SIL765: Networks and System Security
Semester II, 2020-2021
Assignment-4

Dipika Tanwar (2020MCS2456)

April 2021

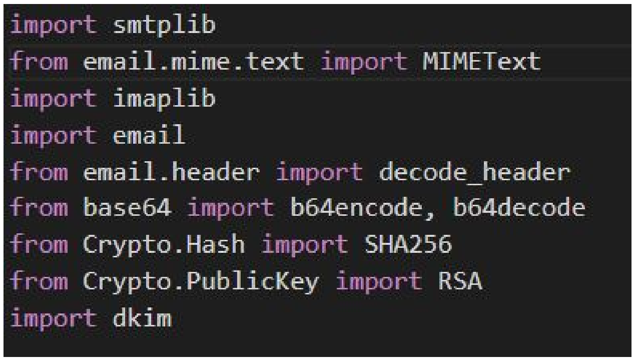
1 Introduction

Below files are implemented:

- **my_sender.py**: This script sends mail to IIT Delhi mail server using python smtplib with my credentials.
- **my_receiver.py**: This script is run just after running sender script. This will fetch first message from IIT account(at the one where message is sent) inbox and calls verifies DKIM signature of parser.
- **my_parser.py**: This script parses security protocols utilized. Has functionlities for printing various mail headers, security iformation, dumping all email headers to output file or verifying DKIM.

2 Environment

2.1 Following libraries are utilized



```
import smtplib
from email.mime.text import MIMEText
import imaplib
import email
from email.header import decode_header
from base64 import b64encode, b64decode
from Crypto.Hash import SHA256
from Crypto.PublicKey import RSA
import dkim
```

