INTERNET

What Can You Learn From An Email Header (Metadata)?

By Guy McDowell / August 13, 2013 / 17 minutes

Did you ever get an email and really wondered where it came from? Who sent it? How could they have known who you are? Surprisingly a lot of that information can be from from the email header, or by using info from the email header to do some detective work.

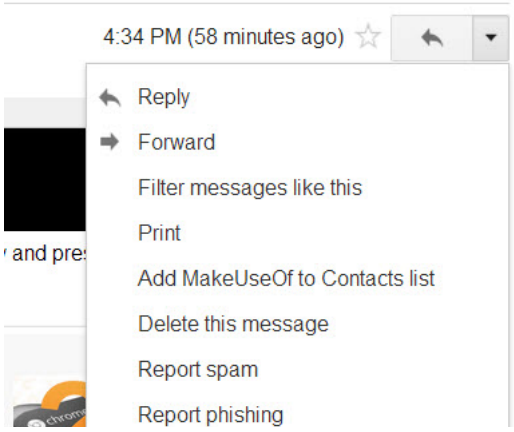
The header is a part of the email message that most people never even see. It contains a lot of data that seems like gobbledygook to the average computer user, so as email use became a daily tool in everyone's life, email clients started to hide this information out of convenience for you. These days, it can even be a bit troublesome to unhide the header, even for those who know it is there. There are so many different email clients out there, both desktop and web-based, that to cover how to unhide the email header could end up being a small book. Today, we're just going to focus on how to unhide the header in Gmail, and then look at what we can glean from the header.

What is an Email Header?

An email header is a collection of information that documents the path by which the email got to you. There may be a lot of information in the header or just the basics. There is a standard for what information should be included in a header, but not really a limit to what information an email server might put into the header. If you are curious about what a standard for an email protocol looks like, check out RFC 5321 – Simple Mail Transfer Protocol. It's a bit hard on the head, especially if you don't need to know this stuff.

Gmail – Unhide the Email Header

Once you have an email message open in Gmail, click on the downward facing arrow near the top-right hand corner of the message. A new menu will show itself. Click on Show original to see the raw email message with its full contents and header revealed.



Guy McDowell
208 articles

With 20+ years of experience in IT, training, and technical trades, it is my desire to share what I've learned with anyone else willing to learn. I strive to do the best job possible in the best manner possible, and with a little humour. Keep in touch: Twitter - Facebook…

Latest Giveaway

Win a OnePlus 3 in our latest giveaway!

Related Articles

INTERNET , OFFICE PRODUCTIVITY

5 Universal Email Tools You Should Use to Make Life Easier

Mihir Patkar / August 23, 2016

OFFICE PRODUCTIVITY

How to Edit Email Fonts & Formatting in Microsoft Outlook

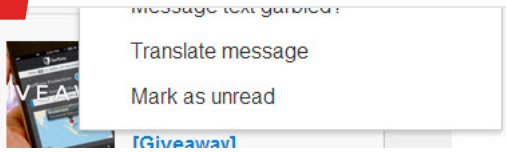
Brad Jones / August 22, 2016

MAC OS X

9 Quick Ways to Share Files & Folders from a Mac

Tim Brookes / August 16, 2016

Latest Deals



A new window or tab will open and you'll see a plain text version of your email with the header at the top, of course. The content of the header will look something like this:

Delivered-To: guy@makeuseof.com
Received: by 10.223.200.70 with SMTP id ev6csp162209fab;
Mon, 29 Jul 2013 14:15:09 -0700 (PDT)
X-Received: by 10.236.227.202 with SMTP id
d70mr27737943yhq.86.1375132508769;
Mon, 29 Jul 2013 14:15:08 -0700 (PDT)
Return-Path: <gmcdowell@somecompany.com>
Received: from mx21.exchange.telus.com (MX21.exchange.telus.com.
[205.206.208.34])
by mx.google.com with ESMTPS id
y27si28720489yhc.101.2013.07.29.14.15.08
for <guy@makeuseof.com>
(version=TLSv1 cipher=RC4-SHA bits=128/128);
Mon, 29 Jul 2013 14:15:08 -0700 (PDT)
Received-SPF: neutral (google.com: 205.206.208.34 is neither permitted
nor denied by best guess record for domain of
gmcdowell@somecompany.com) client-ip=205.206.208.34;
Authentication-Results: mx.google.com;
spf=neutral (google.com: 205.206.208.34 is neither permitted nor denied
by best guess record for domain of gmcdowell@somecompany.com)
smtp.mail=gmcdowell@somecompany.com
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-Anti-Spam-Result:
AkYBAN3a9lHNztK7hGdsb2JhbABYA4JCebVsiEWBHBYOAQEBChZDgiQBAQEEBSAIARs
X-IronPort-AV: E=Sophos;i="4.89,772,1367992800";
d="jpg'145?scan'145,208,217,145";a="14712973"
Received: from unknown (HELO mail.exchange.telus.com)
([205.206.210.187])
by mx21.exchange.telus.com with ESMTP/TLS/AES128-SHA; 29 Jul 2013
15:15:07 -0600
Received: from HEXMBVS12.hostedmsx.local ([10.9.6.115]) by
HEXHUB13.hostedmsx.local ([::1]) with mapi; Mon, 29 Jul 2013 15:13:48
-0600
From: Guy McDowell <gmcdowell@somecompany.com>
To: "guy@makeuseof.com" <guy@makeuseof.com>
Date: Mon, 29 Jul 2013 15:15:03 -0600
Subject: What's an E-mail Header?
Thread-Topic: What's an E-mail Header?
Thread-Index: Ac6MoKVNNmE/49PeSfezKxVNOP2KEQ==
Message-ID:
<5FE22E33565B894BBE2CB78DD0396DA01808A1B1B2@HEXMBVS12.hostedmsx.local>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
acceptlanguage: en-US
Content-Type: multipart/related;

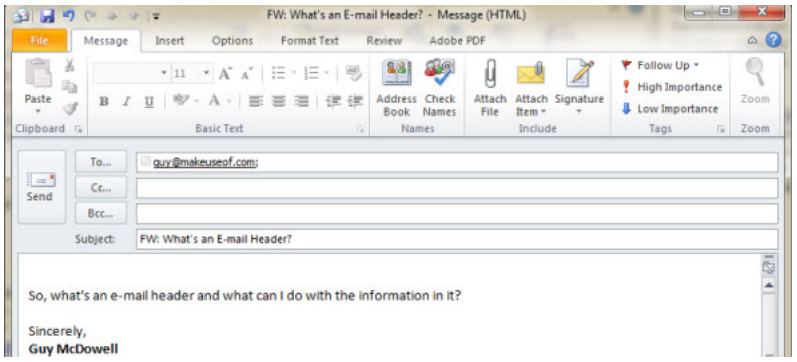
MIME-Version: 1.0

That's nice. What does that mean?

How is the Email Header Created?

By knowing how the header is created along the path an email travels, you will develop keener insight into what a header's data means. Let's look at the parts as they are added, and what the most important parts mean.

On the Sender's Computer



Part of the header is created when the sender creates the email to send to the recipient. This will include such information as when the email was composed, who composed it, the subject line and to whom the email is being sent. This is the part of the header that you are most familiar seeing as the Date:, From:, To:, and Subject: lines on the top of your email.

From: Guy McDowell <gmcdowell@somecompany.com>
To: "guy@makeuseof.com" <guy@makeuseof.com>
Date: Mon, 29 Jul 2013 15:15:03 -0600
Subject: What's an Email Header?

On the Sender's Email Service

More information is added to the header once the email is actually sent. This is provided by the email service that the sender is using. In this case, the sender is using a hosted email service, so the IP address shown is an address that is internal to the service provider's network. Performing a WHOIS search on it will not provide any useful information. What we can do is perform a Google search on the server name **HEXMBVS12.hostedmsx.local** and we can find that the service provider is Telus. If we do some digging around in the Telus website, we'll find that they offer a Hosted Microsoft Exchange service. That suggests that the sender is probably using either Microsoft Outlook, Outlook Express, or Outlook Web Access. Information added here includes, the IP address of the sender ([10.9.6.115]), the time sent by the sender's email service (Mon, 29 Jul 2013 15:13:48 -0600), and the Message-ID for that particular message as added by the email service.

(5FE22E33565B894BBE2CB78DD0396DA01808A1B1B2@HEXMBVS12.hostedmsx.local).
Received: from HEXMBVS12.hostedmsx.local ([10.9.6.115]) by HEXHUB13.hostedmsx.local ([::1]) with mapi; Mon, 29 Jul 2013 15:13:48 -0600
Message-ID:

...y to the Recipient's Email Service

From there, the email may take any number of routes to end up at the recipient's email service. This can be added to the header to show the 'hops' the email had to make to get to you. These hops start at the server that most recently handled the email and go back to the server that originally handled it, in reverse chronological order. In this example, all the hops are internal at the sender's email service.

Third, and Final Hop

Received: from mx21.exchange.telus.com (MX21.exchange.telus.com. [205.206.208.34])
by mx.google.com with ESMTPS id y27si28720489yhc.101.2013.07.29.14.15.08
for <guy@makeuseof.com>
(version=TLSv1 cipher=RC4-SHA bits=128/128);
Mon, 29 Jul 2013 14:15:08 -0700 (PDT)
Received-SPF: neutral (google.com: 205.206.208.34 is neither permitted nor denied by best guess record for domain of gmcdowell@somecompany.com) client-ip=205.206.208.34;
Authentication-Results: mx.google.com;
spf=neutral (google.com: 205.206.208.34 is neither permitted nor denied by best guess record for domain of gmcdowell@somecompany.com)
smtp.mail=gmcdowell@somecompany.com
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-Anti-Spam-Result: AkYBAN3a9lHNztK7hGdsb2JhbABYA4JCebVsiEWBHBYOAQEBChZDgiQBAQEEBSAIARsoAhQEARUQAQEBCh4FEAEDCQIMJgE
X-IronPort-AV: E=Sophos;i="4.89,772,1367992800";
d="jpg'145?scan'145,208,217,145";a="14712973"

Third Hop Explanation

This is the hop that takes it from Telus to the recipients email server. We can tell that it was received by mx.google.com, so the recipient has their email service with Google. Here it is good to note the line **Received-SPF:** SPF, or Sender Policy Framework, is a standard by which a sender's email server can declare itself to be the legitimate sender of the email. In this case, the qualifier is **neutral**, which means that nothing can be said about the validity of this e-mail, good or bad. Had it registered as **fail**, it would have been rejected by Gmail's servers. If it were **softfail**, Gmail would have accepted it, but flagged it as possibly not being from whom it says it is from.

Just below that, you'll also see three lines starting with **X-IronPort-Anti-Spam**. The first, **X-IronPort-Anti-Spam-Filtered: true**, is tacked on by Telus' IronPort anti-spam appliance. IronPort is a part of Cisco, so it's considered to be pretty reliable. The **X-IronPort-Anti-Spam-Result** line is meant solely for the IronPort appliances and cannot be decoded for human eyes – unless you work for Cisco and need to decode it. The third, **X-IronPort-AV**, shows that the sender has their own anti-spam appliance from Sophos. It could have read McAfee or Norton, or whatever filter your email goes through. As the recipient, this can give you a little more confidence that the email is valid.

Second Hop

Received: from unknown (HELO mail.exchange.telus.com) ([205.206.210.187])
by mx21.exchange.telus.com with ESMTP/TLS/AES128-SHA; 29 Jul 2013 15:15:07 -0600

Second Hop Explanation

It becomes obvious here that Telus is the service provider. If there is any doubt about this, perform a WHOIS check on the IP address shown: 205.206.210.187. If you aren't familiar with what a WHOIS check is or how to do one, take a read over Dave Leclairs review, . You'll find that the IP address also leads to Telus. That gives you a little more confidence that the email is legitimate. We can also

how far apart are the two servers.

