EXPERIMENT-4

MHA Analyzer (Message Header Analyzer)

Aim:

To parse and interpret raw email headers—making them human-readable and helping investigators trace the email's route, source IP, delays, and authentication status.

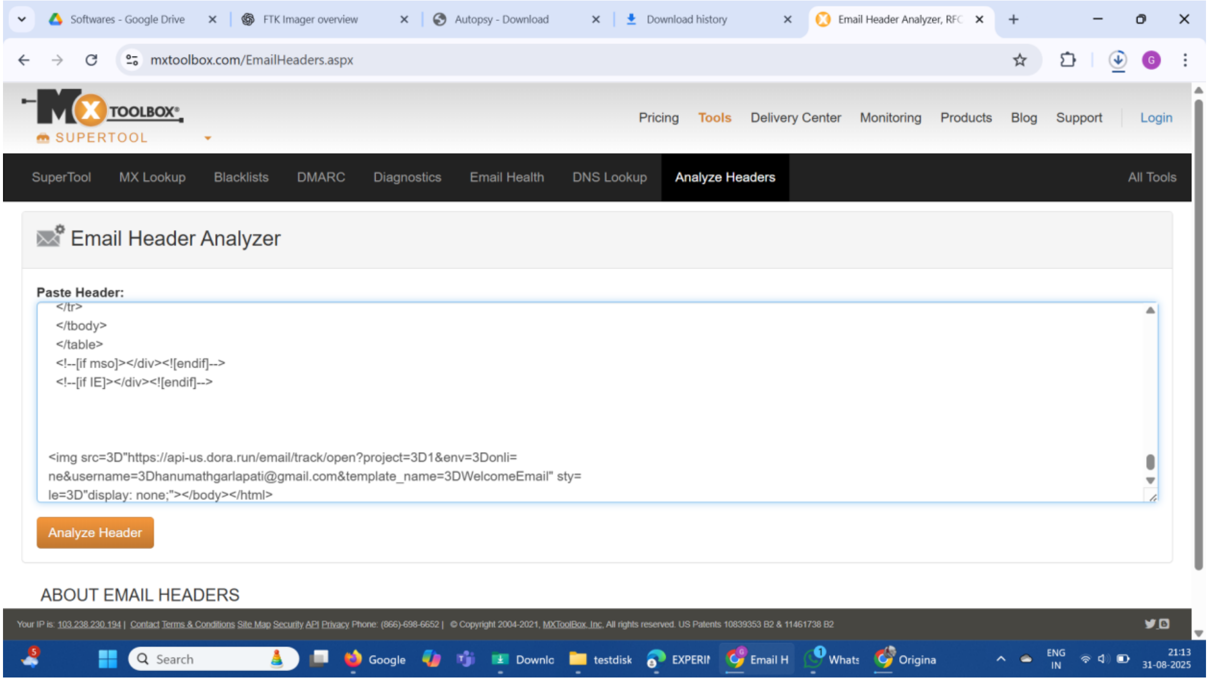
Tools / Features:

- A **Flask-based web tool** developed by lnxg33k that accepts pasted email headers and translates them into a clearer, visual format. It identifies hop delays, source IPs, and even the country of each hop.
- Available both as:
  - A **web-based standalone version** hosted at *mha.azurewebsites.net*
  - An **Outlook add-in** that integrates directly into Outlook/OWA to display header analysis inline

Process:

1. **Via Web**:
   a. Navigate to the MHA web app (e.g., mha.azurewebsites.net).
   b. Paste the raw email header text into the input field.
   c. The tool instantly parses and visualizes the routing path, delays, and metadata.
2. **Via Outlook Add-in**:
   a. Install the Message Header Analyzer add-in via Exchange Admin Center or Office Store
   b. Once enabled, open an email in Outlook or OWA and click the MHA icon to view the parsed header details inline.

OUTPUT:



Email Header Analyzer

Paste Header:

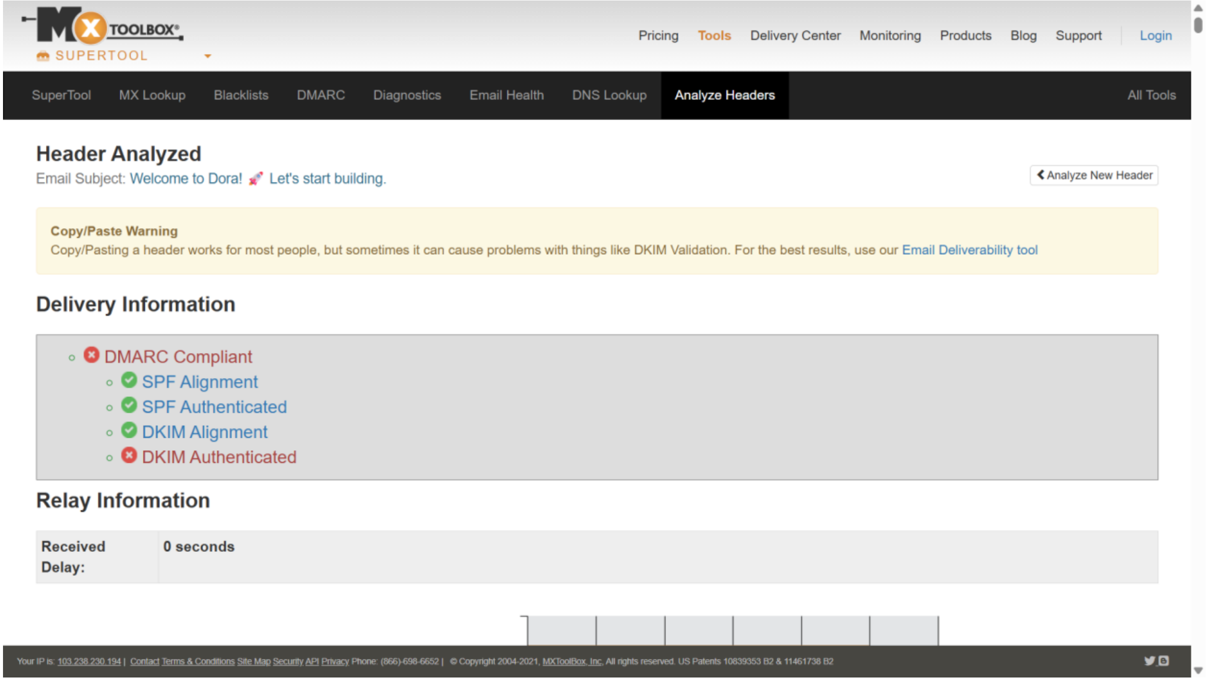
```
  </tr>
  </tbody>
  </table>
  <!--[if mso]></div><![endif]-->
  <!--[if IE]></div><![endif]-->



<img src=3D"https://api-us.dora.run/email/track/open?project=3D1&env=3Donli=
ne&username=3Dhanumathgarlapati@gmail.com&template_name=3DWelcomeEmail" sty=
le=3D"display: none;"></body></html>
```

ABOUT EMAIL HEADERS

Your IP is: 103.238.230.194 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2
Search
Google
Downlo
testdisk
EXPERI
Email H
Whats
Origina
ENG
IN
21:13
31-08-2025



Header Analyzed

Email Subject: Welcome to Dora! 🚀 Let's start building.

Copy/Paste Warning
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our Email Deliverability tool