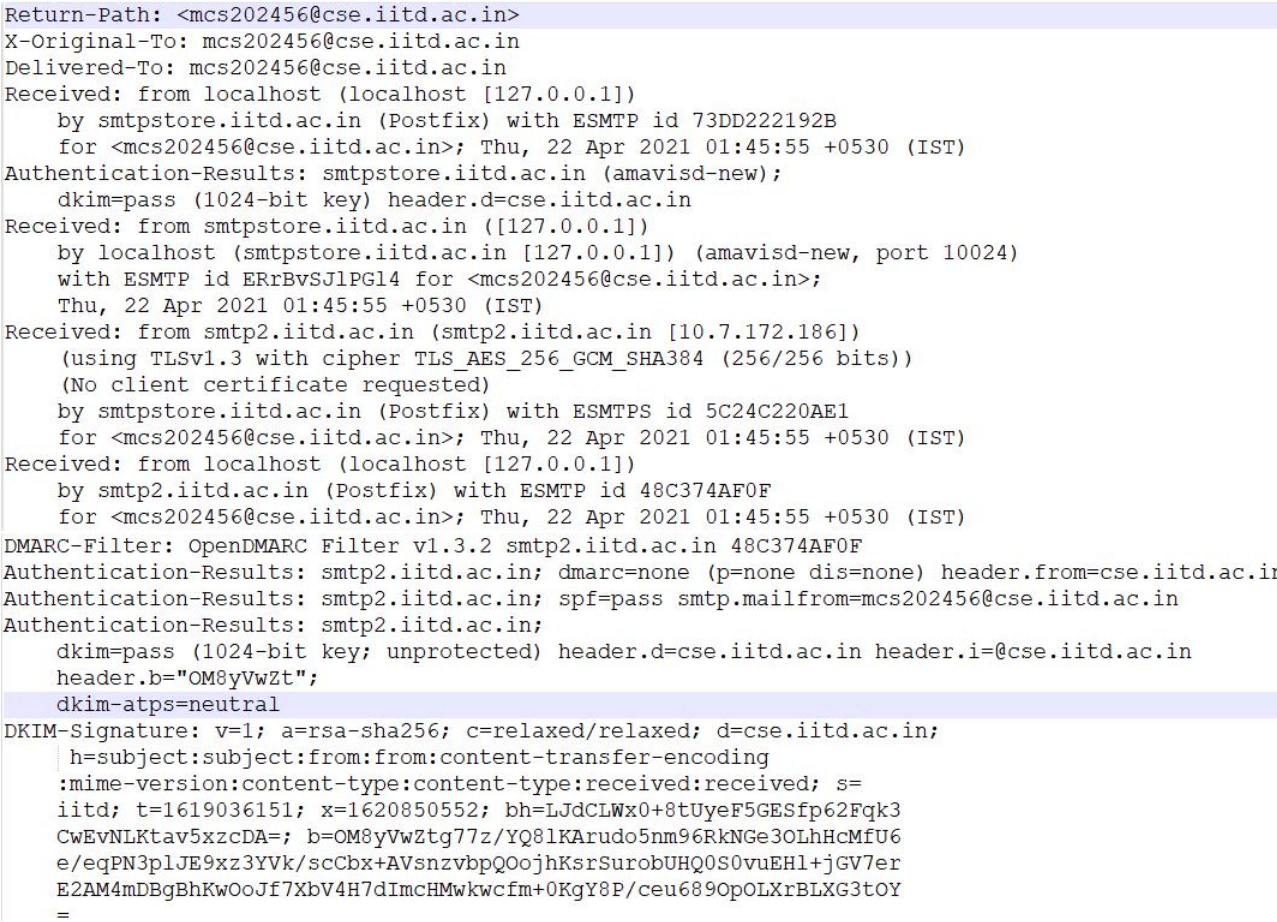
3 How to Run

- **my_sender.py**: python my_sender.py
- **my_receiver.py**: python my_receiver.py
- **my_parser.py** : No need to run this file. This file functions are utilised by my_receiver.py to parse and fill security protocol information to verify DKIM signaure.

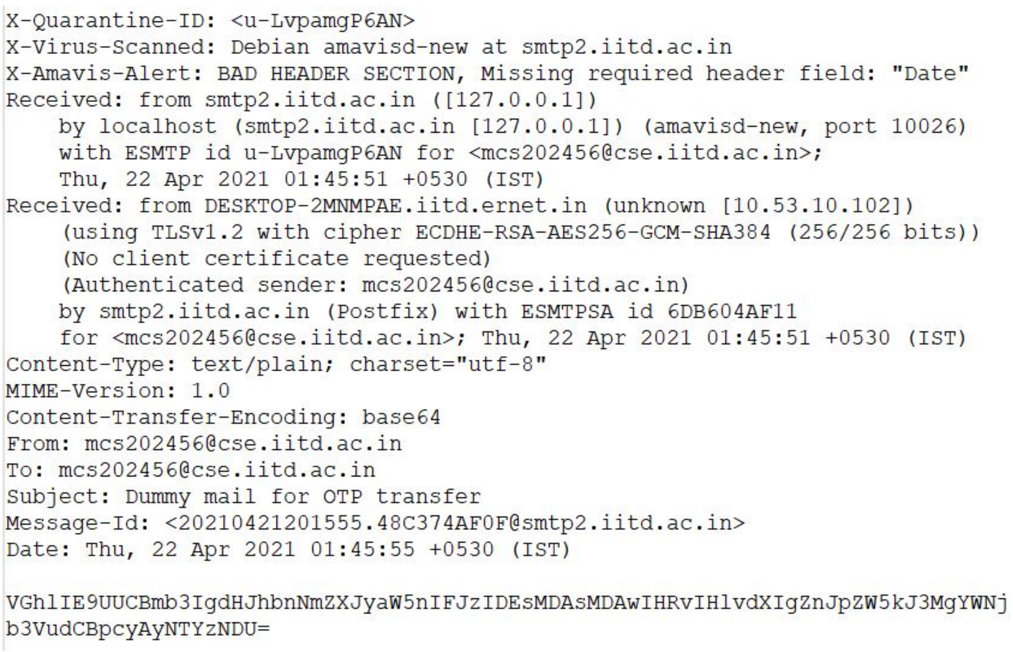
4 Screenshots

These screen shots are captured from file which are created with functionality of my_parser.py

