Email Forensics By Kevin Harianto

1. Sent an email from personal to sheridan:

Graphical user interface, text, application

Description automatically generated

^The above shows that the sheridan account had received an email from personal.

1. Analyzing the header:

Graphical user interface, text, letter

Description automatically generated

^part of header data

Table

Description automatically generated

^Header data analyzed with the same subject proving that it is the same email being analyzed.

Text, Word

Description automatically generated

^Analyzing the email headers found.

Graphical user interface, text, application

Description automatically generated

SPF and DKIM header analysis:

DMARC is a domain-based Message Authentication, Reporting and Conformance. This basically means that it protects email senders and recipients from spam, spoofing and phishing. (DMARC) This is accomplished by allowing an organization to publish a policy that defines an email authentication practice and provides the instructions for the email servers on how to enforce these authentication processes. (DMARC) This header works by relying on SPF and DKIM standards for email authentication as well as utilizing the domain name system. (DMARC)

Text

Description automatically generated SPF and DKIM information is highlighted in the MX lookup as SPF allows the senders to define what IP addresses are allowed to send mail for a particular domain. DKIM provides the encryption key and digital signature to verify that an email message was not faked or altered, while DMARC as previously described unifies this authentication mechanism into a common framework and allow the domain owners to take control on how the authentication process would react. (DMARC)

From the list of headers:

Text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

…

Graphical user interface

Description automatically generated with low confidence

ARC-Seal Email Header: The ARC header is used to preserve email authentication results while also verifying the identity of email links (hops) that move the message towards the destination. (ARC) The Seal area is basically the signature that includes the message header information as well as the results of the authentication that occurred from DMARC. (ARC)

ARC-Message-Signature: This signature takes a snapshot of the message header inforation, this includes the to, from, subject and body. (ARC)

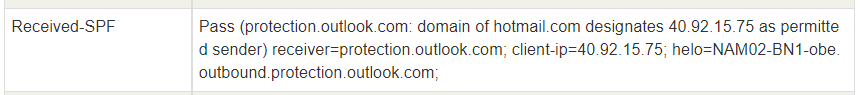
ARC-Authentication-Results: Contains the email authentication results such as the SPF, DKIM and DMARC.

Authentication-Results:



^SPF, also known as sender policy franework is an email authentication technique to prevent spammers from sending on behalf of the victims domain. Because it is pass, This means that the email sent from the source was authenticated to be from an allowed source and not from a spammer sending on behalf of the source. Because the authentication results for DKIM and DMARC was pass as well the action took was none and it allowed the email to be sent sucessfully. This is due to the fact that DKIM provides the validation for the source with the digital signature and DMARC being the unifiyng authentiation standard. The header showed that it was from the email provider source as well as the reason being 100 due to the fact that it passed every authentication mechanism. (DMARC)

Received-SPF:



Due to the fact that the header was passed means that the source (personal email) was permitted to send the email towards the school’s without getting blocked as it verified that the email was authentic. This also means that the email was able to be read by the schools’s email without being blocked for potential hazards with the source authenticated. (SPF)

DKIM-Signature:

Text

Description automatically generated

^This header reveals which domain was used to sign the email in the encryption process. (DKIM) This is validated through the DNS query for the public key in the domain. Because it was considered validated, this reveals that the destination was from hotmail.com domain due to the signature matching. In terms of the relevant codes for DKIM, V stands for the version, a is the digital signature method with it being RSA encryption. This also used sha256 for encrypting the key, and d is the domain on which it was validated to be.

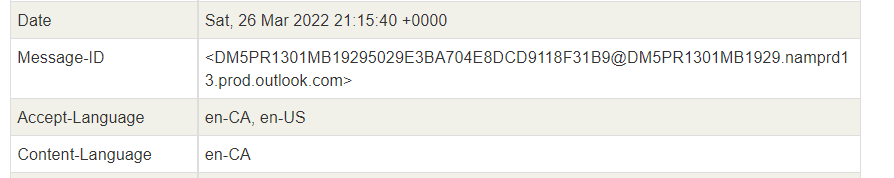
From, To, Subject Headers:

Graphical user interface, text, application

Description automatically generated

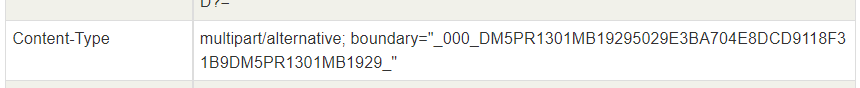
^The from header Displays who the message is from, in this case the email was sent from the person account which is shown here. The to header shows to whom the email was addressed to, in this case being the school’s email. The Subject and Thread-Topic header being the topic created by the personal email, in this case being called testing email as that was the topic that was created by the personal email.

Date, message-ID, Language Headers:



^Date was when the email was composed, in this case it was composed at Saturday March 26th. Message-ID header is the unique string assigned by the system towards the email in this case it is being shown here. The language header is the languag in which the message is in.

Content-Type Header:



^This header shows that the multipart/alternative is used when the same information is presented in different body parts in different forms. In this case it is being ordered by increasing complexity. (content) With the boundary being shown which areas the same information is presented at for the message. (content)

MIME Header:

Graphical user interface, application

Description automatically generated

^This header is the nultipurpose internet mail extension as they allow for flexibility in how the reader would like to view the message. (content)

Return-Type Header:

A picture containing table

Description automatically generated

^This header shows the email address for the return mail. This is where the reply will go to when the message is sent beack.

1. Responding back to the email:

Graphical user interface, text, application, chat or text message, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

^These screenshots show that the email was sucessfully replied back from the school’s email.

Text, letter

Description automatically generated

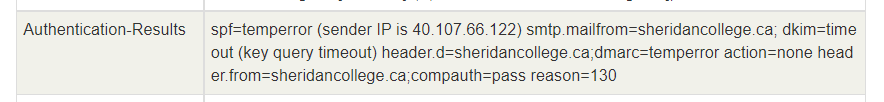
^Viewing the message’s header information responded back by the school’s email.

Analyzing the received headers:

Graphical user interface, text, application

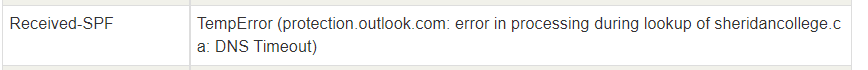
Description automatically generated

NOTE: Because we didn’t go over ARC I will not be covering it here like last time, even though the concept is the same. This is also proven to be the case with the slides showing the main headers to explain.



^This header shows the entire results for the authentication, because the spf is temperror this forces the email server to return a temporary failure. It would also prompt the user to make another attempt to resend the email. This also usually meant that the DNS had timed out when the check was taking place. This is short lived and a retry will yield a pass. (err) From portion of the header being shown that the email response was sent for school’s email, and the DKIM for the key signature was also timed out. With these errors generating this makes the DMARC header become and overall temporar error as well however the authentication still passed as there was no evidence that the email was sent from a malicious actor.

Received-SPF header:



^This overall header proved my hypothesis on how the error most likely originated from the DNS timeout during the lookup of the school’s email domain, generated from the security section provided by the personal email’s server vendor -in this case being outlook.com-.

Text

Description automatically generated

^Because DKIM-Signature header is the header responsible for revealing whch domain was used to sign the email in the encryption process as explained previously, this header reveals that it was using the same method like the school’s email server uses. This being version 1, and the a for authentication being RSA digital signature with sha256 encryption to prevent man in the middle attacks and hiding the message contents from attackers. (DKIM) This also showed that the domain was proved to be sheridan college’s mail server -d=sheridancollege.ca-. This also meant that the user did infact respond using the schools email towards the personal account.

From, To, Subject, Topic Headers:

Graphical user interface, text, application

Description automatically generated

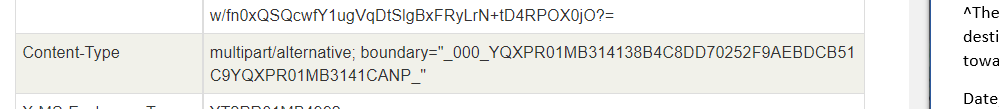
^The from header showing that the reply was sent from school’s email. To header being shown that the destination is towards the personal email back. The Subject header being revealed that it is a reply towards the testing email while the thread topic -the original one- still being the same email.

