

BÁO CÁO BÀI TẬP

Môn học: Pháp chứng kỹ thuật số

Kỳ báo cáo: Buổi

Tên chủ đề: Email Forensics

GVHD: Nguyễn Tấn Cầm

Ngày báo cáo: 31/5/2023

Nhóm:

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2			
3			

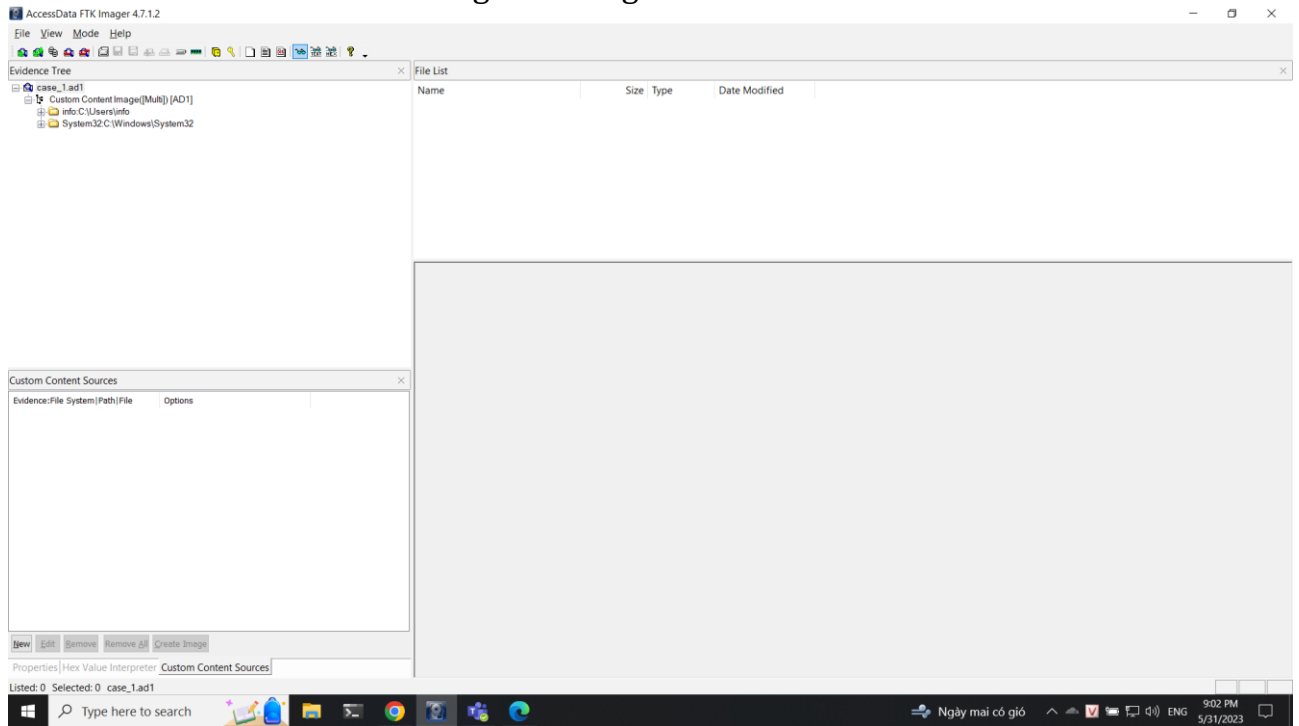
2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Thực hiện	Thành viên thực hiện	Kết quả tự đánh giá
1	Email Forensics	Tìm flag	100%	

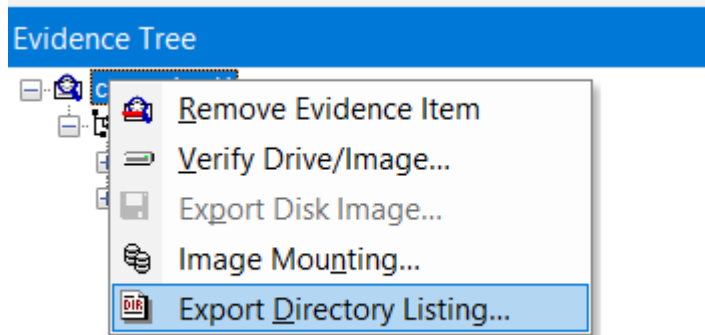
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành,