First Hop

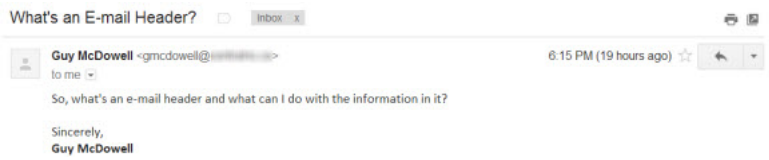
Received: from HEXMBVS12.hostedmsx.local ([10.9.6.115]) by HEXHUB13.hostedmsx.local ([::1]) with mapi; Mon, 29 Jul 2013 15:13:48 -0600

First Hop Explanation

The first hop is the sender's email server that receives his email message. At this point the email is still moving internally within the sender's email server's network. You can tell by the fact that the IP address starts with **10**. IP address that start with 10 are reserved for internal use only.

At the Recipient's E-mail Server

Delivered-To: guy@makeuseof.com
Received: by 10.223.200.70 with SMTP id ev6csp162209fab;
Mon, 29 Jul 2013 14:15:09 -0700 (PDT)
X-Received: by 10.236.227.202 with SMTP id d70mr27737943yhq.86.1375132508769;
Mon, 29 Jul 2013 14:15:08 -0700 (PDT)
Return-Path: <gmcdowell@somecompany.com>



Once it gets to the recipient's email service, more information is added to the header — which of the recipient's email services servers received it and when, what email server the message was received from, the intended recipient's email address, and the sender's stated 'reply to' email address. back in the Third Hop, we saw that the recipient's email service was with Google. We can tell that this email was received by one internal server and passed on to another – 10.236.227.202 to 10.223.200.70. Most importantly we can tell by the **Return-Path: <gmcdowell@somecompany.com>** that the email to reply to and the email of the sender is the same. This also tells us that there is a good chance this email is legitimate.

Other Things from Other Headers

This particular email header is limited in its information because a hosted email service is being used. If the sender were using their own email server, we might be able to gain a little more information. We might be able to determine exactly what mail client they are using. Or we could perform a WHOIS on the sender's IP address and get an approximate location of the sender. We could also perform a simple web search on the sender's domain and see if there is a website for them. Based on that website, we may be able to find out even more information about the sender. You might conduct a web search on the email address itself and start doxing the person. If you're not familiar with the concept of 'doxing' familiarize yourself with Joel Lee's **What Is Doxing & How Does It Affect Your Privacy?** Also take a read over Ryan Dube's article, **15 Websites to Find People On The Internet**.

What Is Doxing & How Does It Affect Your Privacy? [MakeUseOf Explains]

Internet privacy is a huge deal. One of the stated perks of the Internet is that you can remain anonymous behind your monitor as you browse, chat, and do whatever it is that you do....

READ MORE

All electronic communications leave footprints. Some are larger and easier to follow. Some are obscured by web filters and proxy servers. Either way, what is left behind tells us something about the person that created them. From that metadata, we might conduct further investigations to learn more about the people involved. Are they hiding something by using a VPN? Are they really from a legitimate business with a legitimate web presence? Is this someone I really want to go on a date with? What can ordinary people learn about me, let alone the NSA?

Take a look at your email headers and see what they say about you. If you find some header lines that don't make much sense, put them in the comments and we'll try to decode them. Have you had to do some email header investigating? Tell us about it! That's how we all learn.

Image Credit: Server Room by torkildr via Flickr.

14 COMMENTS

WRITE A COMMENT

Scroll down for the next article

INTERNET

Print Vs. Digital: What Is the Future for News? [You Told Us]

By Dave Parrack / August 13, 2013 / 6 minutes

Print media was once king, but sales of newspapers and other physical publications have receded sharply in the face of the wealth of options offered by the Internet. It has all been one way traffic to this point, with people invariably switching away from print media to adopt digital media as their new ruler.

What Do You Use For News? [You Told Us]

Dave Parrack
1461 articles

Dave Parrack is a writer and editor from the UK with unhealthy levels of interest in technology and pop culture. You can connect with him on About.me.

Latest Giveaway

READ MORE

giveaway!

However, Jeff Bezos, founder and CEO of Amazon, recently surprised a great many people by personally purchasing The Washington Post, an august newspaper most famous for breaking the Watergate scandal. Could this be a sign that there is life left in print yet? Or is this actually just another sign of how new media is winning the war on old media?

This was the debate that formed the basis for last week's *We Ask You* debate all about 'Print vs Digital'.

The Results

We asked you, ***Print Vs. Digital: What Is The Future For News?*** This question elicited a rather disappointing response, with just a handful of interested parties choosing to have their say on the issue. Still, those good people who did get involved generally had lots to say on the matter.

The picture that emerged from the comments is one where print media is revered but is almost certain to be heading for destruction. Sentiments such as the following, all of which are applied to reading newspapers and magazines, suggest there is a lot of love out there for print media.

"*The … satisfaction that comes from reading a printed newspaper cannot be replaced.*"
"*Nothing can substitute the smell of a fresh newspaper.*"
"*A newspaper can be folded until it can be read in tight quarters.*"
"*I can't shake the comfort of holding a newspaper in my hand, leaning on my chair.*"

The people quoted above may prefer printed media, but most openly admit they cannot see a future for it in the face of such overwhelming competition from the Web. Which means there will be a lot of disappointed people around when newspapers are phased out in favor of websites, media portals, apps, and eBook editions.

The video embedded below shows how much effort goes into producing a daily newspaper, which cannot even be compared to the (lack of) infrastructure and resources required to run a website.

Why Is The Newspaper Business Dying?

Comment Of The Week

We had great input from the likes of Harshit J, likefunbutnot, and Lisa O, to name just a few. *Comment Of The Week* goes to dragonmouth, who, as well as the respect of myself and hopefully everybody reading this, receives a T-shirt for this comment:

Print vs. Digital: What Is the Future for News? [We Ask You]

Jeff Bezos, the founder and CEO of Internet retail giant Amazon, has bought The Washington Post for $250 million. This makes Bezos, a leading light in the digital, online world thanks to his disrupting of...

Related Articles

SOCIAL MEDIA

How to Keep Up with the Trends on Social Media

Shay Meinecke / April 6, 2016

ENTERTAINMENT , SOCIAL MEDIA

Beat the Bullies! How Celebrities React to Mean Tweets

Rob Nightingale / May 25, 2015

ANDROID , INTERNET

"My Child Is Being Bullied" – Check out These 7 Helpful Resources

Rob Nightingale / May 12, 2015

Latest Deals

I prefer a newspaper/magazine to online news. Part of it is habit but part of it is convenience. A newspaper can be folded until it can be read in tight quarters. If you drop it, the worst that happens is that somebody steps on it or the wind blows it all over. It does not need batteries/power to be read. Once read, it can be put to many other uses. It is recyclable.
Newspapers and their reporters have a code of ethics and supposedly check the facts/sources of their stories before publishing them. In comparison, it is Wild West as far as online news outlets are concerned. The only goal is to be the firstest with the mostest, damn the facts, full speed ahead.
Having said that, I know that hardcopy newspaper have no future. The one, big shortcoming of newspapers in today's world is that cannot deliver breaking news with the immediacy of electronic media. With society's lust for immediate gratification, newspapers just don't make it.

We liked this comment for various reasons. It details some of the advantages print media has over digital media, and in particular calls into question online journalists' obsession with being first rather than factual. The flipside of this coin is newspapers' in-built failure to deliver breaking news.

5 Great Multi-Source News Websites

READ MORE

We will be asking a new question tomorrow, so please join us then. *We Ask You* is a weekly column dedicated to finding out the opinions of MakeUseOf readers. We ask you a question and you tell us what you think. The question is open-ended and is usually open to debate. Some questions will be purely opinion-based, while others will see you sharing tips and advice, or advocating tools and apps to the MakeUseOf readership. This column is nothing without your input, all of which is valued.

Image Credit: [BarZaN] Qtr

0 COMMENTS

WRITE A COMMENT