EXPERIMENT--04

Aim:

To use a Mail Header Analyzer (MHA) to trace an email's origin and verify its authenticity by examining its header for signs of spoofing.

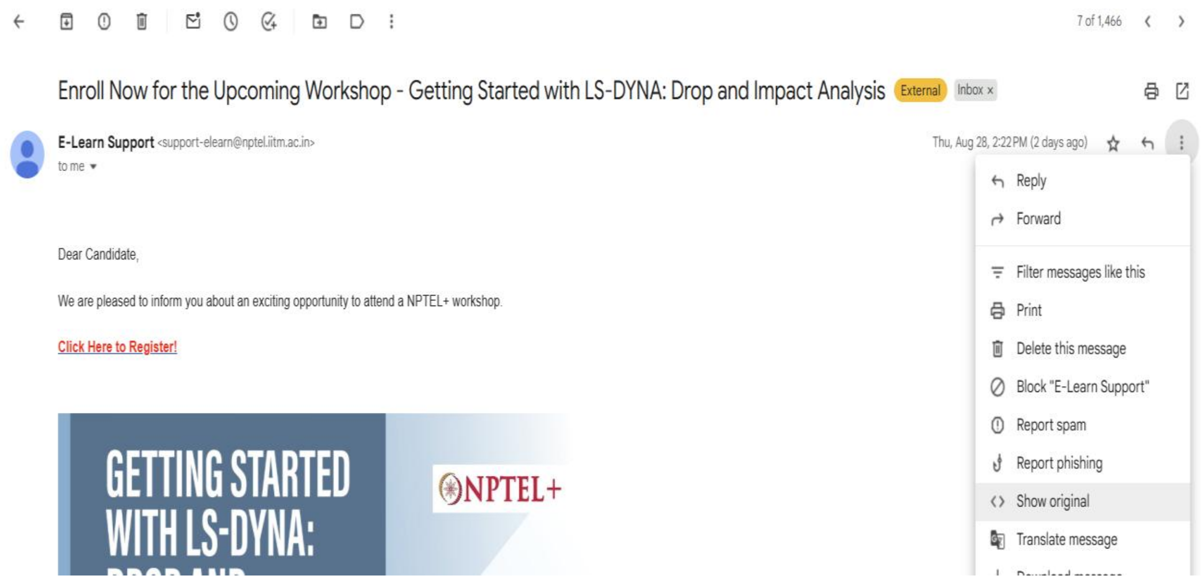
Tools Used:

- Mail Header Analyzer (online tool or built-in)
- Web browser
- Sample email with full header

Procedure:

1. Open the email and access its full header information (available in most email clients under “Show Original” or “View Source”).
2. Copy the entire email header text.
3. Open a Mail Header Analyzer tool (e.g., MxToolbox MHA or Google Apps Toolbox).
4. Paste the copied email header into the analyzer's input field.
5. Run the analysis to extract details such as the sender's IP address, mail servers used, and authentication results.
6. Check for SPF, DKIM, and DMARC authentication results to detect possible spoofing.
7. Compare the originating IP address with the claimed sender domain to verify legitimacy.

Outputs:



Enroll Now for the Upcoming Workshop - Getting Started with LS-DYNA: Drop and Impact Analysis External Inbox ×

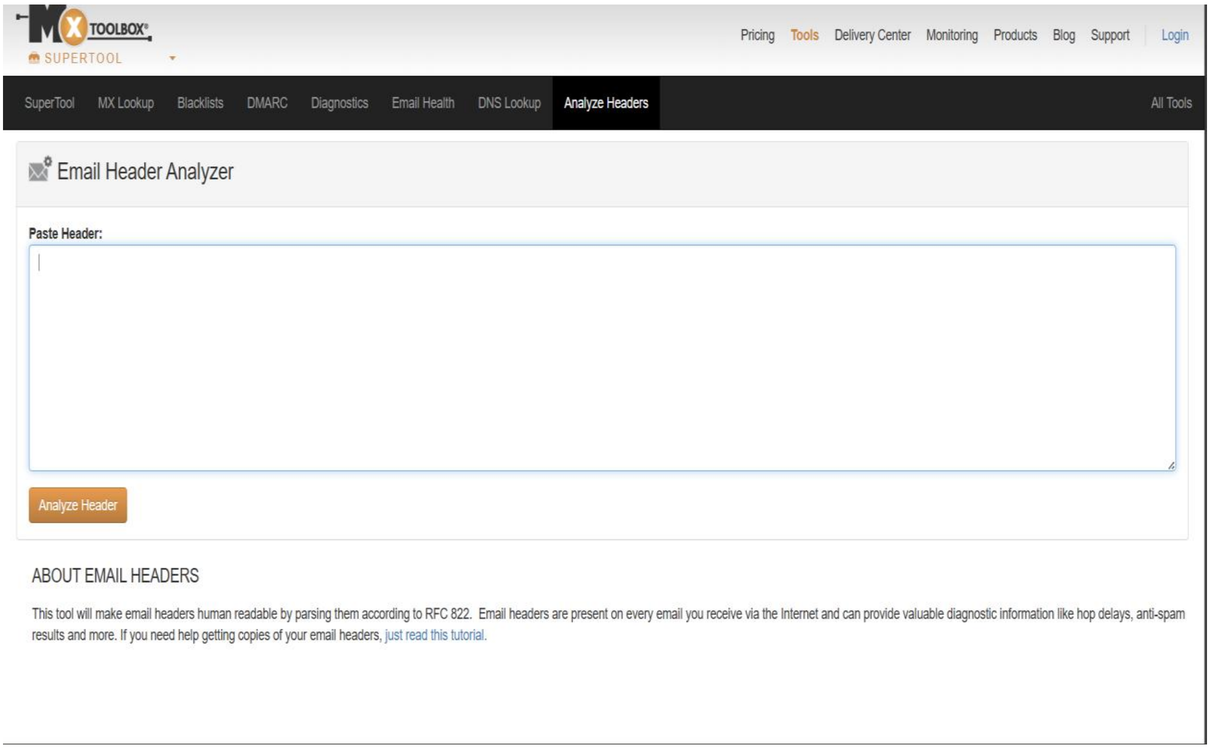
E-Learn Support <support-elearn@nptel.iitm.ac.in>
to me

Thu, Aug 28, 2:22 PM (2 days ago)

Dear Candidate,

We are pleased to inform you about an exciting opportunity to attend a NPTEL+ workshop.

Click Here to Register!

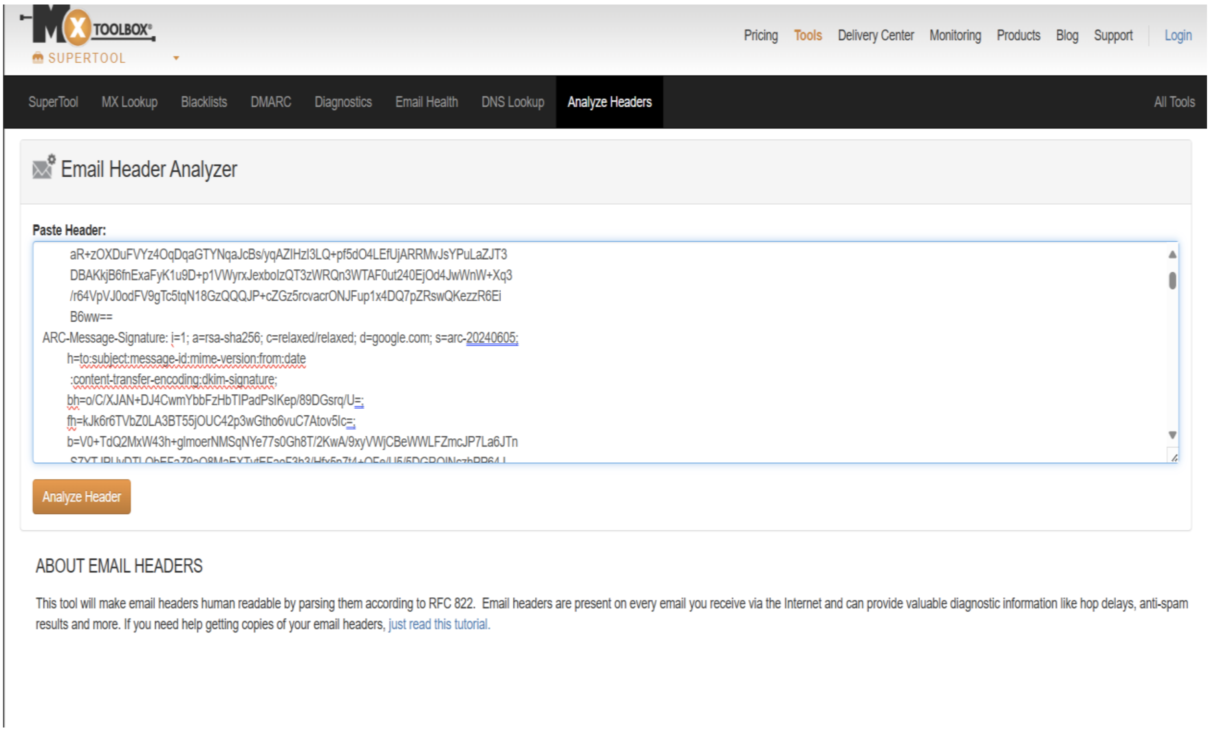


Email Header Analyzer

Paste Header:

ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, just read this tutorial.



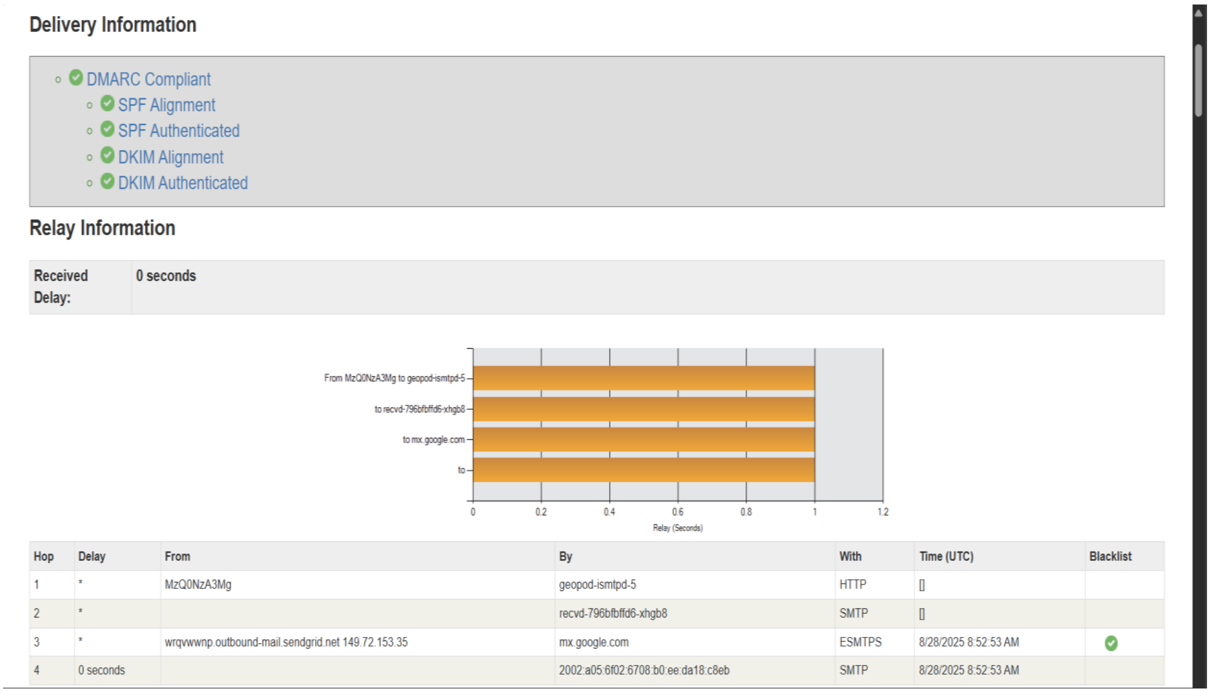
Email Header Analyzer

Paste Header:

```
        aR+zOXDuFVYz4OqDqaGTYNqaJcBs/yqAZIHzI3LQ+pf5dO4LEfUjARRMvJsYPuLaZJT3
        DBAKkjB6fnExaFyK1u9D+p1VWyrxJexboIzQT3zWRQn3WTAF0ut240EjOd4JwWnW+Xq3
        /r64VpVJ0odFV9gTc5tqN18GzQQQJP+cZGz5rcvacrONJFup1x4DQ7pZRswQKezzR6Ei
        B6ww==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
       h=to:subject:message-id:mime-version:from:date
        :content-transfer-encoding:dkim-signature;
       bh=o/C/XJAN+DJ4CwmYbbFzHbTIPadPsIKep/89DGsrq/U=;
       fh=kJk6r6TVbZ0LA3BT55jOUC42p3wGtho6vuC7Atov5Ic=;
       b=V0+TdQ2MxW43h+gImoerNMSqNYe77s0Gh8T/2KwA/9xyVWjCBeWWLFZmcJP7La6JTn
```

ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, just read this tutorial.



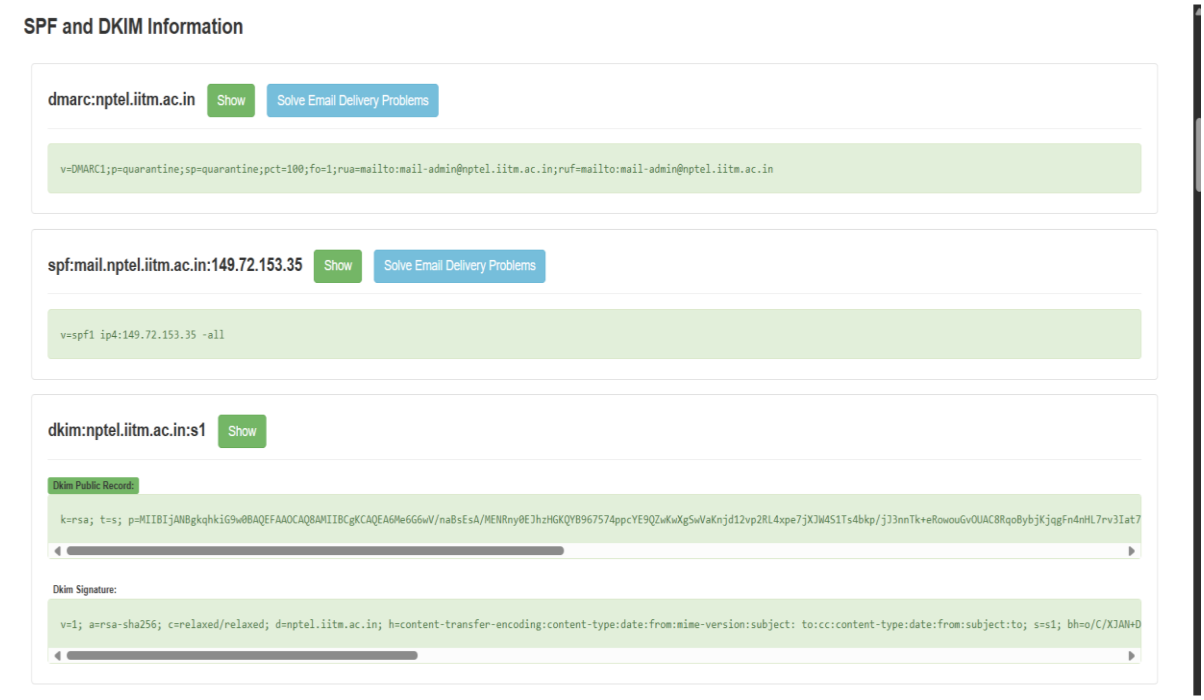
Delivery Information

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

Relay Information

Received Delay:	**0 seconds**

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	MzQ0NzA3Mg	geopod-ismtpd-5	HTTP	[]	
2	*		recvd-796bfbffd6-xhgb8	SMTP	[]	
3	*	wrqvwwnp.outbound-mail.sendgrid.net 149.72.153.35	mx.google.com	ESMTPS	8/28/2025 8:52:53 AM	✓
4	0 seconds		2002:a05:6f02:6708:b0:ee:da18:c8eb	SMTP	8/28/2025 8:52:53 AM	



