ASSIGNMENT NO:1

In [ ]:
```
NAME:DARSHAN BELE
ROLLNO:14110
```

In [1]:
```
import re
from email import message_from_string

def extract_ip_from_received(received_headers):
    ips = []
    for header in received_headers:
        match = re.findall(r'\[?(\d{1,3}(?:\.\d{1,3}){3})\]?', header)
        ips.extend(match)
    return ips

def analyze_email_header(header_text):
    # Parse header using Python's email module
    msg = message_from_string(header_text)

    print("\n=== Basic Header Info ===")
    print(f"From            : {msg.get('From')}")
    print(f"To              : {msg.get('To')}")
    print(f"Subject         : {msg.get('Subject')}")
    print(f"Date            : {msg.get('Date')}")
    print(f"Return-Path     : {msg.get('Return-Path')}")
    print(f"Message-ID      : {msg.get('Message-ID')}")
    print(f"X-Originating-IP: {msg.get('X-Originating-IP')}")
    print(f"Authentication-Results: {msg.get('Authentication-Results')}")

    print("\n=== Tracing Email Route ===")
    received_headers = msg.get_all('Received')
    if received_headers:
        ips = extract_ip_from_received(received_headers)
        for i, header in enumerate(received_headers):
            print(f"\nHop {len(received_headers)-i}:")
            print(header.strip())
        print("\nPossible Origin IPs (From Received headers):")
        for ip in ips:
            print(f"-> {ip}")
    else:
        print("No 'Received' headers found!")

    print("\n=== Analysis Complete ===\n")

# Sample header input
sample_header = """\
Return-Path: <alerts@fakepaypal.com>
Received: from userpc.fakewifi.local (unknown [185.220.101.5])
        by mx1.mailhost.net (Postfix) with ESMTPSA id A1234B567C
        for <user@example.com>; Tue, 6 Aug 2024 09:45:12 +0530 (IST)
Received: from smtp.fakepaypal.com ([45.33.32.156])
        by smtp.sendmail.io with SMTP id 67890ABC
        for <alerts@fakepaypal.com>; Tue, 6 Aug 2024 09:40:00 +0530 (IST)
From: "PayPal Security Alert" <alerts@fakepaypal.com>
```

```
To: user@example.com
Subject: [IMPORTANT] Verify your PayPal Account Now
Date: Tue, 6 Aug 2024 09:39:59 +0530
Message-ID: <fakeid123456@fakepaypal.com>
X-Originating-IP: [203.0.113.88]
Authentication-Results: spf=fail dkim=fail dmarc=fail
"""

# Run analysis
analyze_email_header(sample_header)
```

```
=== Basic Header Info ===
From            : "PayPal Security Alert" <alerts@fakepaypal.com>
To              : user@example.com
Subject         : [IMPORTANT] Verify your PayPal Account Now
Date            : Tue, 6 Aug 2024 09:39:59 +0530
Return-Path     : <alerts@fakepaypal.com>
Message-ID      : <fakeid123456@fakepaypal.com>
X-Originating-IP: [203.0.113.88]
Authentication-Results: spf=fail dkim=fail dmarc=fail

=== Tracing Email Route ===

Hop 2:
from userpc.fakewifi.local (unknown [185.220.101.5])
        by mx1.mailhost.net (Postfix) with ESMTPSA id A1234B567C
        for <user@example.com>; Tue, 6 Aug 2024 09:45:12 +0530 (IST)

Hop 1:
from smtp.fakepaypal.com ([45.33.32.156])
        by smtp.sendmail.io with SMTP id 67890ABC
        for <alerts@fakepaypal.com>; Tue, 6 Aug 2024 09:40:00 +0530 (IST)

Possible Origin IPs (From Received headers):
-> 185.220.101.5
-> 45.33.32.156

=== Analysis Complete ===
```

In [ ]: