Email Headers and Email Authentication Trifecta (DMARC, SPF, DKIM)

Disclaimer:
This article is written in good faith and is intended to provide general information about email headers and authentication systems such as DMARC, SPF, and DKIM. While every effort has been made to ensure the accuracy of the information provided, this article is not an authoritative guide or a substitute for professional advice. Email systems can vary widely, and readers are encouraged to consult official documentation, industry best practices, or a qualified professional for specific implementation and troubleshooting needs. The author and publisher disclaim any liability for errors, omissions, or outcomes resulting from the use of this information.

If an organization asks to find out the origination of an email that was sent to a Google Workspace account, the original unmodified email needs to be sent in for analysis. The email should **NOT** be forwarded in the usual manner as Gmail creates a new email with your information as the sender, and the original email's content is placed in the body of the forwarded message (either inline or as an attachment). For this whitepaper, the service GMail is used as an example but the same principle applies at Microsoft Outlook and other popular email providers.

Email Headers Analysis

Obtain the Original Email

To obtain the actual email with the original headers there are a few ways to do it:

Forward as Attachment

This method includes the entire original email, headers and all, as an attachment.

1. To forward an email as an attachment in Gmail:
2. Open Gmail for the account that received the email and select the email you want to forward.
3. Click the three-dot menu (⋮) in the top-right corner.
4. Choose Forward as attachment.
5. Compose your email, and the original email will be included as an .eml file.

Download the Email

If you want to retain headers for analysis or archiving, you can download the email as a .eml file:

1. Open the email in Gmail.
2. Click the three-dot menu (⋮).
3. Select Download message.

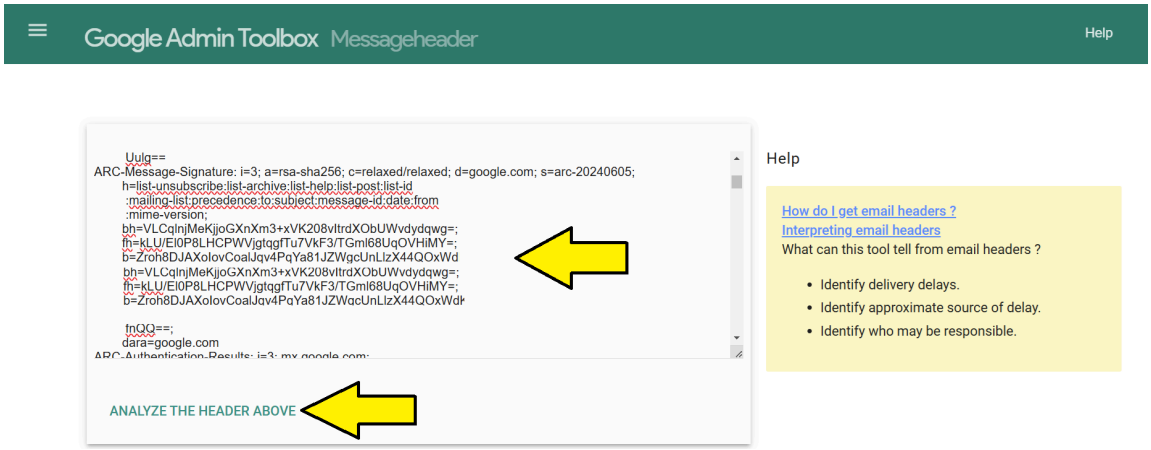
Inside Gmail

If you're analyzing headers from within an account that received the actual original email:

1. Open the email.
2. Click the three-dot menu (⋮).
3. Select Show original. This will display all the headers and the raw message body.
4. Copy the entire message to your clipboard.

