In [25]:

```
import email
import re
```

In [26]:

```
# The legitimate email from Atlassian
legitimate_header = """Delivered-To: sargampuram3@gmail.com
Received: by 2002:a05:612c:2222:b0:501:9217:d523 with SMTP id fn34csp2258
        Tue, 16 Sep 2025 04:30:18 -0700 (PDT)
X-Google-Smtp-Source: AGHT+IFN+ZtyXOhu2hYgizNzEfL0tan2SH2UeYkSD8OAxqAUgEs
X-Received: by 2002:a05:6a20:244b:b0:23d:45b2:8e3c with SMTP id adf61e73a
        Tue, 16 Sep 2025 04:30:18 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1758022218; cv=none;
        d=google.com; s=arc-20240605;
        b=hk+fjdW8An1KkXI59xIFGDs8lLgczqEIqyxlpM8m7qWCOBAzdxj+Dl89bWEI1Il
         S9Gc0l9ZpR5z++h/oJEWJGEWq0v9kVozjkFvfi9yaVqQmmMPDlkaWGD6MOmZK1hT
         HCnpKKyPfZxGLjvjmfR0Tq47NETt050slaEZGudtrRRbTcYiYdKM4ixRzHsPUyO9
         INHnJ667nsuq60VyHzLx2tJhquQT5De8EFzJJyoHIbBl+t+l209EZFVsT3orYM0C
         LwUpBN8K9kWuRrsKuK70Eda3Wc14/DHO4Ee8NYJqLVCDs/GC3hQenpUcZ2vmAPTI
         NYOQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com
        h=to:list-unsubscribe-post:list-unsubscribe:reply-to:subject
         :message-id:mime-version:from:date:dkim-signature:dkim-signature
        bh=HkadpNXgFYmlsR5Ppd/hspfraFiM7TfRlYnHXnzAxxA=;
        fh=1n0/KkjGFe01IRup0SjSMjEu+sFv5XvZruyLErMMJSU=;
        b=ZDsPcyEuT6NiJw0rGeDFEGerzk8JL3Cl1UmuHrKUkQPi+k4yLqirKTQvLWrWiRg
         kRQ5PMMEPlNdJbafXNObkA8xDo6gSld/yiktevQ9D6Nbshds0jWFj/U7wzTA9qZj
         NqxbuYHdGTTc/83vfOGVSXdT2bkTNjQWmV2tYF2kGD4FrNZqQngcho/I6heiPLWt
         OQqOxNRja50vSnW5mkadbF1OFb3qSeHkZ4EwxKDHNfPJA2vNX2EXdOfHDFKLP9d6
         U3p/E1seb9/iD/6Exb16rf41z42fCJqoynEnaQeT1s5Nmiphoy8ic/7asNVfo09Q
         saKw==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@atlassiancommunity.com header.s=bvy header.b=h
       dkim=pass header.i=@sendgrid.info header.s=smtpapi header.b=kTE+YF
       spf=pass (google.com: domain of bounces+4551147-fb38-sargampuram3=
Return-Path: <bounces+4551147-fb38-sargampuram3=gmail.com@em623.atlassian
Received: from o1.ptr7481.bevy.com (o1.ptr7481.bevy.com. [50.31.42.31])
        by mx.google.com with ESMTPS id 41be03b00d2f7-b54a94ca4f1si771213
        for <sargampuram3@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Tue, 16 Sep 2025 04:30:18 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounces+4551147-fb38-sargampura
Authentication-Results: mx.google.com;
       dkim=pass header.i=@atlassiancommunity.com header.s=bvy header.b=h
       dkim=pass header.i=@sendgrid.info header.s=smtpapi header.b=kTE+YF
       spf=pass (google.com: domain of bounces+4551147-fb38-sargampuram3=
From: Atlassian Community Events <no-reply@atlassiancommunity.com>
Subject: Don't forget to RSVP!
