# Email Forensic Analysis Report – yagnasree43@gmail.com Case (IMTEX Expo Invitation)

## Objective:

To analyze and identify phishing indicators in a suspicious email received by yagnasree43@gmail.com, claiming to be an invitation to 'IMTEX Connect Jamshedpur 2025'. The goal is to determine if the message is a phishing attempt and document all indicators found.

## 1. Email Metadata Overview

Subject: Invitation to Visit MTX Connect Jamshedpur 2025 – A 2-Day B2B Expo on Machine Tools & Manufacturing Technologies
From: imtex@imtexblr.in
To: yagnasree43@gmail.com
Date: Fri, 17 Oct 2025 17:00:13 +0000
Message-ID: <4urhjgyzgqbk.rLKrefV6ksx-xMu94P-fDg2@tracking.imtexblr.in>

## 2. Header Analysis (SPF, DKIM, DMARC)

• SPF: PASS – The sender domain (imtexblr.in) authorizes IP 178.33.84.76.
• DKIM: PASS – The DKIM signature matches imtexblr.in domain.
• DMARC: PASS – Domain policy allows this configuration.
⚠However, these can be spoofed if the attacker gains control of sending service via ElasticEmail.

IP Trace: 178.33.84.76 (OVH SAS, France) — hosting used by multiple third-party bulk mail senders, which increases phishing likelihood.

## 3. Body Content and Link Analysis

The email body is encoded in Base64, containing a large amount of formatted HTML text promoting an industrial event. However, the message includes embedded tracking links hosted on 'tracking.imtexblr.in' and third-party redirect URLs.

⚠Suspicious Links Identified:
1. http://tracking.imtexblr.in/tracking/click?... – redirects through unknown tracking service.
2. Multiple 'unsubscribe' and 'open pixel' tracking URLs.
3. Hidden transparent tracking images (1x1 px).
These techniques are commonly used in phishing or bulk email campaigns.

## 4. Tools Used

1. MXToolbox – Header & SPF/DKIM/DMARC validation
2. Google Message Header Analyzer – Timeline and IP trace
3. VirusTotal – URL scan for malicious redirects
4. URLVoid – Domain reputation check

## 5. Phishing Indicators Found

- Generic marketing tone urging participation in an event without prior contact.
- Use of external tracking links (tracking.imtexblr.in) instead of legitimate IMTEX domain.
- Embedded tracking pixels to gather recipient data.
- Hosted via third-party bulk mailing service (ElasticEmail), not official IMTEX servers.
- Base64-encoded HTML content, often used to obscure malicious payloads.

## 6. Conclusion and Recommendations

Although the email appears professional, the technical indicators suggest that it may be a phishing attempt aimed at collecting user data or distributing tracking links disguised as event registration pages.

✅Recommendation:

- Do not click on any links or download attachments.
- Report this email to the organization's IT or cybersecurity department.
- Block the sender and mark the message as spam/phishing.
- Perform a full system scan if any links were clicked.