4.1 Mail: 'my_sender.py' to 'iit mail box'



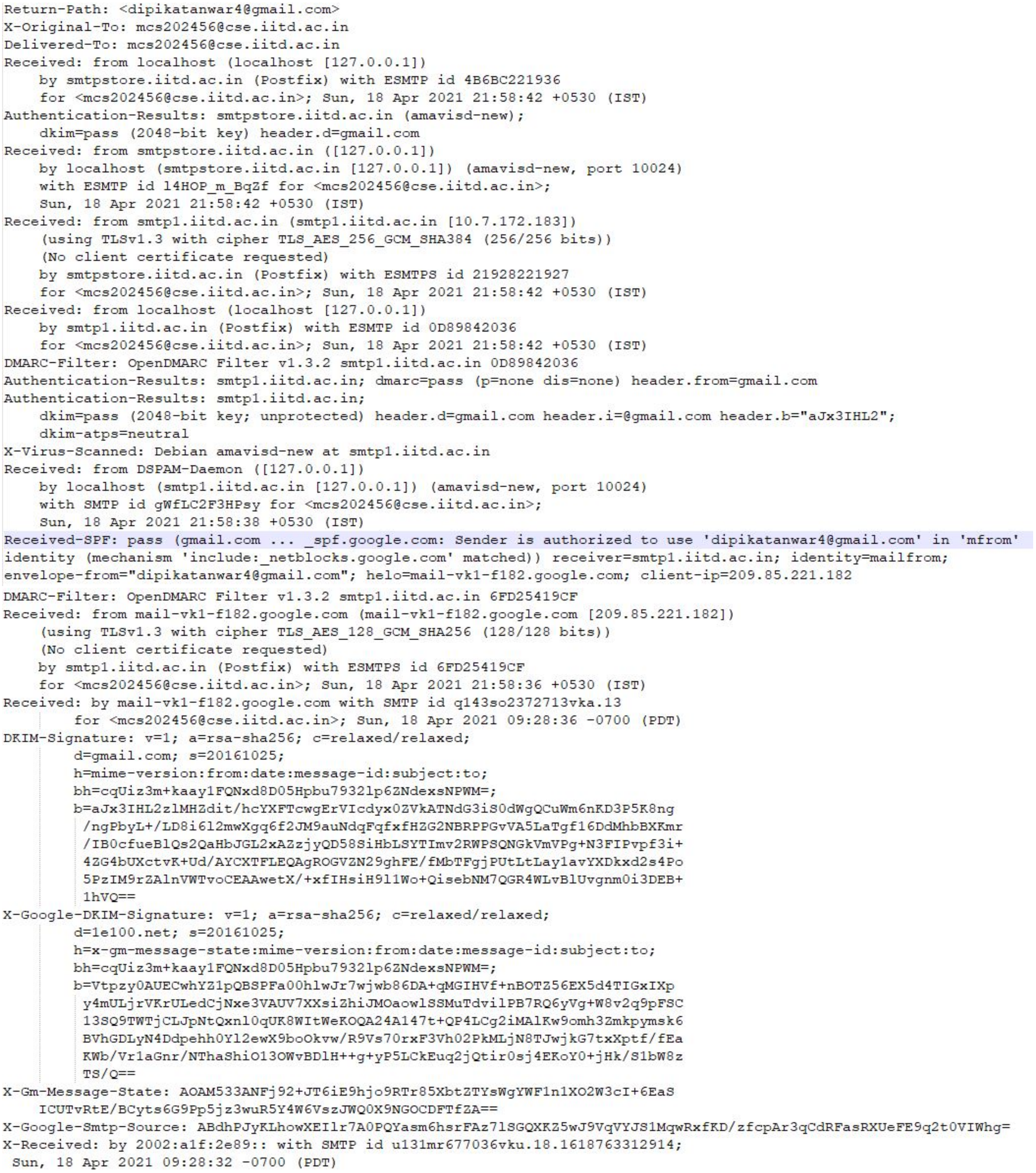
```
Return-Path: <mcs202456@cse.iitd.ac.in>
X-Original-To: mcs202456@cse.iitd.ac.in
Delivered-To: mcs202456@cse.iitd.ac.in
Received: from localhost (localhost [127.0.0.1])
    by smtpstore.iitd.ac.in (Postfix) with ESMTP id 73DD222192B
    for <mcs202456@cse.iitd.ac.in>; Thu, 22 Apr 2021 01:45:55 +0530 (IST)
Authentication-Results: smtpstore.iitd.ac.in (amavisd-new);
    dkim=pass (1024-bit key) header.d=cse.iitd.ac.in
Received: from smtpstore.iitd.ac.in ([127.0.0.1])
    by localhost (smtpstore.iitd.ac.in [127.0.0.1]) (amavisd-new, port 10024)
    with ESMTP id ERrBvSJlPGl4 for <mcs202456@cse.iitd.ac.in>;
    Thu, 22 Apr 2021 01:45:55 +0530 (IST)
Received: from smtp2.iitd.ac.in (smtp2.iitd.ac.in [10.7.172.186])
    (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits))
    (No client certificate requested)
    by smtpstore.iitd.ac.in (Postfix) with ESMTPS id 5C24C220AE1
    for <mcs202456@cse.iitd.ac.in>; Thu, 22 Apr 2021 01:45:55 +0530 (IST)
Received: from localhost (localhost [127.0.0.1])
    by smtp2.iitd.ac.in (Postfix) with ESMTP id 48C374AF0F
    for <mcs202456@cse.iitd.ac.in>; Thu, 22 Apr 2021 01:45:55 +0530 (IST)
DMARC-Filter: OpenDMARC Filter v1.3.2 smtp2.iitd.ac.in 48C374AF0F
Authentication-Results: smtp2.iitd.ac.in; dmarc=none (p=none dis=none) header.from=cse.iitd.ac.i
Authentication-Results: smtp2.iitd.ac.in; spf=pass smtp.mailfrom=mcs202456@cse.iitd.ac.in
Authentication-Results: smtp2.iitd.ac.in;
    dkim=pass (1024-bit key; unprotected) header.d=cse.iitd.ac.in header.i=@cse.iitd.ac.in
    header.b="OM8yVwZt";
    dkim-atps=neutral
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=cse.iitd.ac.in;
     h=subject:subject:from:from:content-transfer-encoding
    :mime-version:content-type:content-type:received:received; s=
    iitd; t=1619036151; x=1620850552; bh=LJdCLWx0+8tUyeF5GESfp62Fqk3
    CwEvNLKtav5xzcDA=; b=OM8yVwZtg77z/YQ8lKArudo5nm96RkNGe3OLhHcMfU6
    e/eqPN3plJE9xz3YVk/scCbx+AVsnzvbpQOojhKsrSurobUHQ0S0vuEHl+jGV7er
    E2AM4mDBgBhKwOoJf7XbV4H7dImcHMwkwcfm+0KgY8P/ceu689OpOLXrBLXG3tOY
    =
```



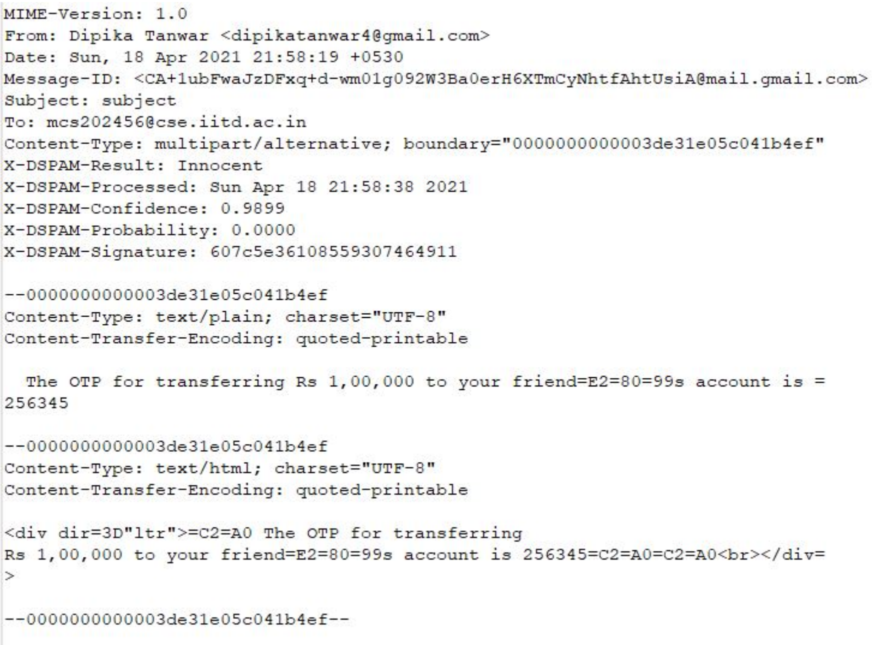
```
X-Quarantine-ID: <u-LvpamgP6AN>
X-Virus-Scanned: Debian amavisd-new at smtp2.iitd.ac.in
X-Amavis-Alert: BAD HEADER SECTION, Missing required header field: "Date"
Received: from smtp2.iitd.ac.in ([127.0.0.1])
    by localhost (smtp2.iitd.ac.in [127.0.0.1]) (amavisd-new, port 10026)
    with ESMTP id u-LvpamgP6AN for <mcs202456@cse.iitd.ac.in>;
    Thu, 22 Apr 2021 01:45:51 +0530 (IST)
Received: from DESKTOP-2MNMPAE.iitd.ernet.in (unknown [10.53.10.102])
    (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
    (No client certificate requested)
    (Authenticated sender: mcs202456@cse.iitd.ac.in)
    by smtp2.iitd.ac.in (Postfix) with ESMTPSA id 6DB604AF11
    for <mcs202456@cse.iitd.ac.in>; Thu, 22 Apr 2021 01:45:51 +0530 (IST)
Content-Type: text/plain; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: base64
From: mcs202456@cse.iitd.ac.in
To: mcs202456@cse.iitd.ac.in
Subject: Dummy mail for OTP transfer
Message-Id: <20210421201555.48C374AF0F@smtp2.iitd.ac.in>
Date: Thu, 22 Apr 2021 01:45:55 +0530 (IST)
```

VGhlIE9UUCBmb3IgdHJhbnNmZXJyaW5nIFJzIDEsMDAsMDAwIHRvIHlvdXIgZnJpZW5kJ3MgYWNj
b3VudCBpcyAyNTYzNDU=

4.2 Mail: 'gmail' to 'iit mail box'

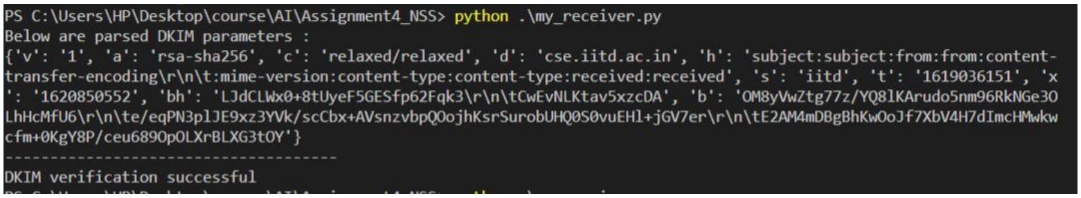


```
Return-Path: <dipikatanwar4@gmail.com>
X-Original-To: mcs202456@cse.iitd.ac.in
Delivered-To: mcs202456@cse.iitd.ac.in
Received: from localhost (localhost [127.0.0.1])
    by smtpstore.iitd.ac.in (Postfix) with ESMTP id 4B6BC221936
    for <mcs202456@cse.iitd.ac.in>; Sun, 18 Apr 2021 21:58:42 +0530 (IST)
Authentication-Results: smtpstore.iitd.ac.in (amavisd-new);
    dkim=pass (2048-bit key) header.d=gmail.com
Received: from smtpstore.iitd.ac.in ([127.0.0.1])
    by localhost (smtpstore.iitd.ac.in [127.0.0.1]) (amavisd-new, port 10024)
    with ESMTP id l4HOP_m_BqZf for <mcs202456@cse.iitd.ac.in>;
    Sun, 18 Apr 2021 21:58:42 +0530 (IST)
Received: from smtp1.iitd.ac.in (smtp1.iitd.ac.in [10.7.172.183])
    (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits))
    (No client certificate requested)
    by smtpstore.iitd.ac.in (Postfix) with ESMTPS id 21928221927
    for <mcs202456@cse.iitd.ac.in>; Sun, 18 Apr 2021 21:58:42 +0530 (IST)
Received: from localhost (localhost [127.0.0.1])
    by smtp1.iitd.ac.in (Postfix) with ESMTP id 0D89842036
    for <mcs202456@cse.iitd.ac.in>; Sun, 18 Apr 2021 21:58:42 +0530 (IST)
DMARC-Filter: OpenDMARC Filter v1.3.2 smtp1.iitd.ac.in 0D89842036
Authentication-Results: smtp1.iitd.ac.in; dmarc=pass (p=none dis=none) header.from=gmail.com
Authentication-Results: smtp1.iitd.ac.in;
    dkim=pass (2048-bit key; unprotected) header.d=gmail.com header.i=@gmail.com header.b="aJx3IHL2";
    dkim-atps=neutral
X-Virus-Scanned: Debian amavisd-new at smtp1.iitd.ac.in
Received: from DSPAM-Daemon ([127.0.0.1])
    by localhost (smtp1.iitd.ac.in [127.0.0.1]) (amavisd-new, port 10024)
    with SMTP id gWfLC2F3HPsy for <mcs202456@cse.iitd.ac.in>;
    Sun, 18 Apr 2021 21:58:38 +0530 (IST)
Received-SPF: pass (gmail.com ... _spf.google.com: Sender is authorized to use 'dipikatanwar4@gmail.com' in 'mfrom'
identity (mechanism 'include:_netblocks.google.com' matched)) receiver=smtp1.iitd.ac.in; identity=mailfrom;
envelope-from="dipikatanwar4@gmail.com"; helo=mail-vk1-f182.google.com; client-ip=209.85.221.182
DMARC-Filter: OpenDMARC Filter v1.3.2 smtp1.iitd.ac.in 6FD25419CF
Received: from mail-vk1-f182.google.com (mail-vk1-f182.google.com [209.85.221.182])
    (using TLSv1.3 with cipher TLS_AES_128_GCM_SHA256 (128/128 bits))
    (No client certificate requested)
    by smtp1.iitd.ac.in (Postfix) with ESMTPS id 6FD25419CF
    for <mcs202456@cse.iitd.ac.in>; Sun, 18 Apr 2021 21:58:36 +0530 (IST)
Received: by mail-vk1-f182.google.com with SMTP id q143so2372713vka.13
        for <mcs202456@cse.iitd.ac.in>; Sun, 18 Apr 2021 09:28:36 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20161025;
        h=mime-version:from:date:message-id:subject:to;
        bh=cqUiz3m+kaay1FQNxd8D05Hpbu7932lp6ZNdexsNPWM=;
        b=aJx3IHL2zlMHZdit/hcYXFTcwgErVIcdyx0ZVkATNdG3iS0dWgQCuWm6nKD3P5K8ng
         /ngPbyL+/LD8i6l2mwXgq6f2JM9auNdqFqfxfHZG2NBRPPGvVA5LaTgf16DdMhbBXKmr
         /IB0cfueBlQs2QaHbJGL2xAZzjyQD58SiHbLSYTImv2RWPSQNGkVmVPg+N3FIPvpf3i+
         4ZG4bUXctvK+Ud/AYCXTFLEQAgROGVZN29ghFE/fMbTFgjPUtLtLay1avYXDkxd2s4Po
         5PzIM9rZAlnVWTvoCEAAwetX/+xfIHsiH9l1Wo+QisebNM7QGR4WLvBlUvgnm0i3DEB+
         1hVQ==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20161025;
        h=x-gm-message-state:mime-version:from:date:message-id:subject:to;
        bh=cqUiz3m+kaay1FQNxd8D05Hpbu7932lp6ZNdexsNPWM=;
        b=Vtpzy0AUECwhYZ1pQBSPFa00hlwJr7wjwb86DA+qMGIHVf+nBOTZ56EX5d4TIGxIXp
         y4mULjrVKrULedCjNxe3VAUV7XXsiZhiJMOaowlSSMuTdvilPB7RQ6yVg+W8v2q9pFSC
         13SQ9TWTjCLJpNtQxnl0qUK8WItWeKOQA24A147t+QP4LCg2iMAlKw9omh3Zmkpymsk6
         BVhGDLyN4Ddpehh0Yl2ewX9boOkvw/R9Vs70rxF3Vh02PkMLjN8TJwjkG7txXptf/fEa
         KWb/Vr1aGnr/NThaShiO13OWvBDlH++g+yP5LCkEuq2jQtir0sj4EKoY0+jHk/S1bW8z
         TS/Q==
X-Gm-Message-State: AOAM533ANFj92+JT6iE9hjo9RTr85XbtZTYsWgYWF1n1XO2W3cI+6EaS
    ICUTvRtE/BCyts6G9Pp5jz3wuR5Y4W6VszJWQ0X9NGOCDFTfZA==
X-Google-Smtp-Source: ABdhPJyKLhowXEIlr7A0PQYasm6hsrFAz7lSGQXKZ5wJ9VqVYJS1MqwRxfKD/zfcpAr3qCdRFasRXUeFE9q2t0VIWhg=
X-Received: by 2002:a1f:2e89:: with SMTP id u131mr677036vku.18.1618763312914;
 Sun, 18 Apr 2021 09:28:32 -0700 (PDT)
```



```
MIME-Version: 1.0
From: Dipika Tanwar <dipikatanwar4@gmail.com>
Date: Sun, 18 Apr 2021 21:58:19 +0530
Message-ID: <CA+1ubFwaJzDFxq+d-wm01g092W3Ba0erH6XTmCyNhtfAhtUsiA@mail.gmail.com>
Subject: subject
To: mcs202456@cse.iitd.ac.in
Content-Type: multipart/alternative; boundary="0000000000003de31e05c041b4ef"
X-DSPAM-Result: Innocent
X-DSPAM-Processed: Sun Apr 18 21:58:38 2021
X-DSPAM-Confidence: 0.9899
X-DSPAM-Probability: 0.0000
X-DSPAM-Signature: 607c5e36108559307464911

--0000000000003de31e05c041b4ef
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable

  The OTP for transferring Rs 1,00,000 to your friend=E2=80=99s account is =
256345

--0000000000003de31e05c041b4ef
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable

<div dir=3D"ltr">=C2=A0 The OTP for transferring
Rs 1,00,000 to your friend=E2=80=99s account is 256345=C2=A0=C2=A0<br></div=
>

--0000000000003de31e05c041b4ef--
```

4.3 screen shot when my_receiver.py is run



```
PS C:\Users\HP\Desktop\course\AI\Assignment4_NSS> python .\my_receiver.py
Below are parsed DKIM parameters :
{'v': '1', 'a': 'rsa-sha256', 'c': 'relaxed/relaxed', 'd': 'cse.iitd.ac.in', 'h': 'subject:subject:from:from:content-
transfer-encoding\r\n\t:mime-version:content-type:content-type:received:received', 's': 'iitd', 't': '1619036151', 'x
': '1620850552', 'bh': 'LJdCLWx0+8tUyeF5GESfp62Fqk3\r\n\tCwEvNLKtav5xzcDA', 'b': 'OM8yVwZtg77z/YQ8lKArudo5nm96RkNGe3O
LhHcMfU6\r\n\te/eqPN3plJE9xz3YVk/scCbx+AVsnzvbpQOojhKsrSurobUHQ0S0vuEHl+jGV7er\r\n\tE2AM4mDBgBhKwOoJf7XbV4H7dImcHMwkw
cfm+0KgY8P/ceu689OpOLXrBLXG3tOY'}
-------------------------------------
DKIM verification successful
```

5 Part-1

5.1 Task

Configuration on which above scripts are run

- Mail is send on port 25 using SMTP function of smtplib.
- Mail is send on port 465 using SMTP_SSL function of smtplib.
- Mail is received by python imaplib using function IMAP4_SSL at port 993.