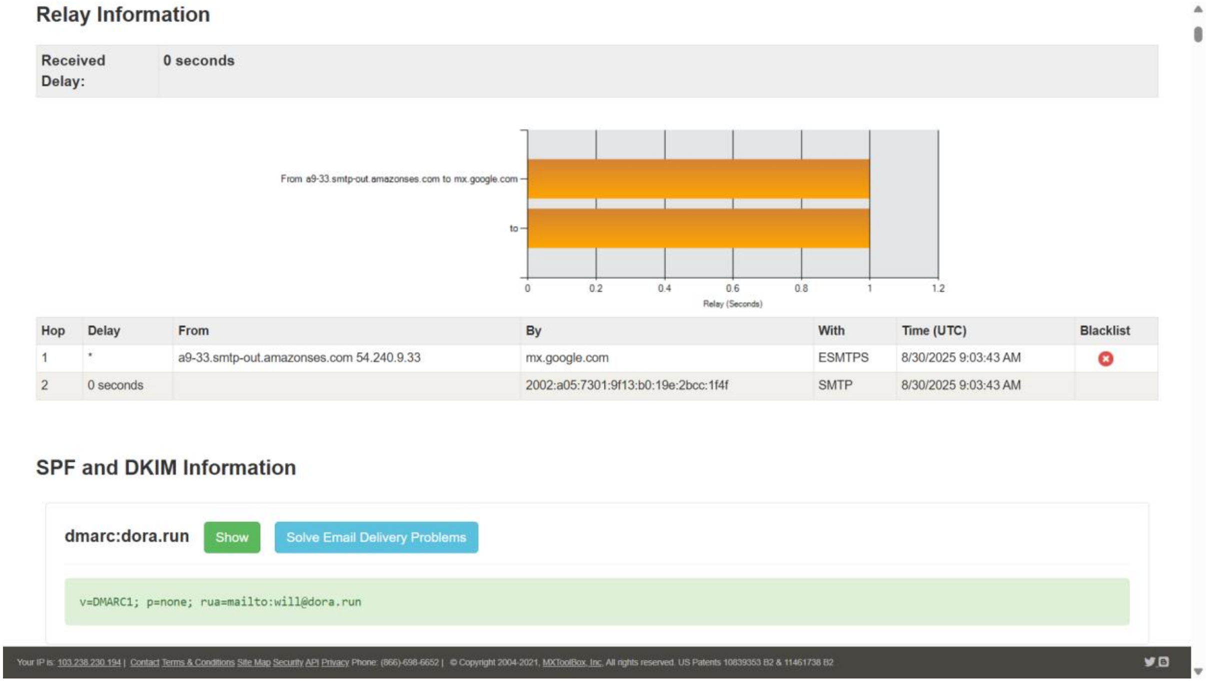
Delivery Information

- ✗ DMARC Compliant
  - ✓ SPF Alignment
  - ✓ SPF Authenticated
  - ✓ DKIM Alignment
  - ✗ DKIM Authenticated

Relay Information

Received Delay:	**0 seconds**

Your IP is: 103.238.230.194 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2



From a9-33.smtp-out.amazonses.com to mx.google.com
to
0
0.2
0.4
0.6
0.8
1
1.2
Relay (Seconds)

Relay Information

Received Delay:	0 seconds

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	a9-33.smtp-out.amazonses.com 54.240.9.33	mx.google.com	ESMTPS	8/30/2025 9:03:43 AM	✖
2	0 seconds		2002:a05:7301:9f13:b0:19e:2bcc:1f4f	SMTP	8/30/2025 9:03:43 AM	

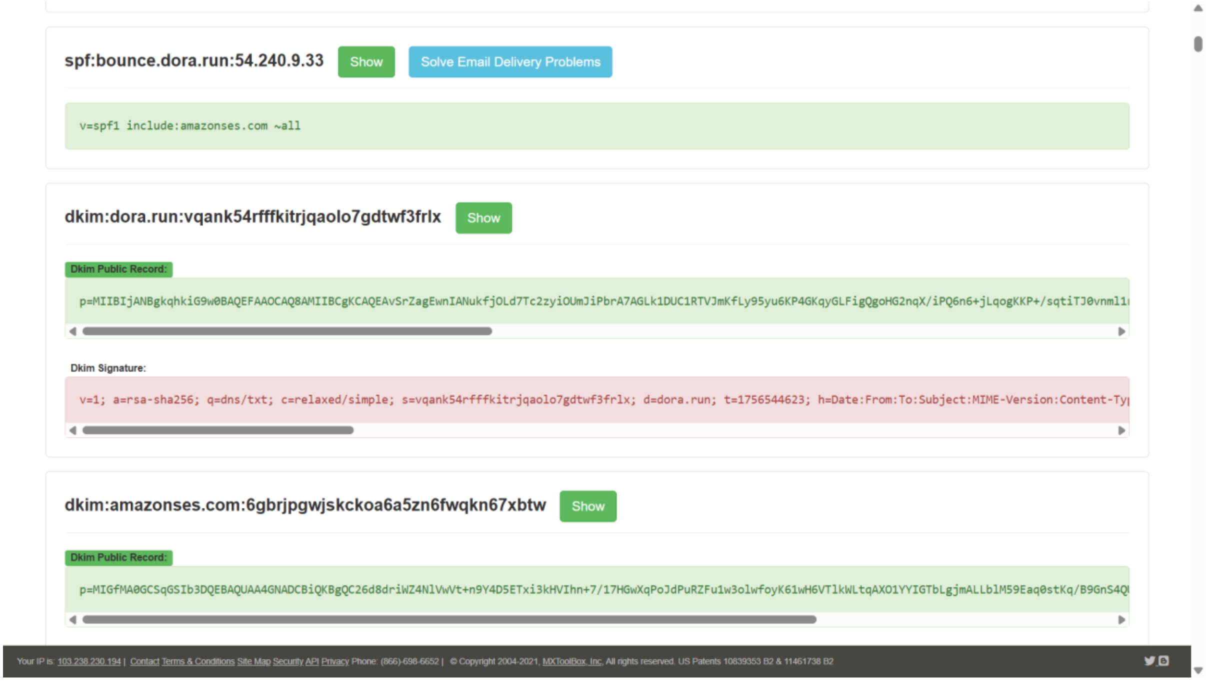
SPF and DKIM Information

dmarc:dora.run

Show
Solve Email Delivery Problems

```
v=DMARC1; p=none; rua=mailto:will@dora.run
```

Your IP is: 103.238.230.194 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc, All rights reserved. US Patents 10839353 B2 & 11461738 B2



spf:bounce.dora.run:54.240.9.33

```
v=spf1 include:amazonses.com ~all
```

dkim:dora.run:vqank54rfffkitrjqaolo7gdtwf3frlx

Dkim Public Record:

```
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvSrZagEwnIANukfjOLd7Tc2zyiOUmJiPbrA7AGLk1DUC1RTVJmKfLy95yu6KP4GKqyGLFigQgoHG2nqX/iPQ6n6+jLqogKKP+/sqtiTJ0vnml1
```

Dkim Signature:

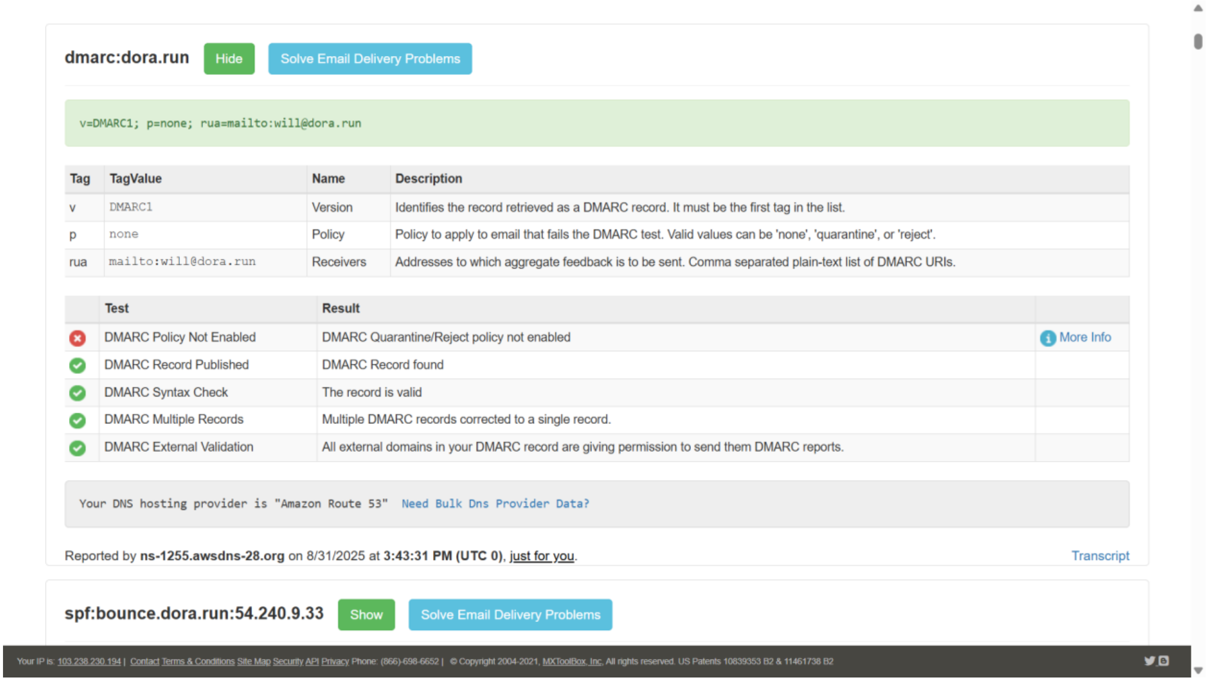
```
v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=vqank54rfffkitrjqaolo7gdtwf3frlx; d=dora.run; t=1756544623; h=Date:From:To:Subject:MIME-Version:Content-Ty
```

dkim:amazonses.com:6gbrjpgwjskckoa6a5zn6fwqkn67xbtw

Dkim Public Record:

```
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC26d8driWZ4NlVwVt+n9Y4D5ETxi3kHVIhn+7/17HGwXqPoJdPuRZFu1w3olwfoyK61wH6VTlkWLtqAXO1YYIGTbLgjmALLblM59Eaq0stKq/B9GnS4Q
```

Your IP is: 103.238.230.194 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc, All rights reserved. US Patents 10839353 B2 & 11461738 B2



dmarc:dora.run

```
v=DMARC1; p=none; rua=mailto:will@dora.run
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
rua	mailto:will@dora.run	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.

	Test	Result	
✗	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	ℹ More Info
✓	DMARC Record Published	DMARC Record found	
✓	DMARC Syntax Check	The record is valid	
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	

```
Your DNS hosting provider is "Amazon Route 53"  Need Bulk Dns Provider Data?
```

Reported by **ns-1255.awsdns-28.org** on 8/31/2025 at **3:43:31 PM (UTC 0)**, just for you.

spf:bounce.dora.run:54.240.9.33

Your IP is: 103.238.230.194 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc, All rights reserved. US Patents 10839353 B2 & 11461738 B2

Result:

- The raw email headers are transformed into a structured, user-friendly format.
- You can easily see the hop-by-hop journey of the email, including timestamps, delays, source IPs, and countries—helpful for tracking and forensic analysis.
- In Outlook, this analysis is accessible directly within the email interface through the add-in.