Mail_Mystery

We are given a file named “Mail_Mystery” but it doesn’t specify the file type. Using the command ‘file’ in the terminal can help us identify the file type.

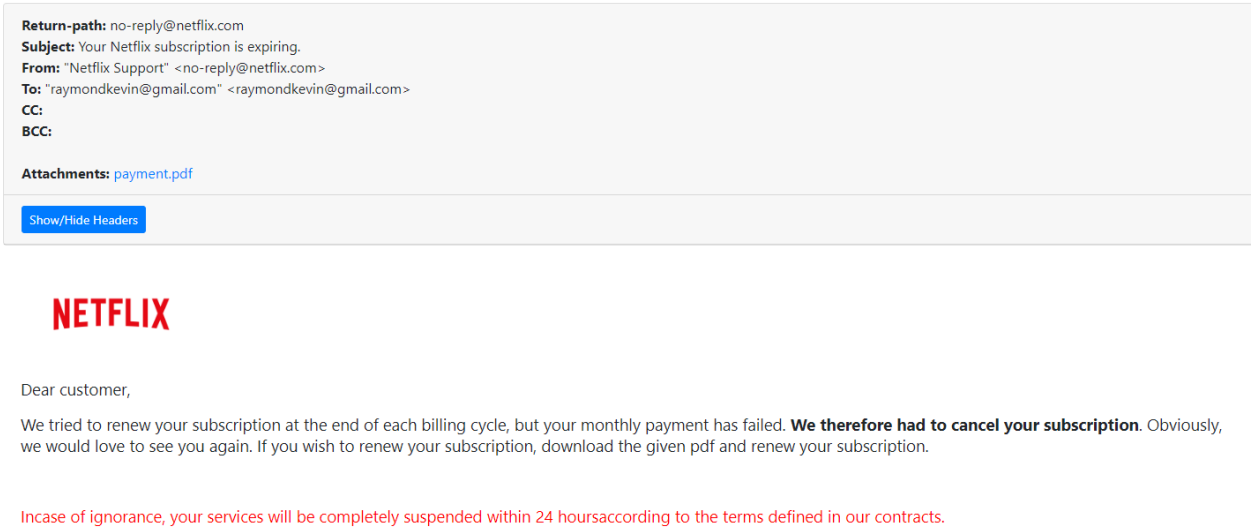
```
└─$ file mail_mystery
mail_mystery: SMTP mail, ASCII text, with CRLF line terminators
```

The file contains ASCII text and shows SMTP mail which tells us it could be a ‘.eml’ file.

By using ‘cat’ command, we can now see that it is indeed a ‘.eml’ file.

```
└─$ cat mail_mystery
Delivered-To: raymondkevin@gmail.com
Received: by 2002:ab0:5a4c:0:b0:7a7:41eb:68b0 with SMTP id m12csp2148870uad;
 Mon, 11 Sep 2023 01:45:15 -0700 (PDT)
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
  by mx.google.com with SMTPS id
 g21-20020a9d5f95000000b006bcb2a3267dsor2786424oti.1.2023.09.11.01.45.14
   for <raymondkevin@gmail.com>        (Google Transport Security);
 Mon, 11 Sep 2023 01:45:15 -0700 (PDT)
X-Received: by 2002:a4a:d291:0:b0:571:28d5:2c71 with SMTP id
 h17-20020a4ad291000000b0057128d52c71mr8940038oos.2.1694421915086;
 Mon, 11 Sep 2023 01:45:15 -0700 (PDT)
X-Received: by 2002:a05:6830:1493:b0:6bc:f639:713d with SMTP id
 s19-20020a056830149300b006bcf639713dmr10375170otq.30.1694421914025; Mon, 11
 Sep 2023 01:45:14 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1694421915; cv=none;        d=google.com;
 s=arc-20160816;
 b=q65HjyAwNd8OlhrsLdSGE7w9+S4E9oXQBFBYSWNccwijxiJ0pFkXS/b3pkPiFtZfsH
 5qSQEvgMtPgDq74YvlqwG2jPbVgO7IvHpq/npeprSWJLrZhjq9YO0ATEoVc2HKpjkx8W
 5DZyYV0PWWOUxGLcQsN/Q8XLjoJdXhW31fMwlZUvqYCePMQoLxL3VwZS7tAD5sN8/TfU
```

For viewing it, we can go to “https://msgeml.com/” and upload the file.



We can see the details of the mail, like -
Return-path: no-reply@netflix.com
Subject: Your Netflix subscription is expiring.
From: "Netflix Support" <no-reply@netflix.com>
To: "raymondkevin@gmail.com" <raymondkevin@gmail.com>
CC:
BCC:

Attachments: payment.pdf

The text in the mail says that “If you wish to renew your subscription, download the given pdf and renew your subscription”.

Let’s go ahead and download the attached file

NETFLIX

Subject: Your Netflix subscription is expiring.

Dear customer,

We tried to renew your subscription at the end of each billing cycle, but your monthly payment has failed. **We therefore had to cancel your subscription**. Obviously, we would love to see you again. If you wish to renew your subscription, click on the link below.

REACTIVATE MY ACCOUNT

Information about your account:

E-mail

Raymondkevin@gmail.com

Service provider

Netflix

In case of ignorance, your services will be completely suspended within 24 hours according to the terms defined in our contracts.

The subject reads “Your Netflix subscription is expiring.” There seems to be a button that reads”Reactivate my account” The hyperlink takes us to the Netflix Subscription plans page:- “https://www.netflix.com/signup/planform”

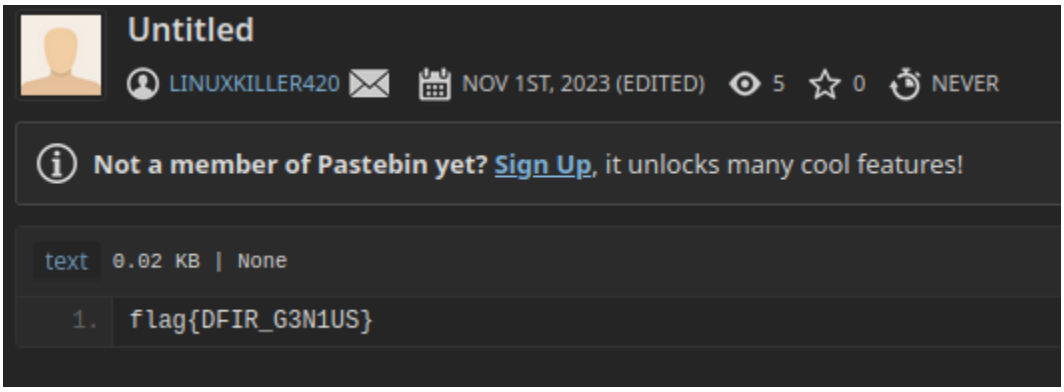
Using ‘exiftool’ reveals more information about the pdf

```
└─$ exiftool payment.pdf
ExifTool Version Number         : 12.63
File Name                       : payment.pdf
Directory                       : .
File Size                       : 105 kB
File Modification Date/Time     : 2023:11:02 04:03:00-04:00
File Access Date/Time           : 2023:11:02 06:59:55-04:00
File Inode Change Date/Time     : 2023:11:02 06:59:55-04:00
File Permissions                : -rw-------
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Page Count                      : 1
Language                        : en
Tagged PDF                      : Yes
XMP Toolkit                     : 3.1-701
Producer                        : Microsoft® Word for Microsoft 365
Creator                         : Rohit Jain
Creator Tool                    : Microsoft® Word for Microsoft 365
Create Date                     : 2023:11:02 07:57:08+0000
Modify Date                     : 2023:11:02 07:57:08+0000
Document ID                     : uuid:166D04B4-3271-4504-9D11-4DF89BBB13DF
Instance ID                     : uuid:166D04B4-3271-4504-9D11-4DF89BBB13DF
Author                          : Rohit Jain
Title                           :
Subject                         : https://pastebin.com/fh4mEK5P
```

There is a pastebin link in the Subject field. Let's go to that link :- 'https://pastebin.com/fh4mEK5P'. But it's password protected.
There doesn't seem to be any password in the strings or metadata.

Let's take a look at that pdf again. Zooming into the 'Reactivate My Account' button, some text is written "**Here's a random string '8HKFPC70hF'.**"

This could be the password for our pastebin link. Using the string as password.



And we got the flag!! - **flag{DFIR_G3N1US}.**