BÁO CÁO CHI TIẾT

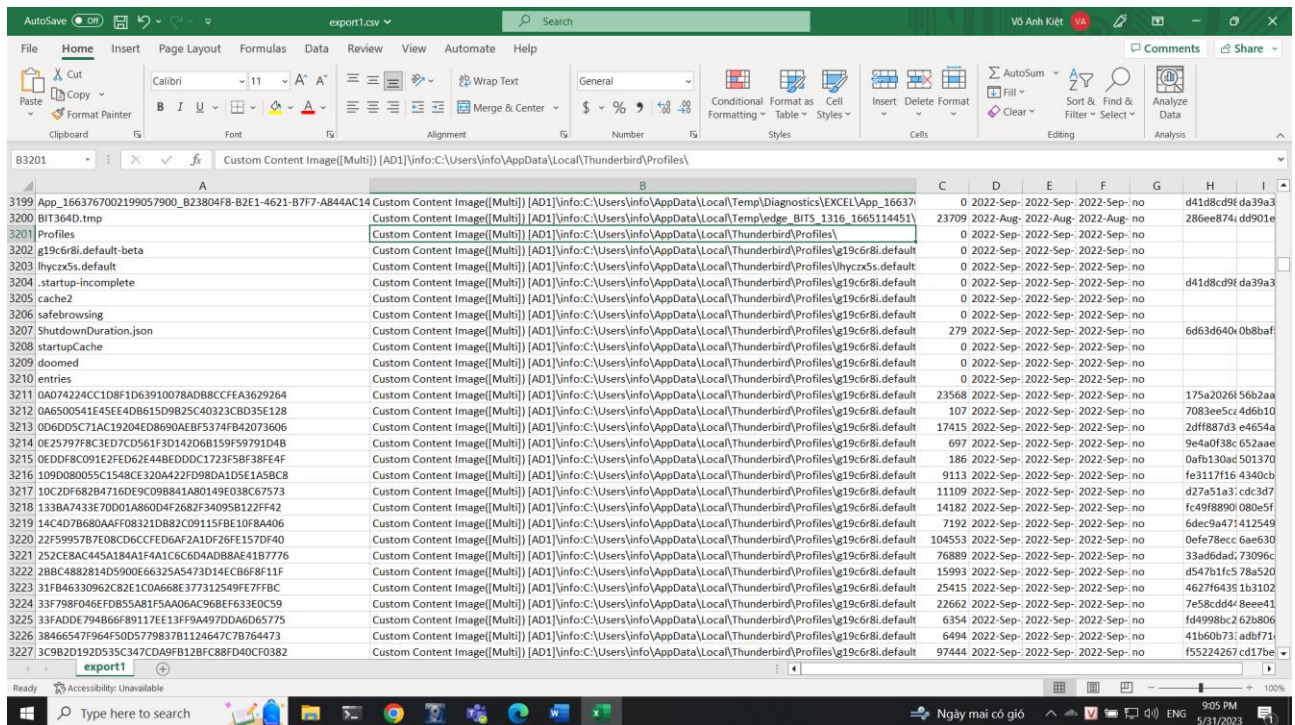
Đầu tiên ta tải file về và mở bằng FTK imager



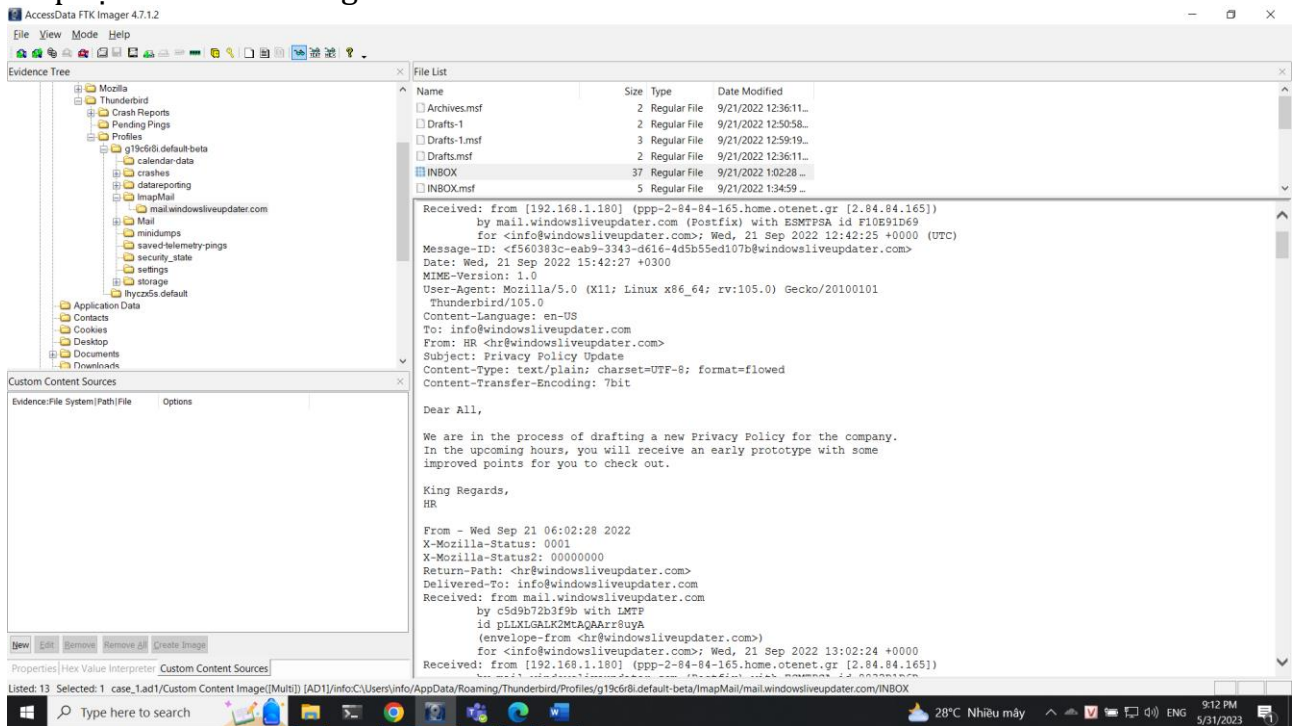
Thực hiện export directory listing



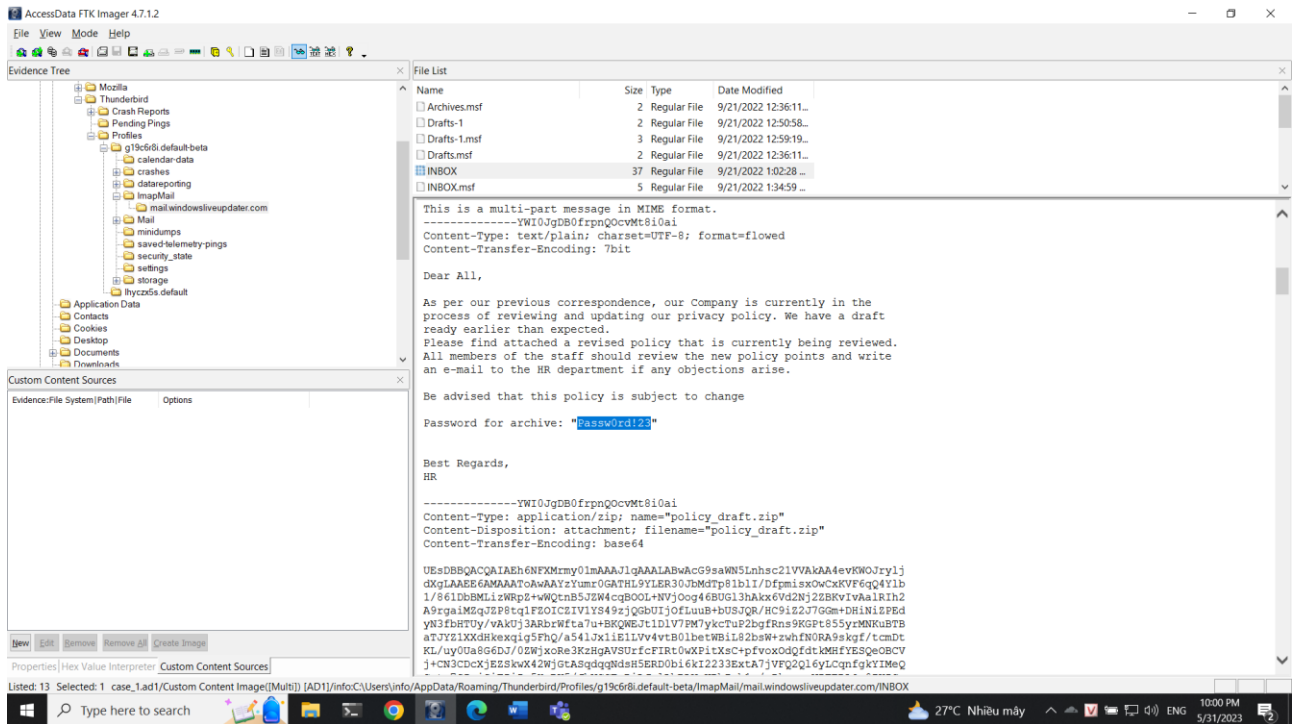
Mở file được xuất ra xem thì ta thấy thông tin của các custom images thunderbird



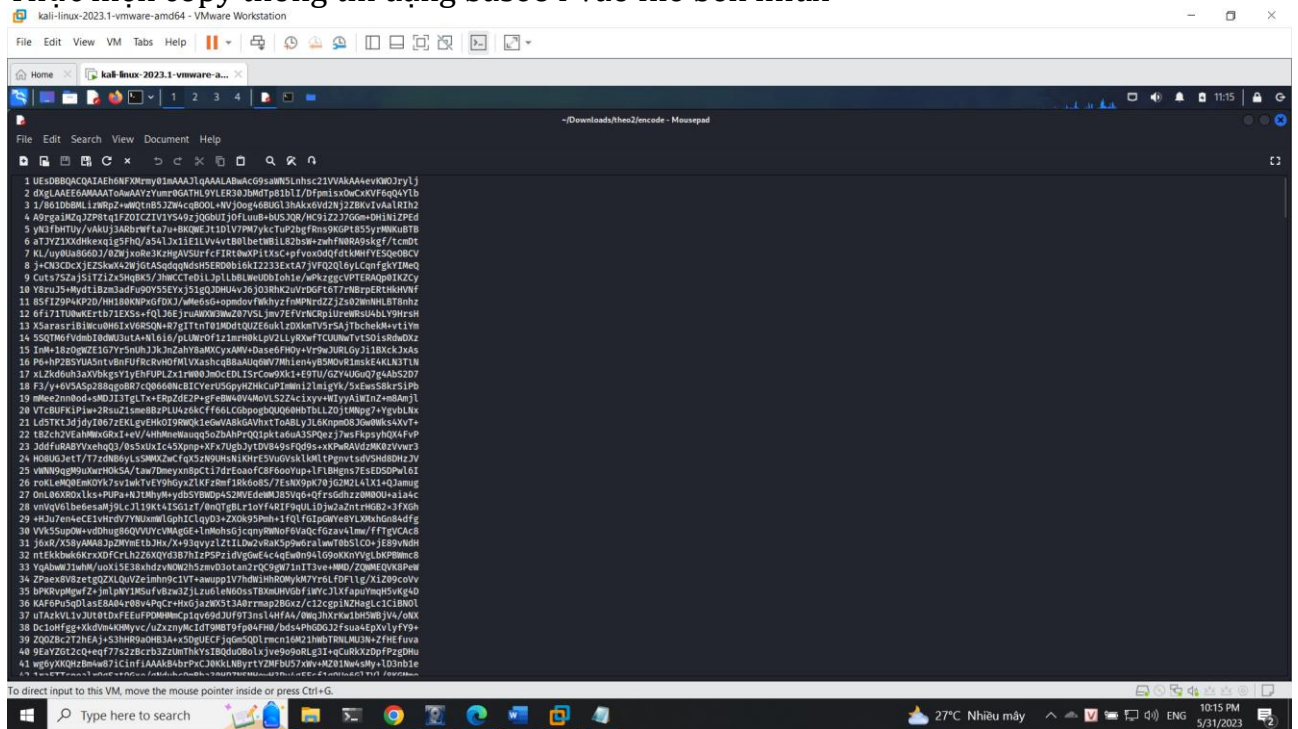
Tiếp tục xem mail trong inbox



Ta có được password khi kéo xuống phía dưới



Thực hiện copy thông tin dạng base64 vào file bên linux

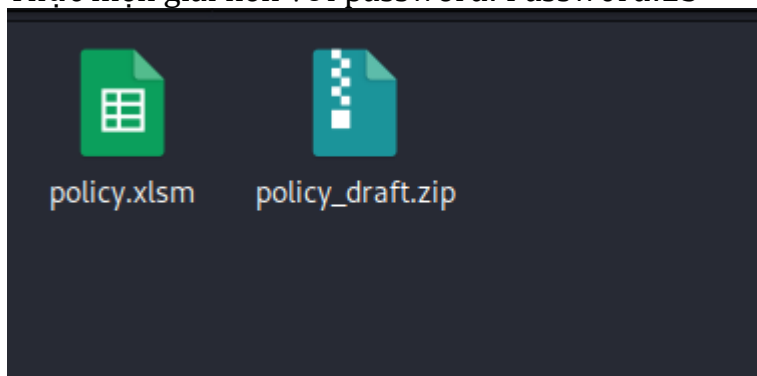


Thực hiện decode base64 và lưu thành file zip


```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~/Downloads/theo2]
$ base64 -d encode > policy_draft.zip

(kali@kali)-[~/Downloads/theo2]
$
```

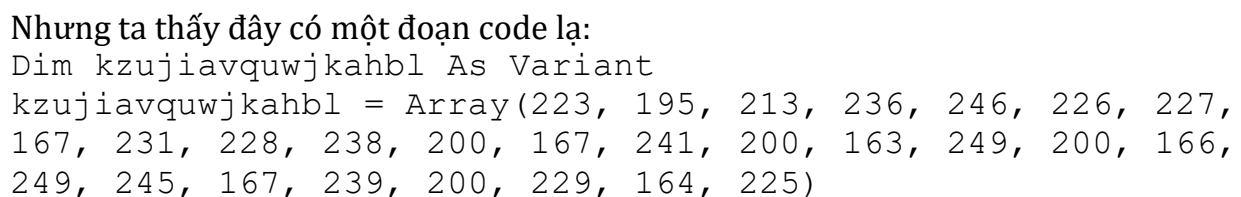
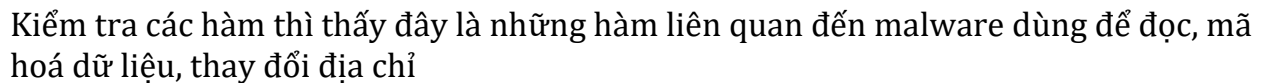
Thực hiện giải nén với password: Passw0rd!23



Cài đặt tool olevtool

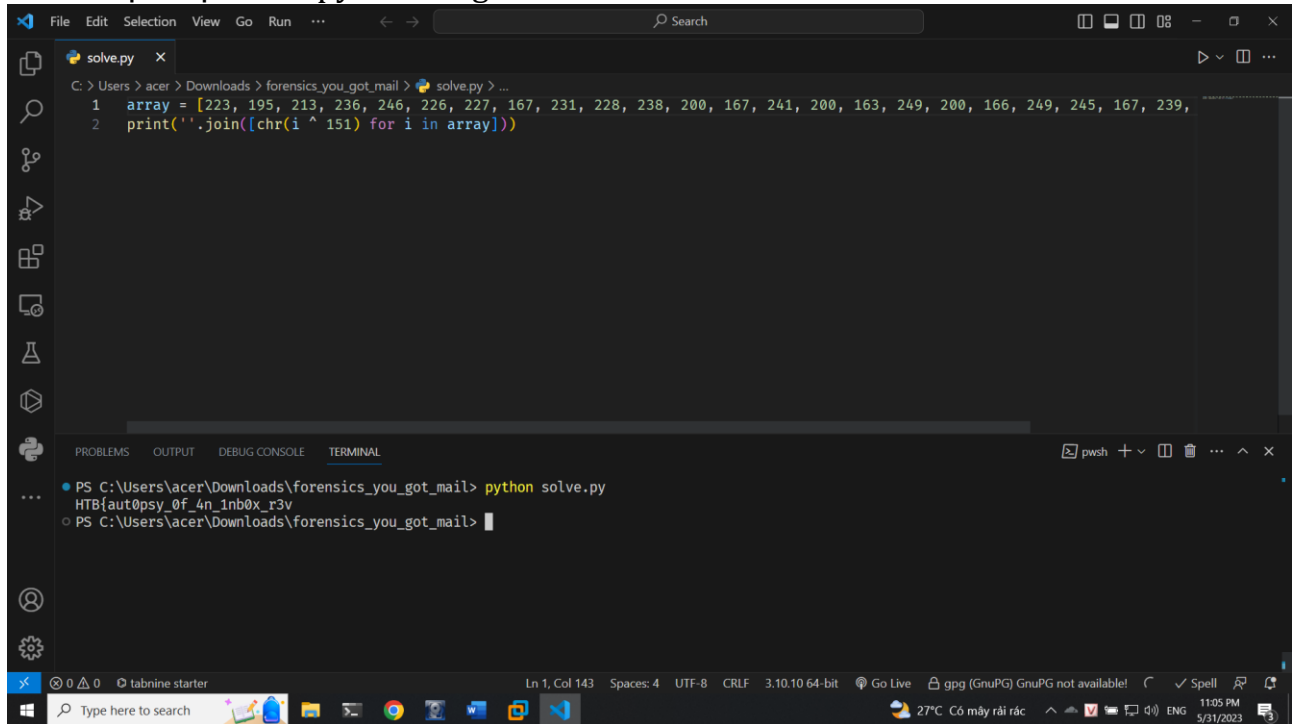
```
kali-linux-2023.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home kali-linux-2023.1-vmware-amd64
File Actions Edit View Help
olevba: command not found
(kali@kali)-[~/Downloads/theo2]
$ sudo -H pip install -U olevtools[full]
[sudo] password for kali:
Collecting olevtools[full]
  Downloading olevtools-0.60.1-py2.py3-none-any.whl (977 kB)
    977.2/977.2 kB 3.2 MB/s eta 0:00:00
Collecting pyparsing<3,≥2.1.0
  Downloading pyparsing-2.4.7-py2.py3-none-any.whl (67 kB)
    67.2/67.2 kB 0.8 MB/s eta 0:00:00
Requirement already satisfied: olefile≥0.46 in /usr/lib/python3/dist-packages (from olevtools[full]) (0.46)
Collecting easygui
  Downloading easygui-0.98.3-py2.py3-none-any.whl (92 kB)
    92.7/92.7 kB 15.8 MB/s eta 0:00:00
Collecting colorclass
  Downloading colorclass-2.2.2-py2.py3-none-any.whl (18 kB)
Collecting pcodedmp>=1.2.5
  Downloading pcodedmp-1.2.6-py2.py3-none-any.whl (38 kB)
Collecting msocrypt-tool
  Downloading msocrypt-tool-5.0.1-py3-none-any.whl (34 kB)
Collecting XLMMacroDeobfuscator
  Downloading XLMMacroDeobfuscator-0.2.7-py3-none-any.whl (50 kB)
    51.0/51.0 kB 11.5 MB/s eta 0:00:00
Requirement already satisfied: cryptography≥35.0 in /usr/lib/python3/dist-packages (from msocrypt-tool→olevtools[full]) (38.0.4)
Collecting pyxlsb2