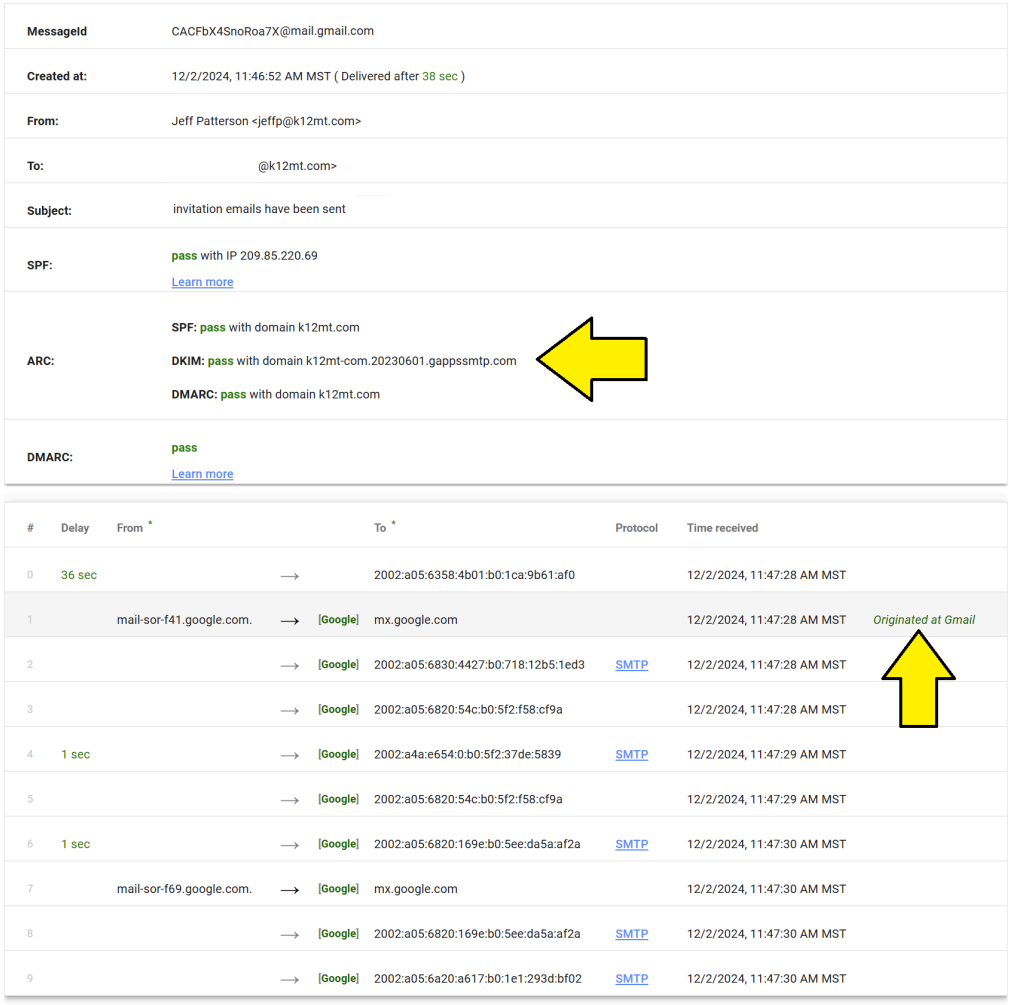
Generating the Email Headers Analysis

1. With either the .eml file of the original email downloaded or the email headers copied to a clipboard, head to https://toolbox.googleapps.com/apps/messageheader/
2. Either drag and drop the .eml file or paste the clipboard into the Header box.
3. Click on **ANALYZE THE HEADER ABOVE**.



4. Here's the essential information to look for:
    a. Email Security: If DMARC is fully in place, you should see all three SPF, DKIM, DMARC as green **passes.**
        i. **Reminder:** If you only have partial DMARC, you actually do not have DMARC. DMARC is basically an all or none system. There are staging to get parts in place but you are not protected by DMARC until all pieces are in place and working.
    b. There is a thread of movement of the email throughout the delivery system from the sender to the receiver. The first few lines are the most important one but the whole thread should be evaluated, especially if the DMARC has not been fully implemented yet and email could have been tampered with. You need to look at the originating email address.
        i. You need to consider the sources of your authorized email senders when looking at the reported sources.
            1. Domain Email Providers (Such as Google Workspace, Microsoft Outlook, etc)
            2. School Website Server Mailer (SendGrid, Twilio, etc, this is a very commonly overlooked one)
            3. Infinite Campus or other SIS (mg.infinitecampus.org, mailgun.org)
            4. Internal Exchange Email Servers (or hosted ones)
            5. Any other legitimate service that sends out email using your domain name and looks like it comes from your domain.

c. An example of an actual email (with information obfuscated for security) is provided below.



MessageId	CACFbX4SnoRoa7X@mail.gmail.com
Created at:	12/2/2024, 11:46:52 AM MST (Delivered after 38 sec)
From:	Jeff Patterson <jeffp@k12mt.com>
To:	@k12mt.com>
Subject:	invitation emails have been sent
SPF:	**pass** with IP 209.85.220.69 Learn more
ARC:	**SPF: pass** with domain k12mt.com **DKIM: pass** with domain k12mt-com.20230601.gappssmtp.com **DMARC: pass** with domain k12mt.com
DMARC:	**pass** Learn more

#	Delay	From *		To *	Protocol	Time received	
0	36 sec		→	2002:a05:6358:4b01:b0:1ca:9b61:af0		12/2/2024, 11:47:28 AM MST	
1		mail-sor-f41.google.com.	→ [Google]	mx.google.com		12/2/2024, 11:47:28 AM MST	*Originated at Gmail*
2			→ [Google]	2002:a05:6830:4427:b0:718:12b5:1ed3	SMTP	12/2/2024, 11:47:28 AM MST	
3			→ [Google]	2002:a05:6820:54c:b0:5f2:f58:cf9a		12/2/2024, 11:47:28 AM MST	
4	1 sec		→ [Google]	2002:a4a:e654:0:b0:5f2:37de:5839	SMTP	12/2/2024, 11:47:29 AM MST	
5			→ [Google]	2002:a05:6820:54c:b0:5f2:f58:cf9a		12/2/2024, 11:47:29 AM MST	
6	1 sec		→ [Google]	2002:a05:6820:169e:b0:5ee:da5a:af2a	SMTP	12/2/2024, 11:47:30 AM MST	
7		mail-sor-f69.google.com.	→ [Google]	mx.google.com		12/2/2024, 11:47:30 AM MST	
8			→ [Google]	2002:a05:6820:169e:b0:5ee:da5a:af2a	SMTP	12/2/2024, 11:47:30 AM MST	
9			→ [Google]	2002:a05:6a20:a617:b0:1e1:293d:bf02	SMTP	12/2/2024, 11:47:30 AM MST	

Understanding the Email Headers Analysis

With all the information gathered, one would look for:

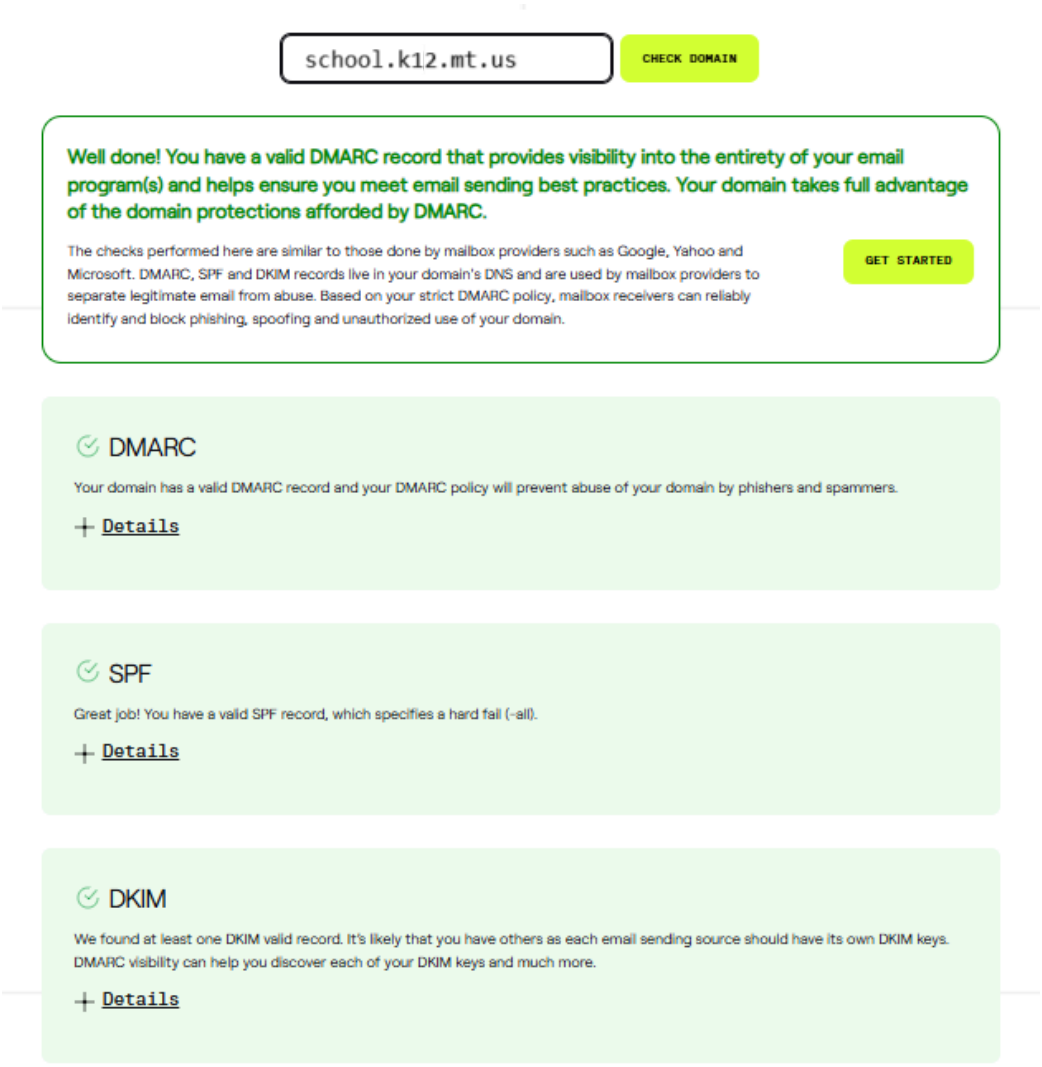
1. If DMARC is fully in place, email is only delivered from authorized servers, and is signed to have not been altered in transition. Thus, the only way the email is delivered is if the email was sent using the user's credentials and using sanctioned services. So this means, it is very extremely likely that the email account itself was compromised somehow.
    a. Look at the account activity in your domain management (Google Admin/Microsoft Admin).
    b. Has 2FA been enabled for the account user?
    c. Does the user practice common security practices?
    d. Does the user work on infected machines that may be monitoring the user's activity?

    e. Does the user have suspicious browser extensions or VPN software or free games/software that may be hiding data harvesting actions?
2. However, if DMARC is not in place, there are more factors to consider:
    1. Where did the email originate? Was it at a trusted source such as listed in the domain's SPF server list (authenticated email senders) such as Google, Infinite Campus.
        a. If the email originated at Google or other authorized servers, that means the account that sent that email was logged into via Gmail and sent from there. Look at the user's account activity to look at history and locations of sign-ins and see if there's suspicious activity there. Other possibility is a compromised user machine but not nearly as common.
        b. If the email originated from IPs or servers or domains located in foreign countries, especially ones in South-East Asia, Russia, North Korea, Africa, Eastern Europe, Central or South America. Basically, any countries that the user did not recently travel to. This email is most likely a spoofed email sent using the user's account name but since there is no DMARC in place, email delivery systems do not know whether this is legitimate or not and delivers the email and lets the spam filters try to do the job.
    2. May the email have been altered in transition? This is unlikely but definitely possible. This would be beyond the scope of all but the most dedicated administrators and not discussed in depth here.

Understanding the Email Authentication Trifecta

Email is generally secured by having three different systems working together. Those three systems are called SPF, DKIM, and DMARC. If any part of the three systems is not fully implemented or configured incorrectly, DMARC will not be working at all and at worse, you may be actually rejecting legitimate emails. Also, an implemented DMARC system will massively increase your domain's email standing with email providers and make your domain emails far less likely to be marked as spam or suspicious. To be clear, DMARC is about other email providers trusting YOUR emails. Your DMARC does not impact incoming email from other domains but your outgoing email using your domain name.

A good way to quickly check your DMARC standing is to enter your full domain name at this link: https://dmarcian.com/domain-checker/



These protocols work together as follows:

- SPF (Sender Policy Framework): Verifies if the sender's IP address/domain name is authorized to send emails on behalf of a domain.
- DKIM (DomainKeys Identified Mail): Adds a cryptographic signature to verify that the email content has not been altered in transit and is from the claimed domain.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance): Enforces policies and provides reporting based on the results of SPF and DKIM checks.

SPF

This is the hardest part of the DMARC system and the one most prone to problems and overlooking. You would need to evaluate every single legitimate email sender that sends email as your domain email system. Consult each system's

documentation on what needs to be configured to ensure they work with DMARC. Some systems may just simply need an IP/domain name excluded, others need DKIM records or CNAME aliases records built to ensure their delivery.

Sample SPF TXT Record (use -all or ~all, never ?all): **include:_spf.google.com include:mg.infinitecampus.org ~all**
Note: There is lots of documentation out there on proper SPF records generation - there are a lot of little details to be aware of if you have a complex organization. There should be only one SPF record.

DKIM

DKIM is a signature that is added to each email before it is sent in transition. If any part of the email is changed, the DKIM signature will not match the email contents and the receiver's email provider should realize that the email has been altered and either reject or warn the recipient.

To implement this, you would go to your domain email management such as Google Admin or Microsoft Admin and generate DKIM records there. You then would add these DKIM records as TXT records to your domain external DNS records. With these, it is very important to make sure the DKIM selector name generated by your domain management is entered correctly in your DNS records.

DKIM Record Name: **big-email._domainkey.example.com**
Sample DKIM Record: **v=DKIM1; p=76E629F05F709EF665853333EEC3F5ADE69A2362BECE40658267AB2FC3CB6CBE**

Note: There can be many DKIM records including aliases to other domain records, especially for website senders or other third party services.

DMARC

DMARC is simply a record telling email providers what to do when they get suspicious emails from you that are not fully compliant with your DMARC records. None means do nothing. Quarantine means mark the email as suspect/spam and act accordingly. Reject means don't deliver the email at all and send a report to this email address in the next reporting cycle. All DMARC analysis and reporting from email providers will be sent to this email address on a regular basis. Either use a stand-alone email account for this and check it occasionally or set up a filtering inbox to receive those reports.

Sample DMARC TXT record: **v=DMARC1; p=reject; rua=mailto:dmarc@school.k12.mt.us**

Note: There should be only one DMARC record.

Tips for DMARC Migration

Set your DMARC record to NONE to start with. Check the DMARC email account in the DMARC record regularly and run a DMARC Log analysis on these records to look for errors

Slowly add DKIM and SPF records in. Check the DMARC reports in the email account again and adjust SPF and DKIM records until all legitimate sources have been added in. Once you have evaluated all services used by your organization and incorporated them into the DMARC record, and you are confident in your DMARC setup, you may be ready to change the DMARC policy from NONE to either QUARANTINE or, preferably, REJECT.

Some fantastic documentation

https://dmarcly.com/blog/what-is-an-spf-record-and-how-does-it-work-spf-record-explained
https://dmarcian.com is a source of fantastic documentation.
https://emailsecurity.fortra.com/blog/pros-cons-dmarc-reject-vs-quarantine
https://www.learndmarc.com/ - fantastic game for email but very technical.[1]

[1]Documentation Version 2024-12-02