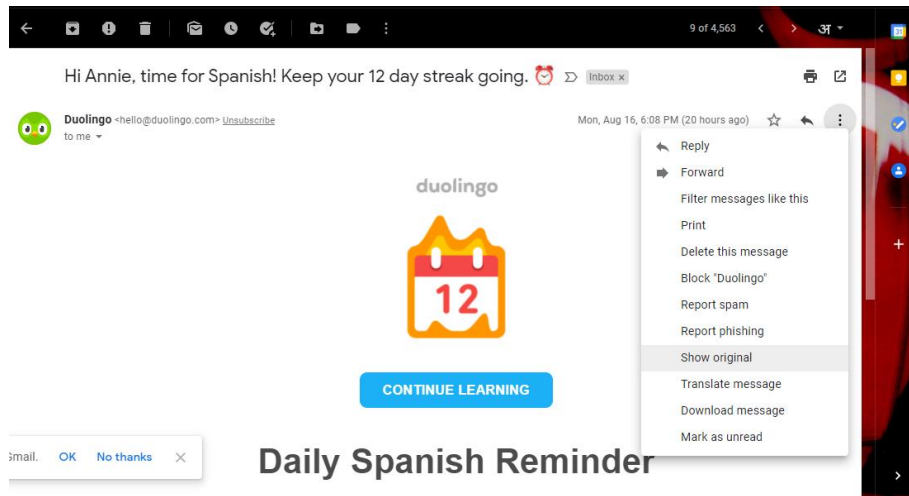


OUTSTANDING – 2

Using google apps toolbox to review email headers

Step-1: Open the e-mail which you want to investigate and check for its header.



Step-2: Coping the original form of the email to further analyze.

Original Message

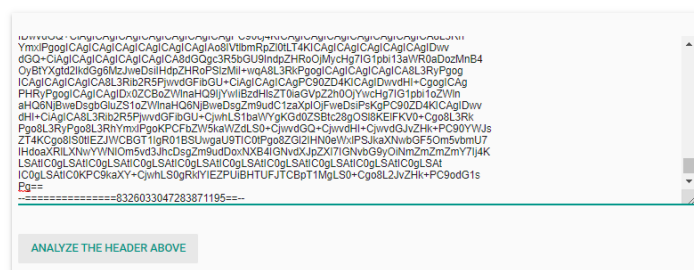
Message ID	<0100017b4ef81b16-fbc2cb5e-803c-4b1c-9690-fd9693293a95-000000@email.amazonses.com>
Created at:	Mon, Aug 16, 2021 at 6:08 PM (Delivered after 1 second)
From:	Duolingo <hello@duolingo.com>
To:	n.anniesupriya@gmail.com
Subject:	Hi Annie, time for Spanish! Keep your 12 day streak going. 📅
SPF:	PASS with IP 54.240.37.56 Learn more
DKIM:	'PASS' with domain duolingo.com Learn more
DMARC:	'PASS' Learn more

[Download Original](#)

[Copy to clipboard](#)

Step-3: Analyzing the message header by using Google Admin Toolbox.

Google Admin Toolbox Messageheader



Example of what the output may look like

Subject:	Messages this week with: Board games, Finance and others
SPF:	pass
DKIM:	pass
DMARC:	pass

Step-4: Now we have vital information for diagnosing the email problems. You can trace the emails direct path and sources that can help troubleshoot breakpoints in the emails path.

toolbox.googleapps.com/apps/messageheader/analyzeheader

MessageId	0100017b4ef81b16-fbc2cb5e-803c-4b1c-9690-fd9693293a95-000000@email.amazonses.com
Created at:	8/16/2021, 6:08:07 PM GMT+5:30 (Delivered after 1 sec)
From:	Duolingo <hello@duolingo.com>
To:	n.anniesupriya@gmail.com
Subject:	Hi Annie, time for Spanish! Keep your 12 day streak going. 🇪🇸
SPF:	pass with IP 54.240.37.56 Learn more
DKIM:	pass with domain duolingo.com pass with domain amazonses.com Learn more
DMARC:	pass Learn more

#	Delay	From *	To *	Protocol	Time received
0	1 sec	a37-56.smtp-out.amazonses.com.	→ [Google] mx.google.com	ESMTPS	8/16/2021, 6:08:08 PM GMT+5:30
1			→ [Google] 2002:a05:6214:d8a::	SMTP	8/16/2021, 6:08:08 PM GMT+5:30
2			→ [Google] 2002:a05:6520:2448:b029:11e:b85f:4a38	SMTP	8/16/2021, 6:08:08 PM GMT+5:30

We have basic information of the email including things such as from, to, date, subject, and MessageId. Mail transfer agents (MTAs) are used to manage this process; each time an email is sent or forwarded by an MTA, it's stamped with date, time, and recipient information.

Similarly, we are checking the email headers for other emails received.