  Downloading pyxlsb2-0.8.9-py3-none-any.whl (40 kB)
    40.0/40.0 kB 0.6 MB/s eta 0:00:00
Collecting lark-parser
  Downloading lark-parser-0.12.0-py2.py3-none-any.whl (103 kB)
    103.5/103.5 kB 13.2 MB/s eta 0:00:00
Collecting xlr2
  Downloading xlr2-1.3.4-py2.py3-none-any.whl (116 kB)
    116.5/116.5 kB 10.1 MB/s eta 0:00:00
Collecting untangle=1.2.1
  Downloading untangle-1.2.1-py3-none-any.whl (4.8 kB)
Collecting roman
  Downloading roman-4.1-py3-none-any.whl (5.5 kB)
Requirement already satisfied: defusedxml<0.8.0,≥0.7.1 in /usr/lib/python3/dist-packages (from untangle=1.2.1→XLMMacroDeobfuscator→olevtools[full]) (0.7.1)
Installing collected packages: pyxlsb2, lark-parser, easygui, xlr2, untangle, roman, pyparsing, msocrypt-tool, colorclass, XLMMac
roDeobfuscator, pcodedmp, olevtools
Attempting uninstall: pyparsing
  Found existing installation: pyparsing 3.0.9
  Not uninstalling pyparsing at /usr/lib/python3/dist-packages, outside environment /usr
  Can't uninstall 'pyparsing'. No files were found to uninstall.
Successfully installed XLMMacroDeobfuscator-0.2.7 colorclass-2.2.2 easygui-0.98.3 lark-parser-0.12.0 msocrypt-tool-5.0.1 olevtools-
0.60.1 pcodedmp-1.2.6 pyparsing-2.4.7 pyxlsb2-0.8.9 roman-4.1 untangle-1.2.1 xlr2-1.3.4
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Thực hiện giải mã file policy.xlsm