To: sargampuram3@gmail.com
Date: Tue, 16 Sep 2025 11:30:17 +0000 (UTC)
"""

# The spam email from "Abhi Loan"
spam_header = """Delivered-To: sargampuram3@gmail.com
Received: by 2002:a05:612c:20a7:b0:501:9217:d523 with SMTP id fj39csp1113
        Sat, 20 Sep 2025 22:55:52 -0700 (PDT)
X-Google-Smtp-Source: AGHT+IHoEg7Rn6LkA4va73DG/AyaJgRc+xjsTN8cTTibO5dQV0T
X-Received: by 2002:a05:620a:1920:b0:82b:5653:76bc with SMTP id af79cd13b
        Sat, 20 Sep 2025 22:55:52 -0700 (PDT)
```

```
ARC-Seal: i=1; a=rsa-sha256; t=1758434152; cv=none;
        d=google.com; s=arc-20240605;
        b=kafrgdDa6PhmRdtkWlSTGyF5LfC18ulPN6wA+oGrJ8JWv0ikwylo6sC0/IlmAwx
         vG7m9L2pZDmCjMbi7dR0wY630ifAQV79rkWHFdfYsCWGA4jWuwnaAbex/1zltPgV
         Q35nThuGhSaTNMfjXNPpKErdR4X8H3a6UzW8s/ndhoV4bxS69W9fni2RfF1Y/Jjo
         /8nudBt9atPz3cm/kNlDuL3iBL3YLZPrcTSYZhQVpWgTL/dyxehhXK2bZ8hNLYWn
         wKWn8+PdFRGO1C3X44tULN6337E3jpzyB95pCGHiwWoPKT3ux/Cpn5vdtIEpdPR2
         aF6g==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com
        h=date:mime-version:list-unsubscribe:feedback-id:list-id:message-
         :subject:to:reply-to:from:domainkey-signature:dkim-signature
         :dkim-signature;
        bh=6cJHqvPDLJtw6l74PEWhfl3cY4x1e/RjlGw3ndDL4uI=;
        fh=1n0/KkjGFe01IRup0SjSMjEu+sFv5XvZruyLErMMJSU=;
        b=Cy+YIqKt9gGgHEFj4ZIhZzNu0+dYUM26rrd2hXz65bDARY4FIrKVIJwCDzf6tyk
         w7LjG5NB3AmmOUwOKeXwT+yiwxWRXDuUGuzcfSdy4vdc4JKJ+qPXP96mzJg4gSGl
         H5qv/VENExED+zqe9iHauCM8uxRkk3PLseWmn8i0B/ADPskoyU4kkDxhiL/a7kVV
         dQW77/vdVA82+Y/n2ZKBoanxlHDr5TcIEeEmnDCZLHyegBYvE2ekDuC5fnq1XPXE
         hauHd9otzXBt6PhO9Kl5I7D2LJNH74fCHmt1YdhUmanntzDry0vtacbeSZ7jbme3
         Auxg==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@keyfor.in header.s=dkim2 header.b="A/+hC19Z";
       dkim=pass header.i=@ekf53.keyfor.in header.s=mail header.b=FuylaoA
       spf=pass (google.com: domain of gh-1-18094-6448a61e1fbf0-184295030
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=keyfor.in
Return-Path: <gh-1-18094-6448a61e1fbf0-1842950304522305536-1758432602@ekf
Received: from ekf53.keyfor.in (ekf53.keyfor.in. [144.217.105.53])
        by mx.google.com with ESMTPS id af79cd13be357-83a2a8a6072si258968
        for <sargampuram3@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128
        Sat, 20 Sep 2025 22:55:52 -0700 (PDT)
Received-SPF: pass (google.com: domain of gh-1-18094-6448a61e1fbf0-184295
Authentication-Results: mx.google.com;
       dkim=pass header.i=@keyfor.in header.s=dkim2 header.b="A/+hC19Z";
       dkim=pass header.i=@ekf53.keyfor.in header.s=mail header.b=FuylaoA
       spf=pass (google.com: domain of gh-1-18094-6448a61e1fbf0-184295030
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=keyfor.in
From: Abhi Loan <newsletter@keyfor.in>
Reply-To: <newsletter@keyfor.in>
To: sargampuram3@gmail.com
Subject: Congratulations! Your Loan Has Been Approved
Date: Sun, 21 Sep 2025 11:25:17 +0530
"""
```

In [27]:

```
def analyze_email_header(header_str):
    """
    Parses the header block of a full email source string and runs a
    forensic analysis based on header information.
    """
    # Isolate the header block before parsing to avoid errors.
    header_block = header_str.split('\n\n', 1)[0]
    headers = email.message_from_string(header_block)

    # --- Basic Information ---
    print("## ✉️ Basic Information")
    from_addr = headers.get('From', 'N/A')
    to_addr = headers.get('To', 'N/A')
    subject = headers.get('Subject', 'N/A')
    print(f"  - From: {from_addr}")
    print(f"  - To: {to_addr}")
    print(f"  - Subject: {subject}")
    print("-" * 20)

    # --- Forensic Investigation (Headers Only) ---
    print("## 🕵️ Forensic Investigation")

    auth_results = headers.get('Authentication-Results', 'Not found')
    spf_results = headers.get('Received-SPF', 'Not found')
    suspicious_flags = 0

    # 1. SPF Check
    print("\n🔍 1. SPF Check:")
    if 'pass' in spf_results.lower():
        print("  - ✅ Result: PASS. The sending server IP is authorized."
    else:
        print("  - ❌ Result: FAIL or NOT FOUND. The server is not author
        suspicious_flags += 1

    # 2. DKIM Check
    print("\n🔍 2. DKIM Check:")
    if 'dkim=pass' in auth_results.lower():
        print("  - ✅ Result: PASS. The email has a valid digital signatu
    else:
        print("  - ❌ Result: FAIL or NOT FOUND. The email's signature is
        suspicious_flags += 1

    # 3. Sender Name vs. Domain Deception Check
    print("\n🔍 3. Sender Deception Check:")
    try:
        # Extract the display name (e.g., "Abhi Loan")
        display_name = from_addr.split('<')[0].strip().lower()

        # Extract the domain from the email address
        from_email_match = re.search(r'<(.+?)>', from_addr)
        from_email = from_email_match.group(1) if from_email_match else f
        from_domain = from_email.split('@')[-1]

        print(f"  - Display Name: '{display_name}'")
        print(f"  - Sender Domain: '{from_domain}'")

        # Check if a key word from the display name exists in the domain
        is_consistent = False
        # Remove generic words like 'events' or 'community' before checki
        critical_name_words = display_name.replace('events', '').replace(
        for word in critical_name_words:
            if word and word in from_domain:
                is_consistent = True
                break

        if is_consistent:
            print("  - ✅ Result: CONSISTENT. The sender name appears to
        else:
            print("  - ❌ Result: DECEPTIVE. The sender name has no relat
            suspicious_flags += 1

    except Exception:
        print("  - ⚠️ Could not perform sender deception check.")
    # --- Conclusion ---
    print("\n" + "="*40)
    print("## 🏁 FINAL CONCLUSION")
    if suspicious_flags > 0:
        print(f"  - This email is POTENTIALLY SPOOFED or DANGEROUS. 🚨")
        print(f"  - Reason: It triggered {suspicious_flags} red flag(s) d
    else:
        print("  - This email appears to be TECHNICALLY AUTHENTIC. ✅")
        print("  - Reason: It passed all header-based security checks.")
    print("="*40 + "\n")
```

In [28]:

```
print("="*15, "Analyzing Legitimate Atlassian Email", "="*15)
analyze_email_header(legitimate_header)
```

```
=============== Analyzing Legitimate Atlassian Email ===============
## ✉️ Basic Information
  - From: Atlassian Community Events <no-reply@atlassiancommunity.com>
  - To: sargampuram3@gmail.com
  - Subject: Don't forget to RSVP!
--------------------
## 🕵️ Forensic Investigation

🔍 1. SPF Check:
  - ✅ Result: PASS. The sending server IP is authorized.

🔍 2. DKIM Check:
  - ✅ Result: PASS. The email has a valid digital signature.

🔍 3. Sender Deception Check:
  - Display Name: 'atlassian community events'
  - Sender Domain: 'atlassiancommunity.com'
  - ✅ Result: CONSISTENT. The sender name appears to match the domain.

========================================
## 🏁 FINAL CONCLUSION
  - This email appears to be TECHNICALLY AUTHENTIC. ✅
  - Reason: It passed all header-based security checks.
========================================
```

In [29]:

```
print("="*15, "Analyzing Spam 'Abhi Loan' Email", "="*15)
analyze_email_header(spam_header)
```

```
=============== Analyzing Spam 'Abhi Loan' Email ===============
## ✉️ Basic Information
  - From: Abhi Loan <newsletter@keyfor.in>
  - To: sargampuram3@gmail.com
  - Subject: Congratulations! Your Loan Has Been Approved
--------------------
## 🕵️ Forensic Investigation

🔍 1. SPF Check:
  - ✅ Result: PASS. The sending server IP is authorized.

🔍 2. DKIM Check:
  - ✅ Result: PASS. The email has a valid digital signature.

🔍 3. Sender Deception Check:
  - Display Name: 'abhi loan'
  - Sender Domain: 'keyfor.in'
  - ❌ Result: DECEPTIVE. The sender name has no relation to the domain. T
his is a major red flag.

========================================
## 🏁 FINAL CONCLUSION
  - This email is POTENTIALLY SPOOFED or DANGEROUS. 🚨
  - Reason: It triggered 1 red flag(s) during header analysis.
========================================
```

```
In [ ]:
```