Implement E-Mail Tracking and Email Investigation

Aim:
To track the origin of an email and perform forensic analysis using email header examination and investigation techniques.

Objective:

- To understand structure of E-mail Header
- To trace sender IP address
- To analyze email metadata
- To identify spoofed or malicious emails

Theory:
E-mail investigation lo main ga manam analyze chesedi:

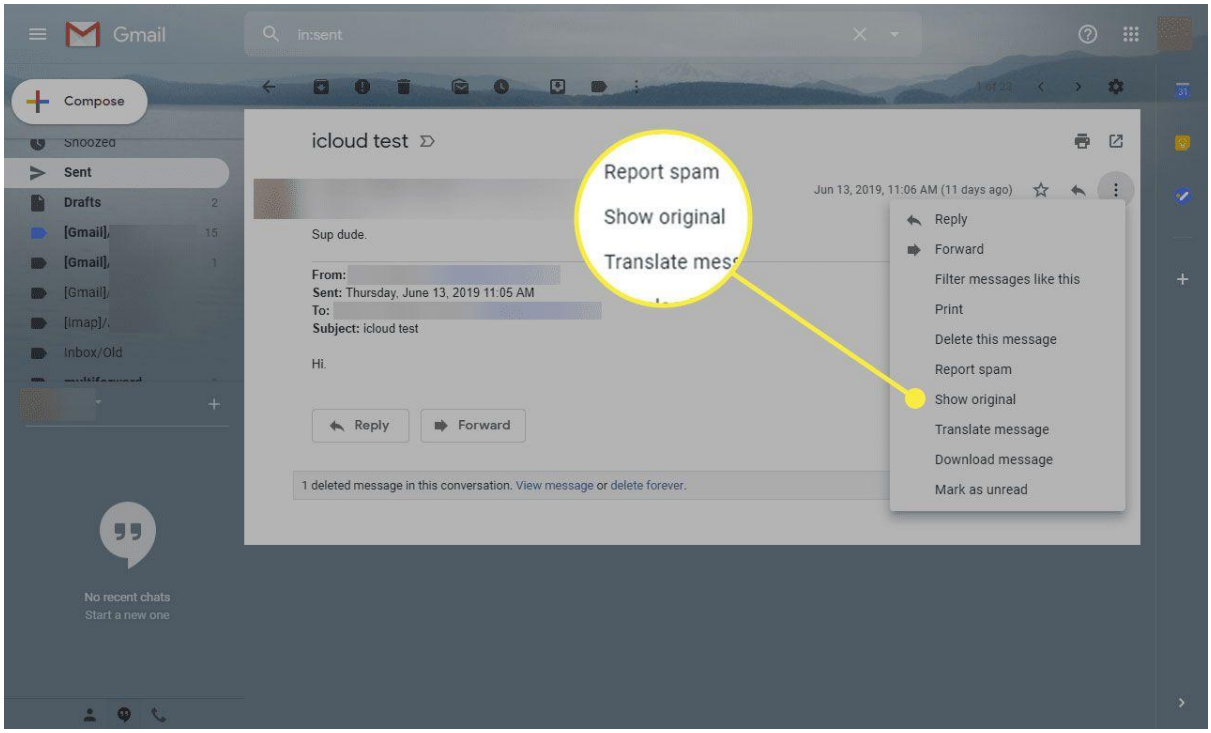
1. **Email Header**
2. **IP Address**
3. **Routing Information**
4. **SPF / DKIM Authentication**
5. **Attachments & Links**

Email header lo complete routing information untundi.
Manam normal inbox lo chuse content (From, To, Subject) kante header lo detailed technical info untundi.

Structure of an Email Header

Message headers ×

```
X-Pm-Content-Encryption: end-to-end
X-Pm-Origin: internal
Subject: Seattle trip
To: Kristen Novak <kristennovak@proton.me>
From: Eric Norbert <eric.norbert@proton.me>
Date: Tue, 14 Mar 2023 16:29:46 +0000
Mime-Version: 1.0
Content-Type: text/html
Message-Id:
<hvllFNSqLpe7Va0W4vl8oXzhimc9lBJQLKOjSg0zJtRzWZkzfohHSH0h5yTrIXn_pQ76eZMB7EzXQG
R3Q15LGKQGec9ZNdSuLgp1rj6TUXI=@proton.me>
X-Pm-Spamscore: 0
Received: from mail.protonmail.ch by mail.protonmail.ch; Tue, 14 Mar 2023
16:29:53 +0000
X-Original-To: kristennovak@proton.me
Return-Path: <eric.norbert@proton.me>
Delivered-To: kristennovak@proton.me
```




```
Received: from mail.litwareinc.com ([10.54.108.101]) by mail.proseware.com with Microsoft
SMTPSVC(6.0.3790.0);
Wed, 12 Dec 2007 13:39:22 -0800
Received: from mail ([10.54.108.23] RDNS failed) by mail.litware.com with Microsoft
SMTPSVC(6.0.3790.0);
Wed, 12 Dec 2007 13:38:49 -0800
From: "Kelly J. Weadock" <kelly@litware.com>
To: <anton@proseware.com>
Cc: <tim@cpandl.com>
Subject: Review of staff assignments
Date: Wed, 12 Dec 2007 13:38:31 -0800
MIME-Version: 1.0
Content-Type: multipart/mixed;
X-Mailer: Microsoft Office Outlook, Build 12.0.4210
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+ipA==
Return-Path: kelly@litware.com
Message-ID: <MAILbbnewS5TqCRL00000013@mail.litware.com>
X-OriginalArrivalTime: 12 Dec 2007 21:38:50.0145 (UTC)
```

Important Fields:

- **From:** Sender email address
- **To:** Receiver address
- **Subject:** Topic
- **Date:** Time stamp
- **Message-ID:** Unique identifier
- **Received:** Mail server routing path
- **Return-Path:** Bounce address
- **SPF/DKIM:** Authentication status

Procedure: Email Tracking & Investigation

Step1 : Obtain Full Email Header

In Gmail:

1. Open email
2. Click 3 dots (⋮)
3. Select **Show Original**
4. Copy full header

In Outlook:

1. Open email
2. File → Properties
3. Copy Internet headers

Step2 : Analyze "Received" Fields

"Received" lines ni bottom nundi top ki read cheyyali.

- First received entry → Original sending server
- Extract IP address

Example:

Received: from unknown (192.168.1.10)

IP address = 192.168.1.10

Step3 : Trace IP Address

Use:

- WHOIS lookup
- IP geolocation tools

Check:

- Country
- ISP
- Organization

Step4 : Verify Email Authentication

Check:

- SPF = Pass/Fail
- DKIM = Valid/Invalid
- DMARC = Pass/Fail

If SPF/DKIM fail ayite → Email spoofing possibility untundi.

Step 5 : Attachment & Link Analysis

- Suspicious attachments (.exe, .zip, .js)
- Hover links → Check real URL
- Use sandbox tools for malware analysis

Tools Used in Email Investigation

- Autopsy – Email artifact extraction
- Forensic Toolkit (FTK) – PST file analysis
- EnCase – Email recovery
- MXToolbox (Header analyzer)
- WHOIS lookup tools

Observations:

- Sender IP identified
- Mail server path traced
- Authentication status verified
- Suspicious links examined

Result:

The origin of the email was successfully traced using header analysis.
Email authenticity verified through SPF/DKIM validation.
Investigation report prepared.

Precautions:

- Do not open suspicious attachments directly
- Work on forensic copy
- Maintain chain of custody
- Document every step

Viva Questions:

1. What is Email Header?
2. What is SPF and DKIM?
3. How to detect email spoofing?
4. What is Message-ID?
5. Why Received fields are important?