```
Dim wwiqwvyhemghupdahkj As Integer
wwiqwvyhemghupdahkj = 0
For i = 0 To 26
    wwiqwvyhemghupdahkj = wwiqwvyhemghupdahkj +
    kzujiavquwjkahbl(i) Xor 151
Next
```

Ta sẽ thực hiện code python và giải mã:

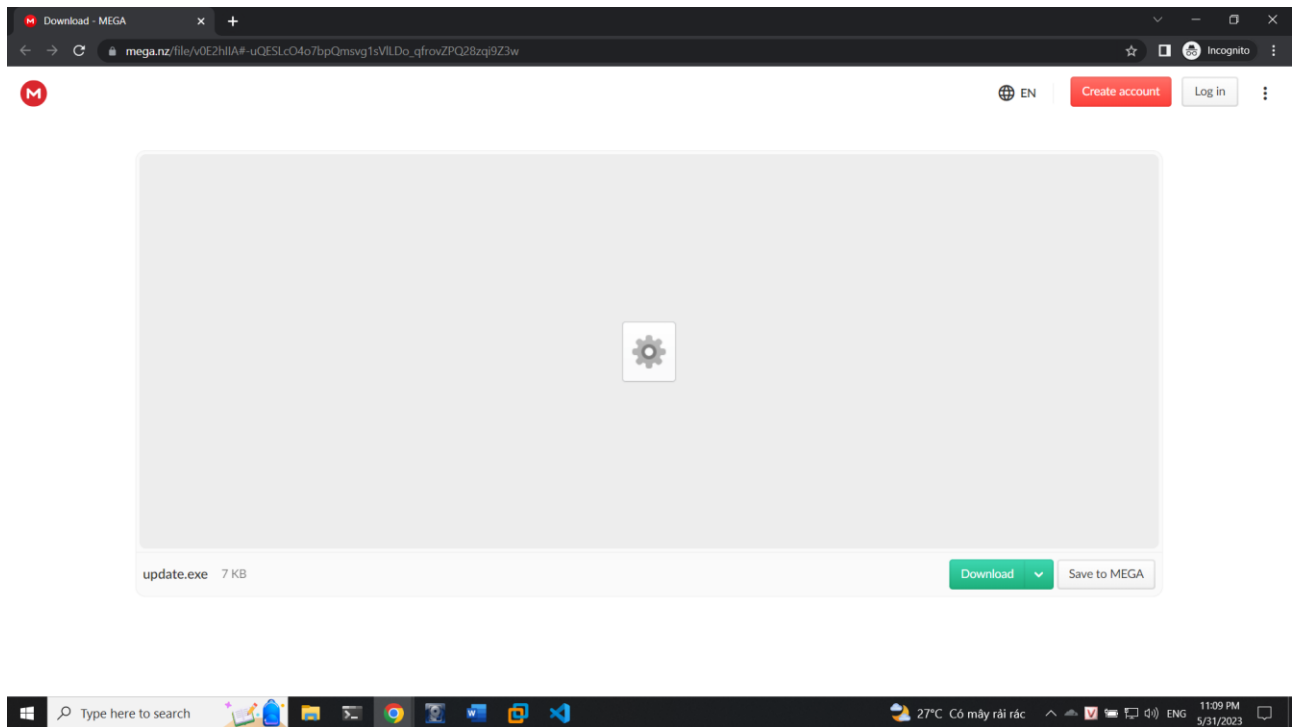


```
1 array = [223, 195, 213, 236, 246, 226, 227, 167, 231, 228, 238, 200, 167, 241, 200, 163, 249, 200, 166, 249, 245, 167, 239,
2 print(''.join([chr(i ^ 151) for i in array]))
```

