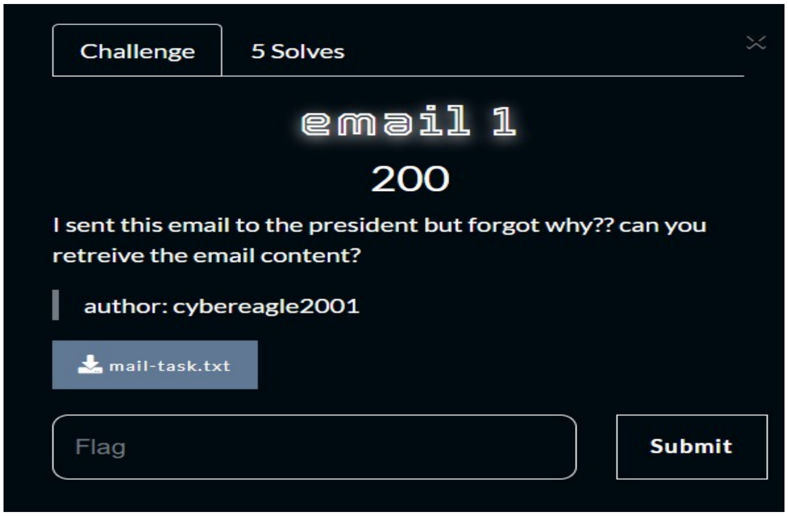
Email Series Writeup
cybereagle2001
HackMaze V0.2

I – Email 1:



email 1

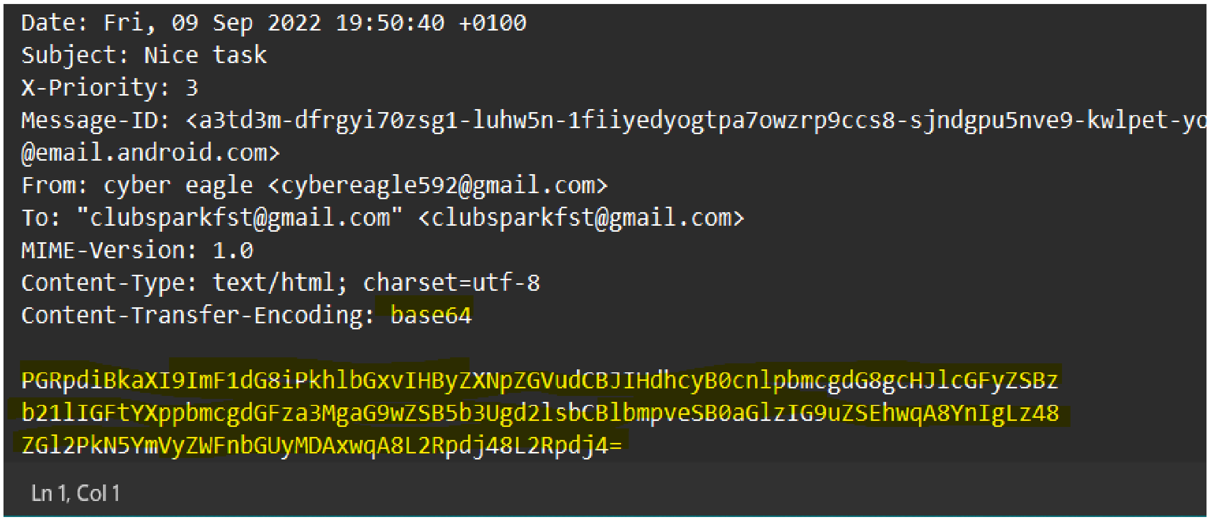
200

I sent this email to the president but forgot why?? can you retreive the email content?

> author: cybereagle2001

In this series users need to analyse an Original Email file in order to track the life cycle of an email. The sender information and the email content.
It's not a hard serie specially for those who are used to read email headers.
An email header is read from bottom to head starting from the content to the servers and smtp servers that allowed the transition of the email.

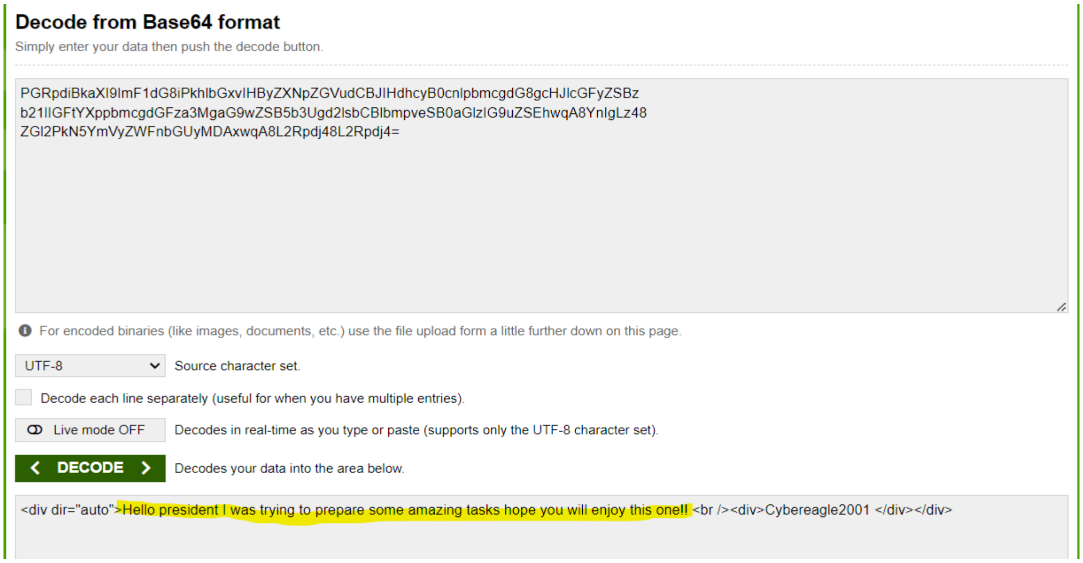
If we go to the bottom of the email we can see the following:



```
Date: Fri, 09 Sep 2022 19:50:40 +0100
Subject: Nice task
X-Priority: 3
Message-ID: <a3td3m-dfrgyi70zsg1-luhw5n-1fiiyedyogtpa7owzrp9ccs8-sjndgpu5nve9-kwlpet-yo
@email.android.com>
From: cyber eagle <cybereagle592@gmail.com>
To: "clubsparkfst@gmail.com" <clubsparkfst@gmail.com>
MIME-Version: 1.0
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: base64

PGRpdiBkaXI9ImF1dG8iPkhlbGxvIHByZXNpZGVudCBJIHdhcyB0cnlpbmcgdG8gcHJlcGFyZSBz
b21lIGFtYXppbmcgdGFza3MgaG9wZSB5b3Ugd2lsbCBlbmpveSB0aGlzIG9uZSEhwqA8YnIgLz48
ZGl2PkN5YmVyZWFnbGUyMDAxwqA8L2Rpdj48L2Rpdj4=
```

we can see that the content of the email is encoded as base64 which is a well known encoding algorithm. We can use the base64 website :



Decode from Base64 format

Simply enter your data then push the decode button.

```
PGRpdiBkaXI9ImF1dG8iPkhlbGxvIHByZXNpZGVudCBJIHdhcyB0cnlpbmcgdG8gcHJlcGFyZSBz
b21lIGFtYXppbmcgdGFza3MgaG9wZSB5b3Ugd2lsbCBlbmpveSB0aGlzIG9uZSEhwqA8YnIgLz48
ZGl2PkN5YmVyZWFnbGUyMDAxwqA8L2Rpdj48L2Rpdj4=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

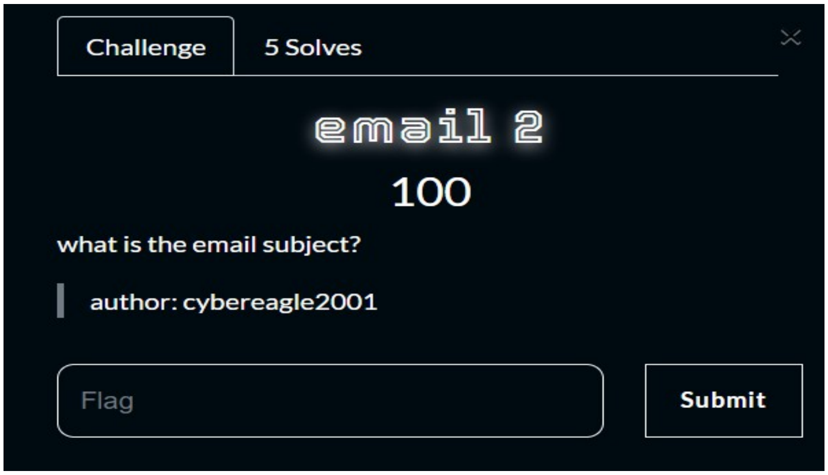
DECODE Decodes your data into the area below.

```
<div dir="auto">Hello president I was trying to prepare some amazing tasks hope you will enjoy this one!! <br /><div>Cybereagle2001 </div></div>
```

this is the content of our email and the flag is :

ESFST{Hello president I was trying to prepare some amazing tasks hope you will enjoy this one!!}

II – Email 2:



email 2

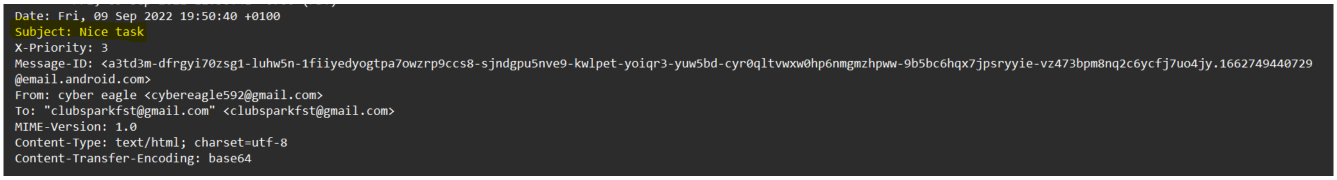
100

what is the email subject?

author: cybereagle2001

The subject of the email can give us a lot of information we can even detect fishing through the subject of the received email if we have suspecious words and specially those related to winning prizes or lottery because at 90% of the time if not more are fishing attacks where the hacker is trying to manipulate the users to gain his credentials or download trojans.

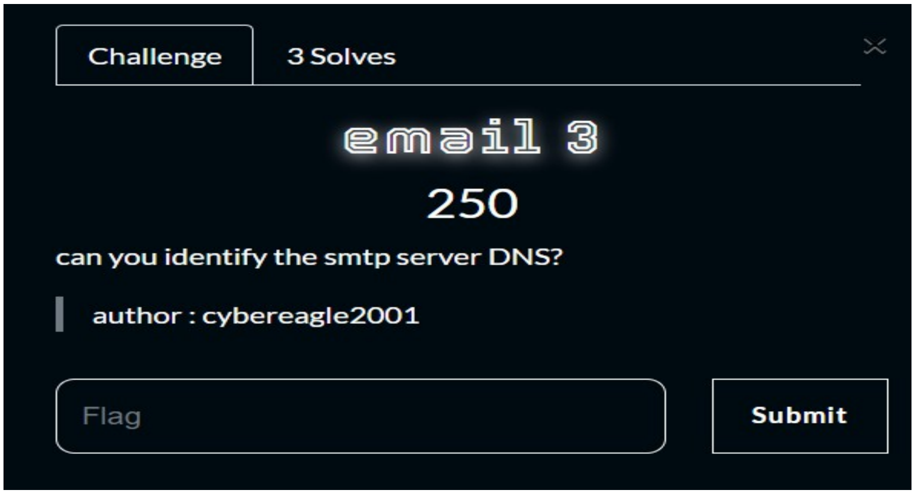
This is an easy task because actually when analyzing the email header we can see the line subject:



```
Date: Fri, 09 Sep 2022 19:50:40 +0100
Subject: Nice task
X-Priority: 3
Message-ID: <a3td3m-dfrgyi70zsg1-luhw5n-1fiiyedyogtpa7owzrp9ccs8-sjndgpu5nve9-kwlpet-yoiqr3-yuw5bd-cyr0qltvwxw0hp6nmgmzhpww-9b5bc6hqx7jpsryyie-vz473bpm8nq2c6ycfj7uo4jy.1662749440729
@email.android.com>
From: cyber eagle <cybereagle592@gmail.com>
To: "clubsparkfst@gmail.com" <clubsparkfst@gmail.com>
MIME-Version: 1.0
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: base64
```

The second flag is : ESFST{Nice task}

III – Email 3



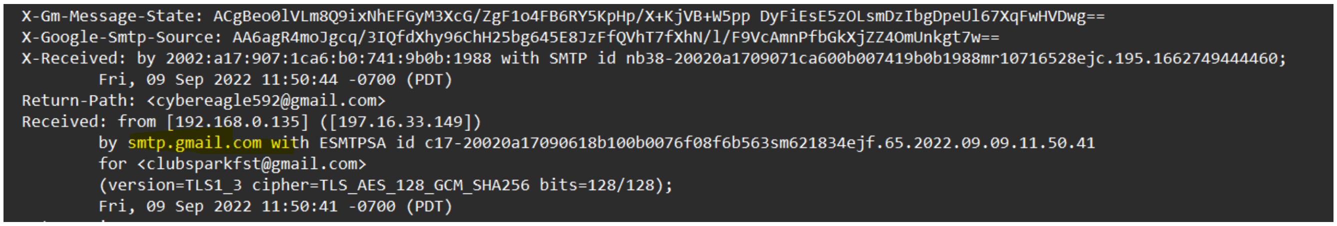
email 3

250

can you identify the smtp server DNS?

author : cybereagle2001

Simple Mail Transfer Protocol is an Internet standardcommunication protocol for electronic mail transmission. Mail servers and other message transfer agents use SMTP to send and receive mail messages. It's so intresting to have the ability to track the DNS (domain name System) of the smtp server because it will allow us to to track the path the email went through:

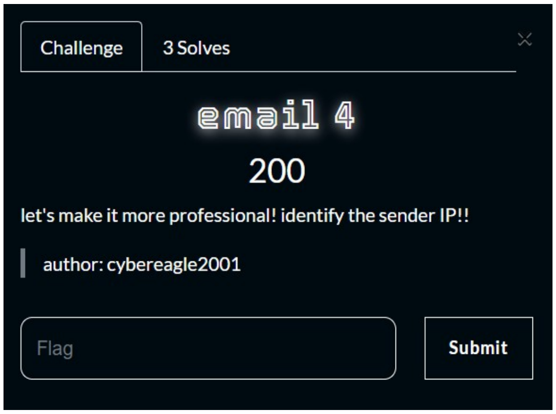


```
X-Gm-Message-State: ACgBeo0lVLm8Q9ixNhEFGyM3XcG/ZgF1o4FB6RY5KpHp/X+KjVB+W5pp DyFiEsE5zOLsmDzIbgDpeUl67XqFwHVDwg==
X-Google-Smtp-Source: AA6agR4moJgcq/3IQfdXhy96ChH25bg645E8JzFfQVhT7fXhN/l/F9VcAmnPfbGkXjZZ4OmUnkgt7w==
X-Received: by 2002:a17:907:1ca6:b0:741:9b0b:1988 with SMTP id nb38-20020a1709071ca600b007419b0b1988mr10716528ejc.195.1662749444460;
        Fri, 09 Sep 2022 11:50:44 -0700 (PDT)
Return-Path: <cybereagle592@gmail.com>
Received: from [192.168.0.135] ([197.16.33.149])
        by smtp.gmail.com with ESMTPSA id c17-20020a17090618b100b0076f08f6b563sm621834ejf.65.2022.09.09.11.50.41
        for <clubsparkfst@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Fri, 09 Sep 2022 11:50:41 -0700 (PDT)
```

we can see that the email went through the smtp server of gmail our flag is :

ESFST{smtp.gmail.com}

IV – Email 4 :



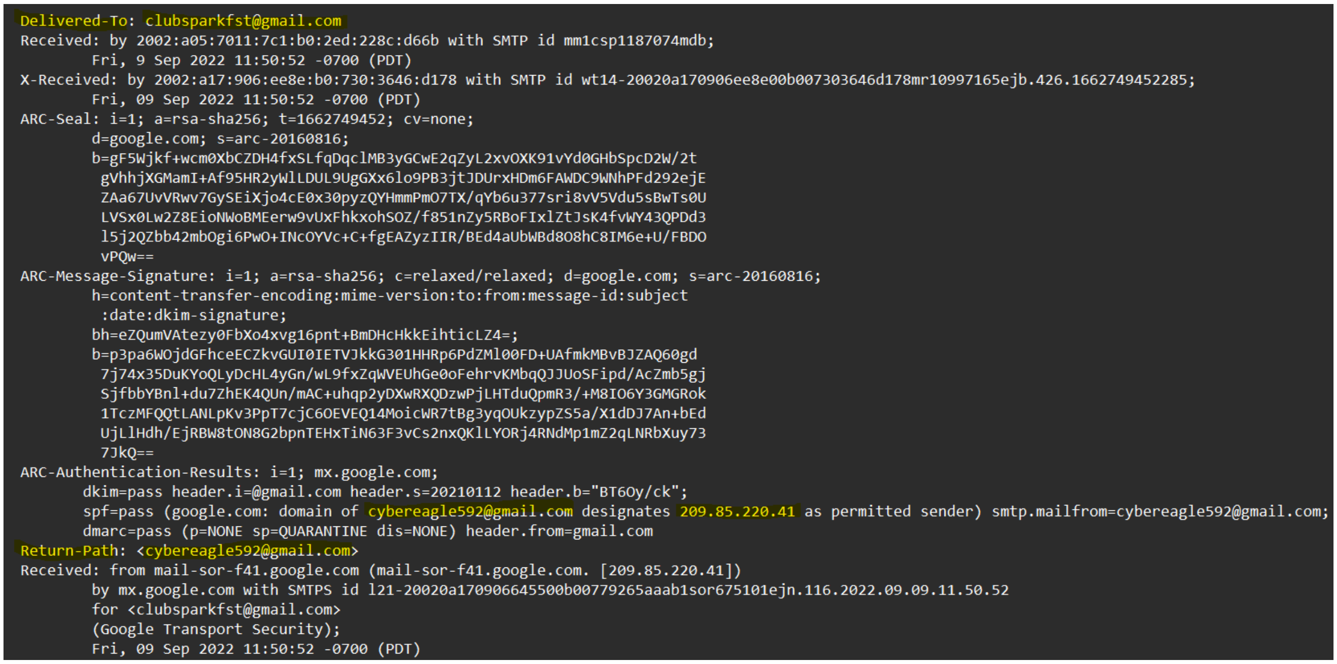
email 4

200

let's make it more professional! identify the sender IP!!

author: cybereagle2001

Let's try to identify the sender IP which is so important when it comes to identifying the hackers in Digital investigation or incident response. To do so we need to go to the TOP of our email header where we can find the sender info :

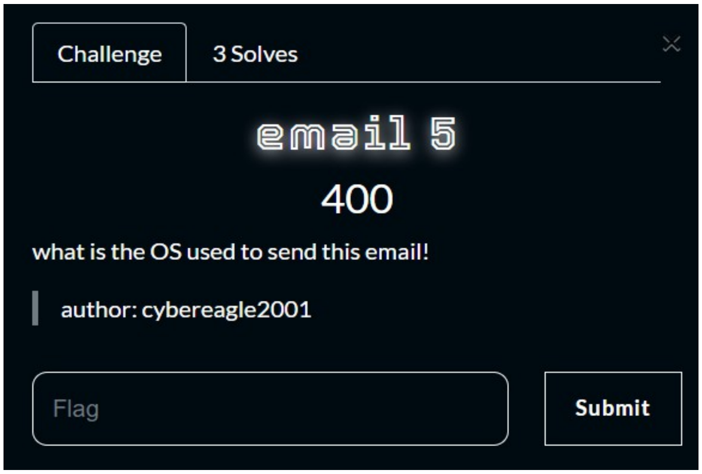


```
Delivered-To: clubsparkfst@gmail.com
Received: by 2002:a05:7011:7c1:b0:2ed:228c:d66b with SMTP id mm1csp1187074mdb;
        Fri, 9 Sep 2022 11:50:52 -0700 (PDT)
X-Received: by 2002:a17:906:ee8e:b0:730:3646:d178 with SMTP id wt14-20020a170906ee8e00b007303646d178mr10997165ejb.426.1662749452285;
        Fri, 09 Sep 2022 11:50:52 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1662749452; cv=none;
        d=google.com; s=arc-20160816;
        b=gF5Wjkf+wcm0XbCZDH4fxSLfqDqclMB3yGCwE2qZyL2xvOXK91vYd0GHbSpcD2W/2t
         gVhhjXGMamI+Af95HR2yWlLDUL9UgGXx6lo9PB3jtJDUrxHDm6FAWDC9WNhPFd292ejE
         ZAa67UvVRwv7GySEiXjo4cE0x30pyzQYHmmPmO7TX/qYb6u377sri8vV5Vdu5sBwTs0U
         LVSx0Lw2Z8EioNWoBMEerw9vUxFhkxohSOZ/f851nZy5RBoFIxlZtJsK4fvWY43QPDd3
         l5j2QZbb42mbOgi6PwO+INcOYVc+C+fgEAZyzIIR/BEd4aUbWBd8O8hC8IM6e+U/FBDO
         vPQw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=content-transfer-encoding:mime-version:to:from:message-id:subject
         :date:dkim-signature;
        bh=eZQumVAtezy0FbXo4xvg16pnt+BmDHcHkkEihticLZ4=;
        b=p3pa6WOjdGFhceECZkvGUI0IETVJkkG301HHRp6PdZMl00FD+UAfmkMBvBJZAQ60gd
         7j74x35DuKYoQLyDcHL4yGn/wL9fxZqWVEUhGe0oFehrvKMbqQJJUoSFipd/AcZmb5gj
         SjfbbYBnl+du7ZhEK4QUn/mAC+uhqp2yDXwRXQDzwPjLHTduQpmR3/+M8IO6Y3GMGRok
         1TczMFQQtLANLpKv3PpT7cjC6OEVEQ14MoicWR7tBg3yqOUkzypZS5a/X1dDJ7An+bEd
         UjLlHdh/EjRBW8tON8G2bpnTEHxTiN63F3vCs2nxQKlLYORj4RNdMp1mZ2qLNRbXuy73
         7JkQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b="BT6Oy/ck";
       spf=pass (google.com: domain of cybereagle592@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=cybereagle592@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <cybereagle592@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id l21-20020a170906645500b00779265aaab1sor675101ejn.116.2022.09.09.11.50.52
        for <clubsparkfst@gmail.com>
        (Google Transport Security);
        Fri, 09 Sep 2022 11:50:52 -0700 (PDT)
```

this email is sent to clubsparkfst@gmail.com from the email cybereagle592@gmail.com this email address designate the IP address 209.85.220.41 which is the sender IP and if we will answer this email it will go to cybereagle592@gmail.com if the Return-Path is not the same email address as the sender it means that that email is spoofed.

Our flag is : `ESFST{209.85.220.41}`

V – Email 5:



email 5

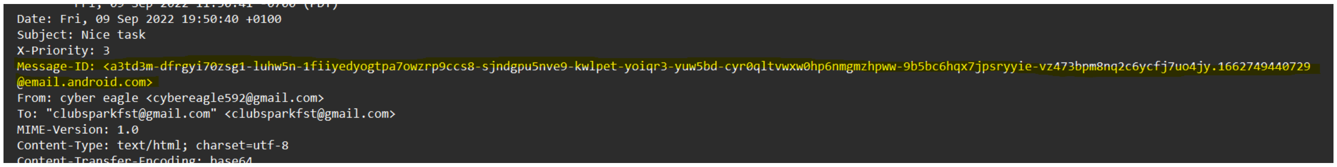
400

what is the OS used to send this email!

author: cybereagle2001

Email like anyother digital file or document reveals a lot about our machines we can identify the operating system running on my device while sending the email which can give us an idea about our hacker.

If we will be more attentive to our email header we can see this :



```
        Fri, 09 Sep 2022 11:50:41 -0700 (PDT)
Date: Fri, 09 Sep 2022 19:50:40 +0100
Subject: Nice task
X-Priority: 3
Message-ID: <a3td3m-dfrgyi70zsg1-luhw5n-1fiiyedyogtpa7owzrp9ccs8-sjndgpu5nve9-kwlpet-yoiqr3-yuw5bd-cyr0qltvwxw0hp6nmgmzhpww-9b5bc6hqx7jpsryyie-vz473bpm8nq2c6ycfj7uo4jy.1662749440729
@email.android.com>
From: cyber eagle <cybereagle592@gmail.com>
To: "clubsparkfst@gmail.com" <clubsparkfst@gmail.com>
MIME-Version: 1.0
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: base64
```

in the message ID we can see that the email ends with @android.com which means that the user used an android device to send the email !!!

Our last flag in this serie is : ESFST{android}