Email-2: An email from Ola gaining basic information. Information of the sender's IP address, Domain name of the sender.

message	
Created at:	8/14/2021, 9:58:45 PM GMT+5:30 (Delivered after)
From:	Ola <noreply@olacabs.com> Using MIME-Lite 3.030 (F2.84; T1.38; A2.12; B3.13; Q3.13)
To:	n.anniesupriya@gmail.com
Subject:	We're almost there 1 day to go!
SPF:	pass with IP 150.129.232.34 Learn more
DKIM:	pass with domain olacabs.com pass with domain env.etransmail.com Learn more
DMARC:	pass Learn more

#	Delay	From *	To *	Protocol	Time received
0		email34.ncdelivery01.com.	→ [Google] mx.google.com	ESMTPS	8/14/2021, 9:58:45 PM GMT+5:30
1			→ [Google] 2002:a05:6602:48a::	SMTP	8/14/2021, 9:58:45 PM GMT+5:30
2			→ [Google] 2002:a05:6520:2448:b029:11e:b85f:4a38	SMTP	8/14/2021, 9:58:45 PM GMT+5:30

Email-3: Analyzing an email header from LinkedIn.

MessageId	885076532.3651772.1628496160380.JavaMail.app@lva1-app72754.prod.linkedin.com
Created at:	8/9/2021, 1:32:40 PM GMT+5:30 (Delivered after 3 sec)
From:	Adithyaas Ambalathil <invitations@linkedin.com>
To:	Annie Supriya <n.anniesupriya@gmail.com>
Subject:	Annie, please add me to your LinkedIn network
SPF:	pass with IP 2620:119:50c0:207:158 Learn more
DKIM:	pass with domain linkedin.com pass with domain mailb.linkedin.com Learn more
DMARC:	pass Learn more

#	Delay	From *	To *	Protocol	Time received
0	2 sec	mailb-hf.linkedin.com	→ [Google] mx.google.com	ESMTPS	8/9/2021, 1:32:42 PM GMT+5:30
1			→ [Google] 2002:a02:a117::	SMTP	8/9/2021, 1:32:42 PM GMT+5:30
2	1 sec		→ [Google] 2002:a05:6520:2448:b029:11e:b85f:4a38	SMTP	8/9/2021, 1:32:43 PM GMT+5:30

As per the analysis, there has been a 3 second delay in the delivery of the email. The protocols used are ESMTPS and SMTP. Domain name and the Ip address of the sender is provided.

Email-4: Gaining information about the email header from Coursera.

MessageId	07d0c1a9-26f3-41f5-8e3b-c19aaea063f4@atl1s11mta345.xt.local
Created at:	8/16/2021, 11:13:39 PM GMT+5:30 (Delivered after 4 sec)
From:	Coursera <Coursera@email.coursera.org>
To:	<n.anniesupriya@gmail.com>
Subject:	Trending this week at Coursera
SPF:	pass with IP 13.111.170.21 Learn more
DKIM:	pass with domain email.coursera.org Learn more
DMARC:	pass Learn more

#	Delay	From *	To *	Protocol	Time received
0	3 sec	mta6.email.coursera.org	→ [Google] mx.google.com	ESMTPS	8/16/2021, 11:13:42 PM GMT+5:30
1			→ [Google] 2002:a05:620a:138a::	SMTP	8/16/2021, 11:13:42 PM GMT+5:30
2	1 sec		→ [Google] 2002:a05:6520:2448:b029:11e:b85f:4a38	SMTP	8/16/2021, 11:13:43 PM GMT+5:30

Basic information of the sender is gathered by this analysis. Here there is a 4 second delay between when the email is sent and when it is released by the client.

Email-5: Email header analysis on email from Myntra.

MessageId	0.0.1A6.12E.1D792C47B37BBE8.0@transmail253.ncapp05.com
Created at:	8/17/2021, 12:05:02 AM GMT+5:30 (Delivered after 1 sec)
From:	Myntra <updates@myntra.com>
To:	n.anniesupriya@gmail.com
Subject:	Get Your Home Wear Without Leaving Your Home
SPF:	pass with IP 175.158.66.253 Learn more
DKIM:	pass with domain myntra.com Learn more
DMARC:	pass Learn more

#	Delay	From *	To *	Protocol	Time received
0	1 sec	transmail253.ncapp05.com.	→ [Google] mx.google.com	ESMTPS	8/17/2021, 12:05:03 AM GMT+5:30
1			→ [Google] 2002:a25:9cc4::	SMTP	8/17/2021, 12:05:03 AM GMT+5:30
2			→ [Google] 2002:a05:6520:2448:b029:11e:b85f:4a38	SMTP	8/17/2021, 12:05:03 AM GMT+5:30

There is a 1 second delay here when the message is received. The protocols used here are ESMTPS and SMTP.