```
PS C:\Users\acer\Downloads\forensics_you_got_mail> python solve.py
HTB{aut0psy_0f_4n_1nb0x_r3v
PS C:\Users\acer\Downloads\forensics_you_got_mail>
```

Ta có được flag đầu là: HTB{aut0psy_0f_4n_1nb0x_r3v

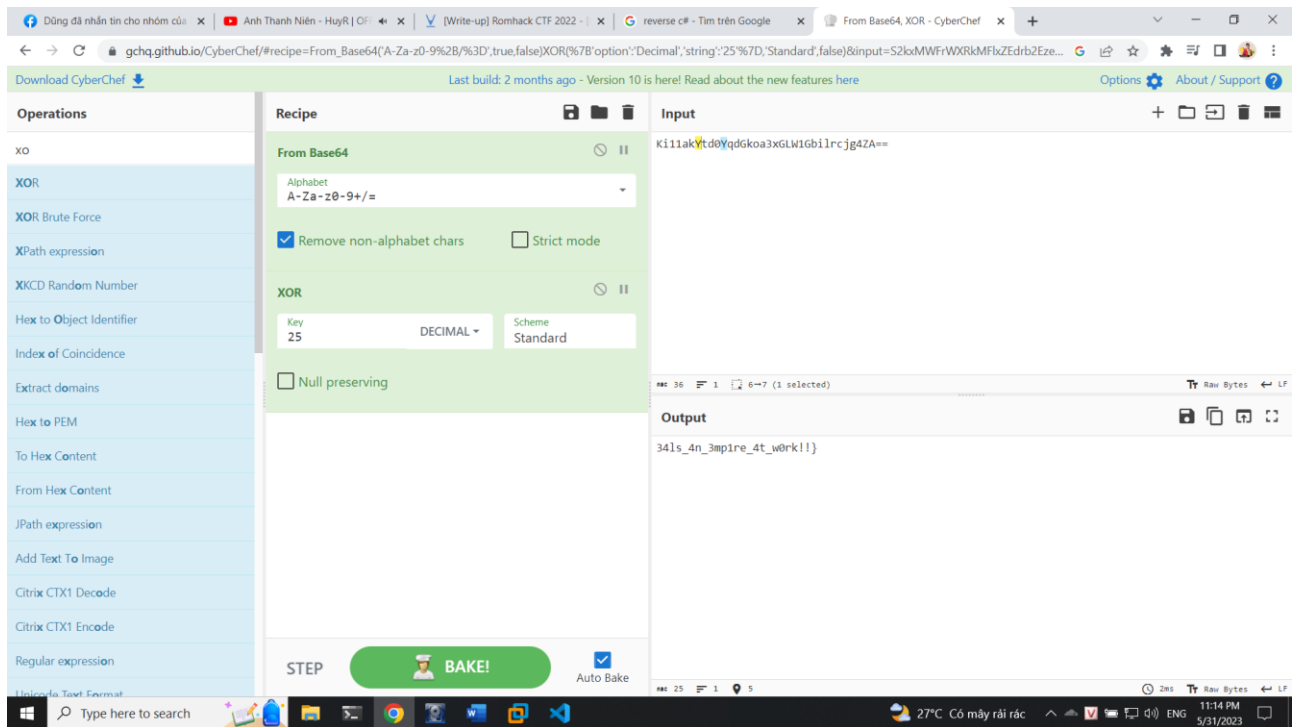
Thực hiện tải file về và thực hiện dịch ngược update.exe



Ta có được code trong phần PSEmpire_Stage1.Program

```
byte[] array2 =  
Convert.FromBase64String("KillakYtd0YqdGkoa3xGLW1Gb1lrcjg4ZA=  
=");  
for (int j = 0; j < array2.Length; j++)  
{  
    array2[j] = (byte)(array2[j] ^ Convert.ToByte(25));  
}
```

Thực hiện sử dụng cyberchef để giải mã



Ta có nữa sau của flag 34ls_4n_3mp1re_4t_w0rk!!}

Flag: HTB{aut0psy_of_4n_1nb0x_r3v34ls_4n_3mp1re_4t_w0rk!!}

*Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.
(Xem trang kế tiếp)*

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.DOCX và .PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

Ví dụ: [NT101.H11.1]-Session1_Group3.

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, trể, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT