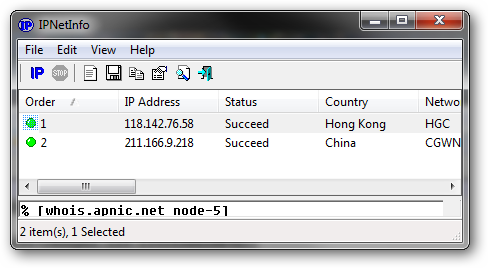
Reply-To: <securityalert@verifybyvisa.com>  
From: “securityalert@verifybyvisa.com”<securityalert@verifybyvisa.com>  
Subject: Notice  
Date: Mon, 5 Mar 2012 21:20:57 +0800  
MIME-Version: 1.0  
Content-Type: multipart/mixed;  
boundary=”—-=\_NextPart\_000\_0055\_01C2A9A6.1C1757C0″  
X-Priority: 3  
X-MSMail-Priority: Normal  
**X-Mailer: Microsoft Outlook Express 6.00.2600.0000**X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000  
X-ME-Bayesian: 0.000000

Now examining the first hop in the email routing reveals that the sender was located at IP address 118.142.76.58 and their email was relayed through the mail server mail.lovingtour.com.

Received: from User ([118.142.76.58])  
by mail.lovingtour.com  
; Mon, 5 Mar 2012 21:38:11 +0800

Looking up the IP information using Nirsoft’s IPNetInfo utility, we can see the sender was located in Hong Kong and the mail server is located in China.



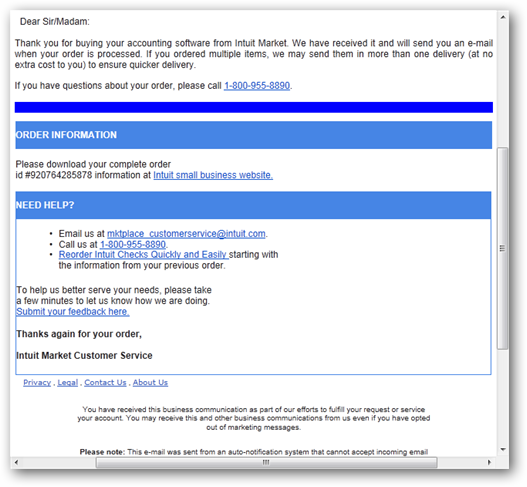


Needless to say this is a bit suspicious.

The rest of the email hops are not really relevant in this case as they show the email bouncing around legitimate server traffic before finally being delivered.

**Examining a Phishing Email – Example 2**

For this example, our phishing email is much more convincing. There are a few visual indicators here if you look hard enough, but again for the purposes of this article we are going to limit our investigation to email headers.



Delivered-To: myemail@gmail.com  
Received: by 10.60.14.3 with SMTP id l3csp15619oec;  
Tue, 6 Mar 2012 04:27:20 -0800 (PST)  
Received: by 10.236.170.165 with SMTP id p25mr8672800yhl.123.1331036839870;  
Tue, 06 Mar 2012 04:27:19 -0800 (PST)  
Return-Path: <security@intuit.com>  
Received: from ms.externalemail.com (ms.externalemail.com. [XXX.XXX.XXX.XXX])  
by mx.google.com with ESMTP id o2si20048188yhn.34.2012.03.06.04.27.19;  
Tue, 06 Mar 2012 04:27:19 -0800 (PST)  
Received-SPF: fail (google.com: domain of security@intuit.com does not designate XXX.XXX.XXX.XXX as permitted sender) client-ip=XXX.XXX.XXX.XXX;  
Authentication-Results: mx.google.com; spf=hardfail (google.com: domain of security@intuit.com does not designate XXX.XXX.XXX.XXX as permitted sender) smtp.mail=security@intuit.com  
Received: with MailEnable Postoffice Connector; Tue, 6 Mar 2012 07:27:13 -0500  
Received: from dynamic-pool-xxx.hcm.fpt.vn ([118.68.152.212]) by ms.externalemail.com with MailEnable ESMTP; Tue, 6 Mar 2012 07:27:08 -0500  
Received: from apache by intuit.com with local (Exim 4.67)  
(envelope-from <security@intuit.com>)  
id GJMV8N-8BERQW-93  
for <jason@myemail.com>; Tue, 6 Mar 2012 19:27:05 +0700  
To: <jason@myemail.com>  
Subject: Your Intuit.com invoice.  
X-PHP-Script: intuit.com/sendmail.php for 118.68.152.212  
From: “INTUIT INC.” <security@intuit.com>  
X-Sender: “INTUIT INC.” <security@intuit.com>  
X-Mailer: PHP  
X-Priority: 1  
MIME-Version: 1.0  
Content-Type: multipart/alternative;  
boundary=”————03060500702080404010506″  
Message-Id: <JXON1H-5GTPKV-0H@intuit.com>  
Date: Tue, 6 Mar 2012 19:27:05 +0700  
X-ME-Bayesian: 0.000000

In this example, a mail client application was not used, rather a PHP script with the source IP address of 118.68.152.212.

To: <jason@myemail.com>  
Subject: Your Intuit.com invoice.  
**X-PHP-Script: intuit.com/sendmail.php for 118.68.152.212**From: “INTUIT INC.” <security@intuit.com>  
X-Sender: “INTUIT INC.” <security@intuit.com>  
X-Mailer: PHP  
X-Priority: 1  
MIME-Version: 1.0  
Content-Type: multipart/alternative;  
boundary=”————03060500702080404010506″  
Message-Id: <JXON1H-5GTPKV-0H@intuit.com>  
Date: Tue, 6 Mar 2012 19:27:05 +0700  
X-ME-Bayesian: 0.000000

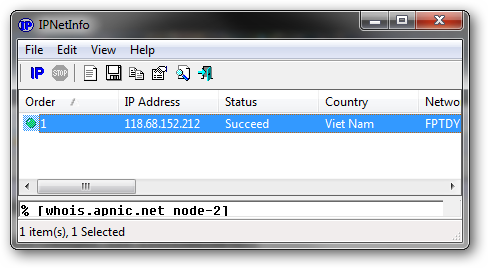
However, when we look at the first email hop it appears to be legit as the sending server’s domain name matches the email address. However, be wary of this as a spammer could easily name their server “intuit.com”.

Received: from apache by intuit.com with local (Exim 4.67)  
(envelope-from <security@intuit.com>)  
id GJMV8N-8BERQW-93  
for <jason@myemail.com>; Tue, 6 Mar 2012 19:27:05 +0700

Examining the next step crumbles this house of cards. You can see the second hop (where it is received by a legitimate email server) resolves the sending server back to the domain “dynamic-pool-xxx.hcm.fpt.vn”, not “intuit.com” with the same IP address indicated in the PHP script.

Received: from dynamic-pool-xxx.hcm.fpt.vn ([118.68.152.212]) by ms.externalemail.com with MailEnable ESMTP; Tue, 6 Mar 2012 07:27:08 -0500

Viewing the IP address information confirms the suspicion as the mail server’s location resolve back to Viet Nam.



While this example is a bit more clever, you can see how quickly the fraud is revealed with only a slight bit of investigation.

**Conclusion**

While viewing email headers probably isn’t a part of your typical day to day needs, there are cases where the information contained in them can be quite valuable. As we showed above, you can quite easily identify senders masquerading as something they are not. For a very well executed scam where visual cues are convincing, it is extremely difficult (if not impossible) to impersonate actual mail servers and reviewing the information inside of email headers can quickly reveal any chicanery.