Date, Message-ID Headers:



^Date header being shown that the reply was composed of on Sunday March 27th. While the message-ID header being shown to be unique to the one previously shown as they are a unique string assigned by the mail system for when it was first created.

Content-Type header:



^This header being shown to be the same one as previously discussed showed that the content was generated as well in the same format with the information being presented in different body parts in different forms as the boundary was being shown to be defined on where the message can be displayed in terms of limits.

Return-Path Header

Table

Description automatically generated

^This header shoed that the reply sent from the personal email travels back to the schools email.

Way the email went from source to destination:

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generated

^First hop for the reply message to go back towards the sheridan email is used with mapi. This is a client protocol that allows accessto their mailbox themselves with their outlook email account. (mapi)

Table

Description automatically generated with low confidence

^2-5 hops showed that the message went throughout the Microsoft SMTP servers right after communicating with the email client account to send the reply. SMTP is an application used by mail servers to deal with mail going between email senders and receivers, which is why this protocol -simple mail transfer protocol- is dominant -used- during the travel towards the sheridan’s email from the personal email. (smtp)

Graphical user interface, text, application

Description automatically generated

^The final hop is used with https. This is criticial in providing security in email and it is used to encrypt streams of network traffic between client and servers. This is mainly used to encrypt webmail messages and it allows the message to stay hidden from packet sniffers and threat agents from looking into your message when you open it. (https) This is also used in almost all email exchanges between servers and users due to this enhanced security with the transition of network traffic being encrypted using TLS. (https)

Looking up the domain’s MX record:

Graphical user interface, text, application

Description automatically generated

^Looking into the google.ca domain and looking into the MX record.

Graphical user interface, text, application, chat or text message

Description automatically generated

^MX records. These are DNS records necessary for delivering email to your addresses as these tell which servers accept incoming main for the domain and thus where it should be routed to. This means that the MX record points to the correct email location to send the message to. (MX)

Graphical user interface, application

Description automatically generated

^SPF and DMARC are both used in email authentication. SPF is the sender policy framework that restricts who can send emails from the domain. This also prevents domain spoofing. (auth) DMARC is known as Domain-based Message Authentication, Reporting and Conformance. This means that it utilizes the SPF and DKIM -which ensures that the content of email remains trusted- with a consistent set of policies and ensures that the transitions are compatible and streamlined. (auth) With this information in mind, these records are a means to authentical the main sever and to prove to the internet service provider, and other clients that the senders are truly authorized to send email. (proof)

References

<https://www.sparkpost.com/resources/email-explained/dmarc-explained/> (DMARC)

<https://prodmarc.com/knowledge/arc-headers/#:~:text=What%20is%20ARC%3F,like%20SPF%2C%20DKIM%2C%20and%20DMARC> (ARC)

<https://www.dmarcanalyzer.com/spf/> (SPF)

<https://www.dmarcanalyzer.com/dkim/dkim-signature/#:~:text=The%20DKIM%20signature%20will%20be,sent%20with%20this%20DKIM%20signature>. (DKIM)

<https://docs.microsoft.com/en-us/previous-versions/office/developer/exchange-server-2010/aa493937(v=exchg.140)#:~:text=The%20multipart%2Frelated%20content%20type,not%20contained%20within%20the%20message>. (content)

<https://www.duocircle.com/content/spf-permerror/spf-temperror#:~:text=An%20SPF%20temperror%20forces%20the,sending%20a%204xx%20status%20code>. (err)

<https://docs.microsoft.com/en-us/exchange/clients/mapi-mailbox-access?view=exchserver-2019#:~:text=MAPI%20is%20a%20client%20protocol,their%20mailbox%20in%20Exchange%20mode>. (mapi)

<https://sendgrid.com/blog/what-is-an-smtp-server/#:~:text=SMTP%20stands%20for%20Simple%20Mail,between%20email%20senders%20and%20receivers>. (smtp)

<https://www.techtarget.com/searchsecurity/answer/What-are-the-most-important-email-security-protocols> (https)

<https://help.dreamhost.com/hc/en-us/articles/215032408-What-is-an-MX-record-> (MX)

<https://www.csoonline.com/article/3254234/mastering-email-security-with-dmarc-spf-and-dkim.html> (auth)

<https://www.smartertools.com/blog/2019/04/09-understanding-spf-dkim-dmarc> (proof)