SPF and DKIM Information

dmarc:nptel.iitm.ac.in

```
v=DMARC1;p=quarantine;sp=quarantine;pct=100;fo=1;rua=mailto:mail-admin@nptel.iitm.ac.in;ruf=mailto:mail-admin@nptel.iitm.ac.in
```

spf:mail.nptel.iitm.ac.in:149.72.153.35

```
v=spf1 ip4:149.72.153.35 -all
```

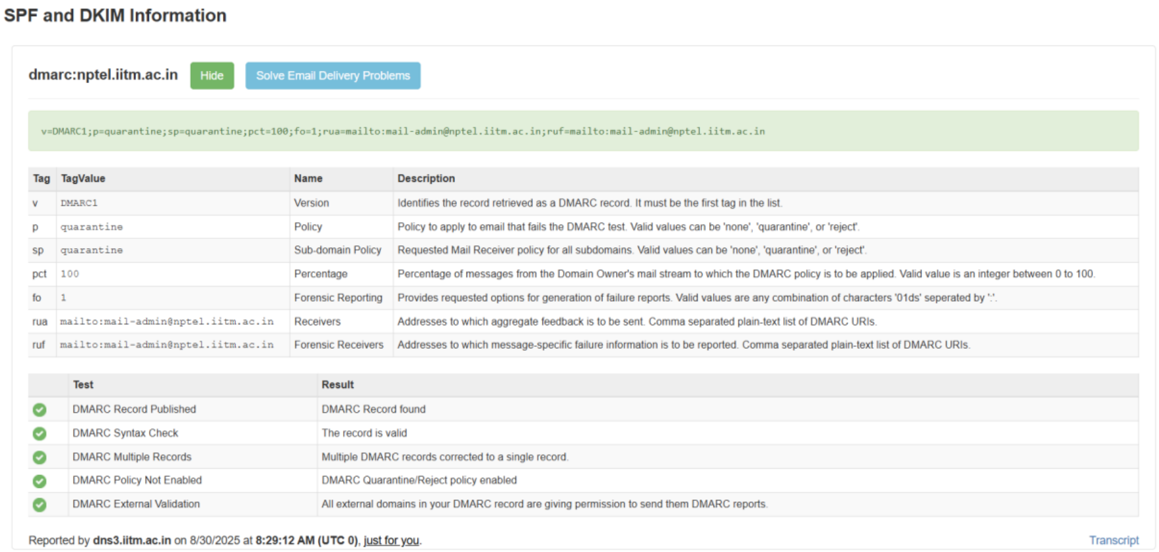
dkim:nptel.iitm.ac.in:s1

Dkim Public Record:

```
k=rsa; t=s; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6Me6G6wV/naBsEsA/MENRny0EJhzHGKQYB967574ppcYE9QZwKwXgSwVaKnjd12vp2RL4xpe7jXJW4S1Ts4bkp/jJ3nnTk+eRowouGvOUAC8RqoBybjKjqgFn4nHL7rv3Iat7
```

Dkim Signature:

```
v=1; a=rsa-sha256; c=relaxed/relaxed; d=nptel.iitm.ac.in; h=content-transfer-encoding:content-type:date:from:mime-version:subject: to:cc:content-type:date:from:subject:to; s=s1; bh=o/C/XJAN+D
```



SPF and DKIM Information

dmarc:nptel.iitm.ac.in

```
v=DMARC1;p=quarantine;sp=quarantine;pct=100;fo=1;rua=mailto:mail-admin@nptel.iitm.ac.in;ruf=mailto:mail-admin@nptel.iitm.ac.in
```

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	quarantine	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
sp	quarantine	Sub-domain Policy	Requested Mail Receiver policy for all subdomains. Valid values can be 'none', 'quarantine', or 'reject'.
pct	100	Percentage	Percentage of messages from the Domain Owner's mail stream to which the DMARC policy is to be applied. Valid value is an integer between 0 to 100.
fo	1	Forensic Reporting	Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' seperated by ':'.
rua	mailto:mail-admin@nptel.iitm.ac.in	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.
ruf	mailto:mail-admin@nptel.iitm.ac.in	Forensic Receivers	Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.

	Test	Result
✓	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 Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.

Reported by **dns3.iitm.ac.in** on 8/30/2025 at **8:29:12 AM (UTC 0)**, just for you.

Result:

The Mail Header Analyzer successfully traced the email’s origin and provided authentication details, helping to identify whether the email was genuine or spoofed.