5.2 Analysis

Information from email header :

- Return-Path: This field exist to return if sending of mail fails. This field shows sends email address.
- Receive header: This shows successful receipt points of sent message.
  1. Our email shows 6 Receiver header so, the email is routed through there points between source (IP address) to destination
  2. Main route points shown: IP address of senders to smtp2.iitd.ac.in to smtpstore.iitd.ac.in to destination localhost.
  3. It has information of authentication protocols with their authentication results. SPF and DKIM shows pass result where as DMARC shows none.
  4. All info about DKIM(v=1; a=rsa-sha256; c=relaxed/relaxed; d=cse.iitd.ac.in) along with its hash tag and DKIM signature is present.
  5. X-headers (X-Quarantine-ID,X-Virus-Scanned and X-Amavis-Alert)are present showing status of virus scanned or missing field error like date was missing at my_sender.py
- Other headers like Content-Type(text/plain; charset="utf-8"), MIME-Version (1.0),content-transfer-encoding (base64), From, To ,Subject, Message-Id and Date are present

Security Analysis
The security against spam ,spoofing is provided by SPF and DKIM. Alythough DMARC which is extended version of SPF and DKIM is not utilized.

1. Send mail with SMTP is possible only with starttls() over port 25 or with SMTP_SSL which shows that sending of mail via secure TLS/SSL is only allowed. Function starttls() upgrades insecure SMTP connection to secure connection with TLS/SSL.
2. Authentication protocols utilized:
   - SPF : Receiving mail server can decide to accept or reject mail by verifying sender email and IP address using SPF record published by domain administrator. Prevents spams with forged email address.
   - DKIM : In bound mail server verifies DKIM signature using public key published by domain owner to check authentication of message.
3. Information about TLS protocols utilisation TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 and shows no client certificate requested during handshake.

6 Part-2

6.1 Tasks performed

1. Send a mail using gmail to iit delhi mail account and fetch the mail with my_receiver.py.

2. **my_parser.py** : This script help to extract security protocol information for both mails (my_sender to iitd server and gmail to iitd server)

6.2 Analysis comparision

1. Gmail utilises DMARC and IITD doesnot utilize DMARC
   - GMAIL: Authentication-Results: dmarc=pass
   - IITD mail: Authentication-Results: dmarc=none
2. Both utilize SPF authentication
   - GMAIL: Received-SPF: pass
   - IITD mail: Authentication-Results: spf=pass
3. Both utilize DKIM authentication. IITD mail utilizez DKIM once whereas GMAIL utilizes it twice.
   - Gmail: 2048-bit key. One with domain gmail.com with sha256 for message and second with domain d=1e100.net and hash tag has additional field gm-message-state
   - IITD mail: 1024-bit key and domain cse.iitd.ac.in with sha256.
4. GMAIL has DSPAM field which is statistical spam filter. Provides below information based on statistics.
   - X-DSPAM-Result: Innocent
   - X-DSPAM-Processed: Sun Apr 18 21:58:38 2021
   - X-DSPAM-Confidence: 0.9899
   - X-DSPAM-Probability: 0.0000
   - X-DSPAM-Signature: 607c5e36108559307464911

6.2.1 Security analysis

The above similarities and differences shows that GMAIL is safer than IIT Delhi mail service .

- GMAIL uses more authentication protocols like DMARC.
- GMAIL uses DSPAM for identifying spams.
- Gmail has multiple hash keys like 2 DKIM verification on dummy mail. Also, longer key is utilized for DKIM.

as it utilises. Also it . Also, DKIM utilized in performed unlike IIT delhi mail where, only one DKIM authentication is performed.

6.3 DKIM comparision

As already observed both utilize DKIM authentication. IITD mail utilizes DKIM once whereas GMAIL utilizes it twice.

- Gmail: 2048-bit key. One with domain gmail.com with sha256 for message and second with domain d=1e100.net and hash tag has additional field gm-message-state.
- IITD mail: 1024-bit key and domain cse.iitd.ac.in with sha256.

6.4 DKIM verification

DKIM verification can be done at receiver end by querying the signer's domain directly to get public key and verify that private key of signer's domain was utilized.

- Computing hash with algorithm mentioned in DKIM field (sha256) and comparing it with 'bh' field parameter of DKIM. If both are not equal verification fails.
- Than with domain and selector info query public key and get the public key for the domain. RSA Decryption of the signature field 'b' with public key must match with hash of 'h' field in DKIM signature.
- Based on 'c' field it must be decided to relax (ignore by striping off) white spaces,etc if field value is relaxed. Otherwise, Hash computed will not match.

The verification of DKIM is performed with help of python dkim library function DKIM.verify(). All the 3 above mentioned steps are executed via this function.