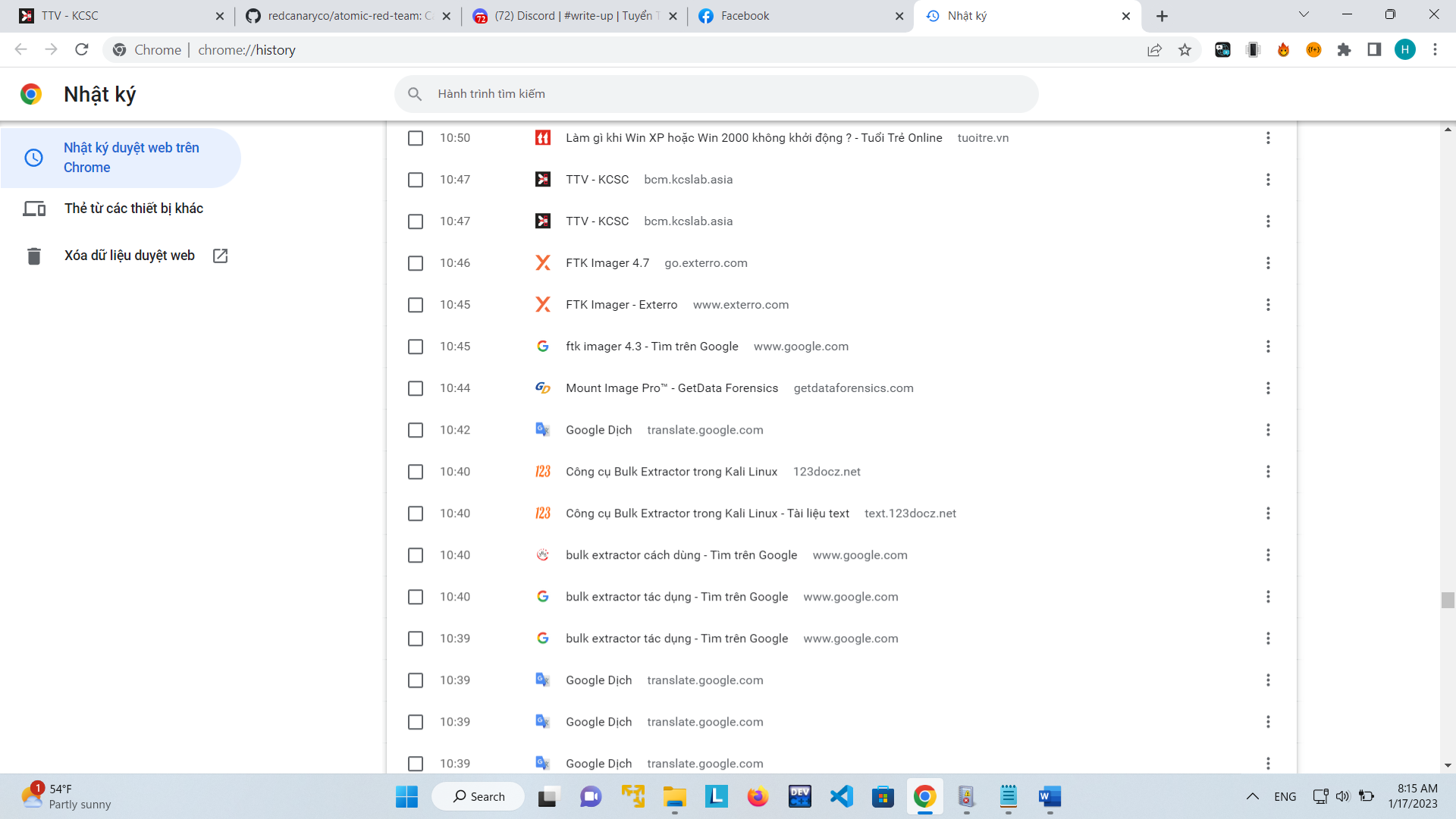
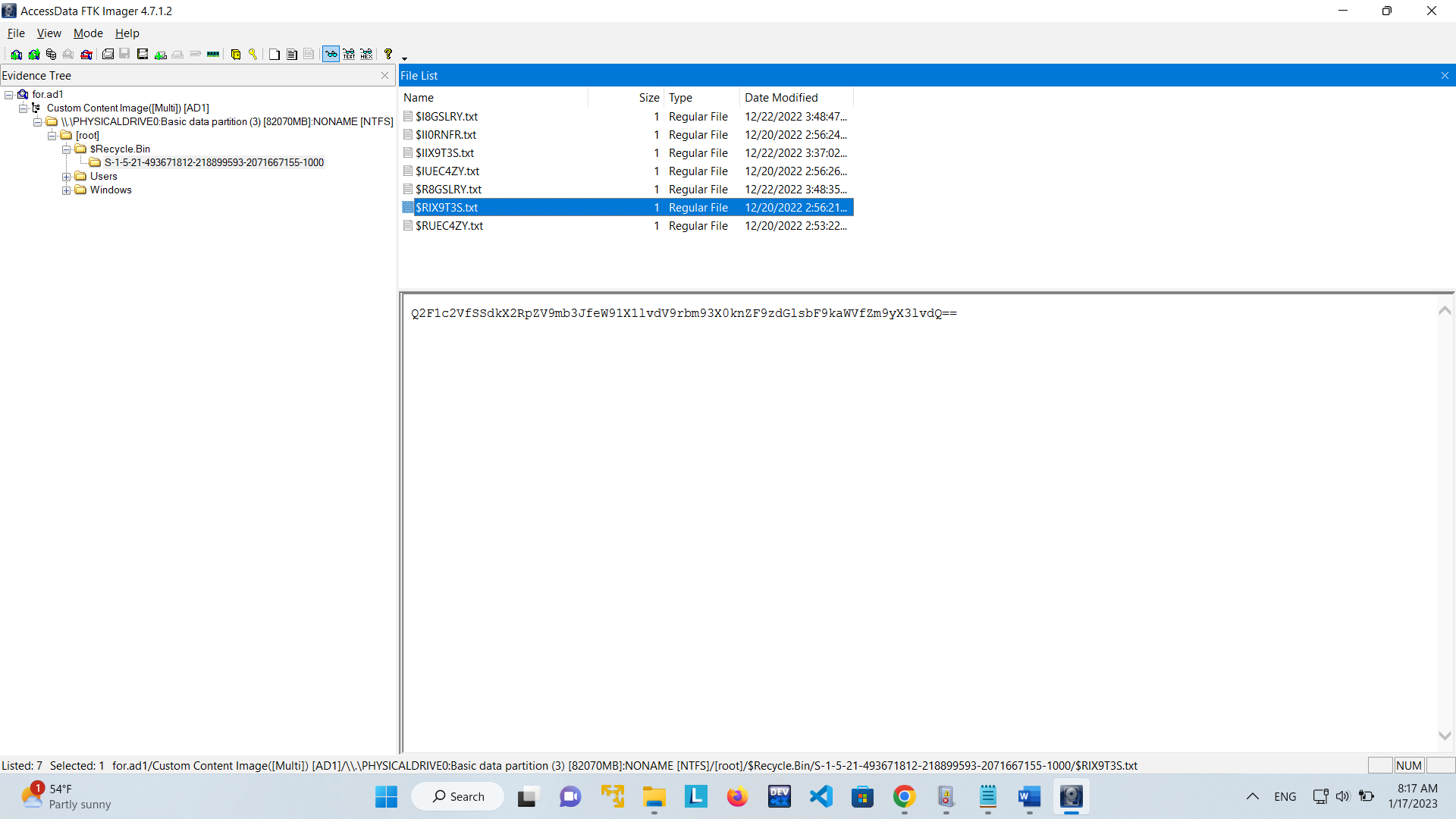
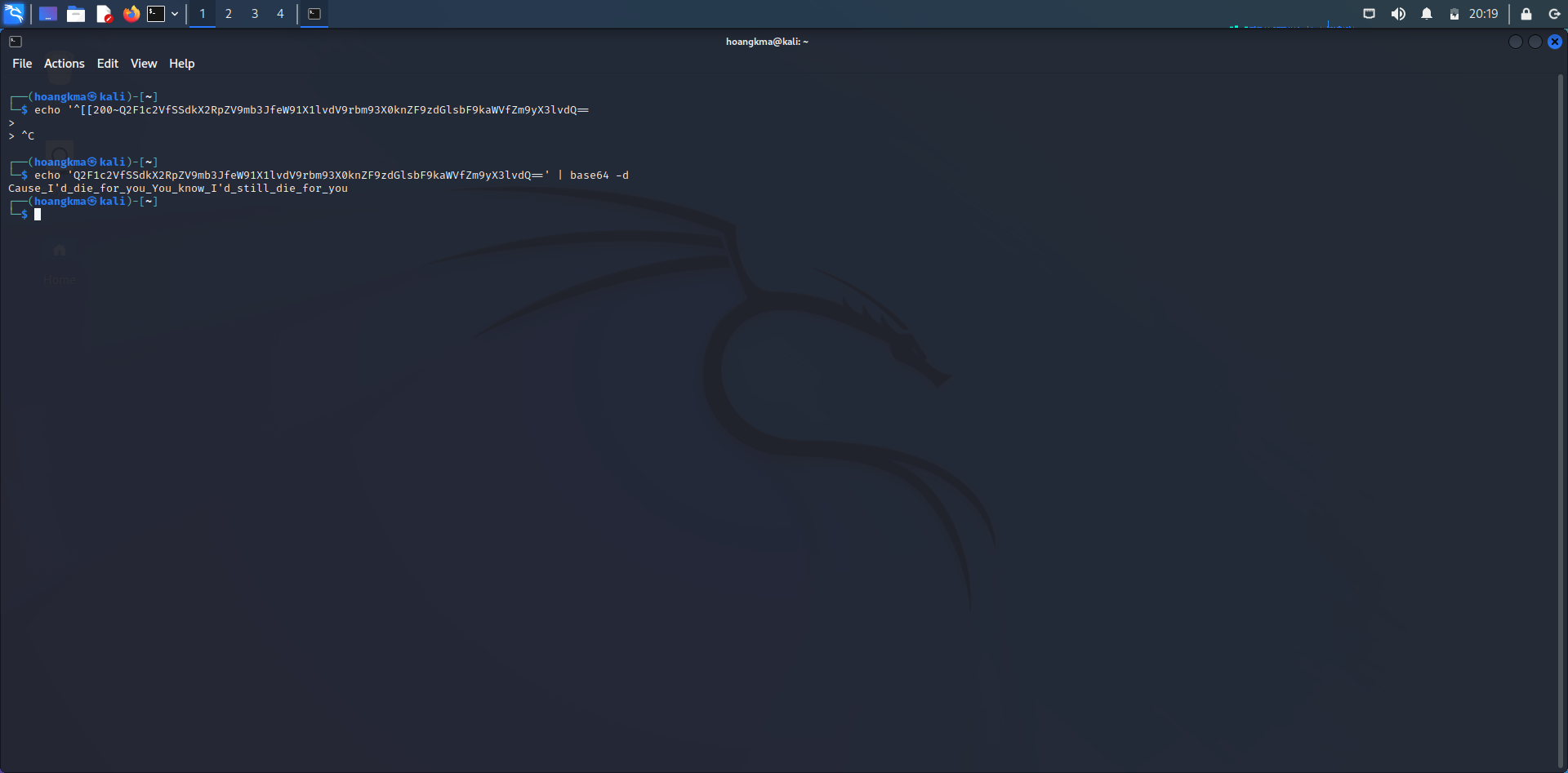
lúc đầu em mất thời gian khá lâu để tìm công cụ phân tích thích hợp cho bài

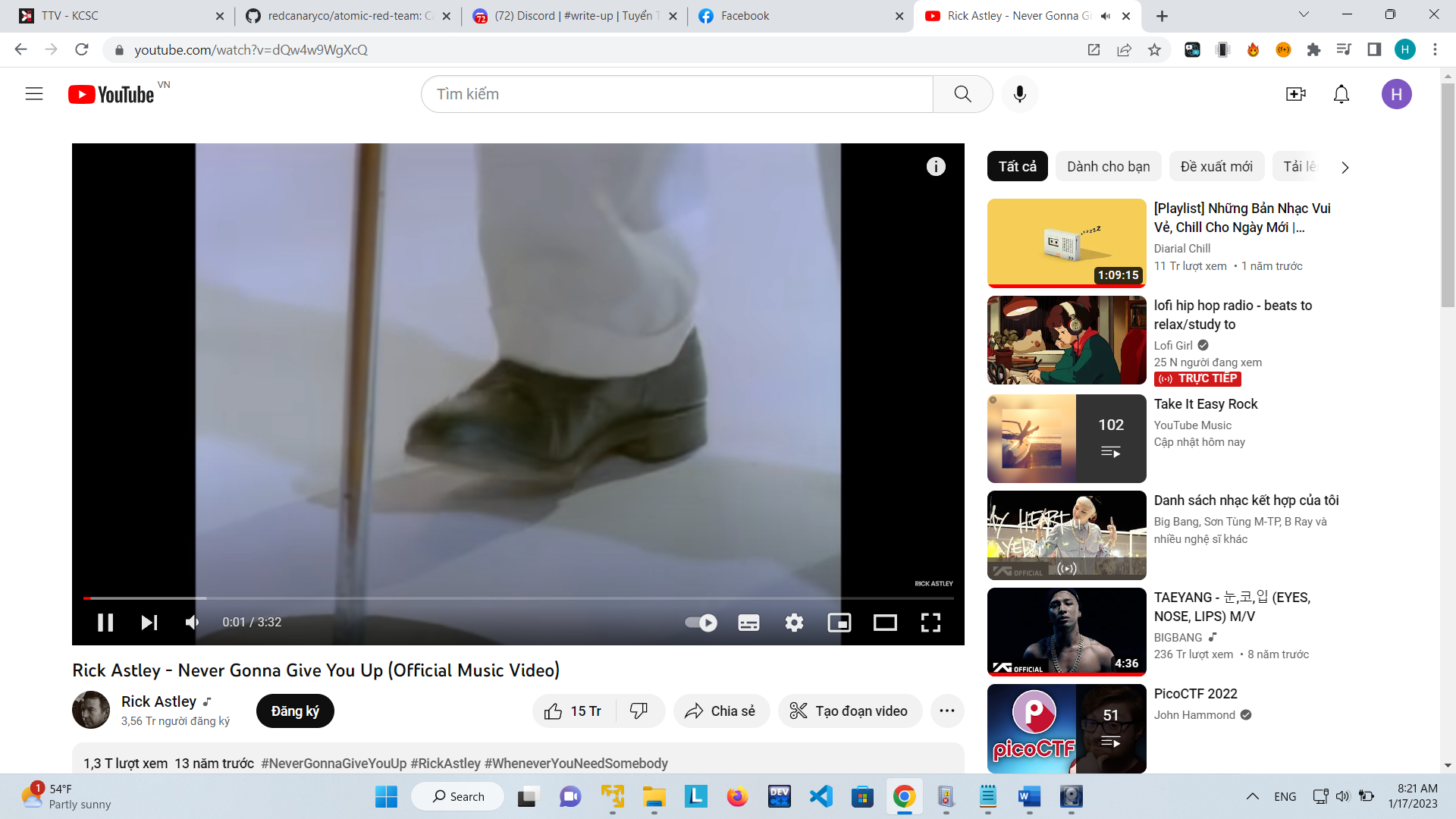
sau khi vào được disk em vào thư mục thùng rác và thấy 3 file lần lượt password và 2 file dễ thấy được mã hóa base64 em tiến hành giải mã



Giải mã em được thông điệp



Và cả ….



Do 3 file trên có tên lần lượt password ứng với file thứ 5 em mạnh dạn đoán tên file thứ 2 ứng với file thứ 6 cũng là phần cờ thứ 2 của bài

Graphical user interface, text, application

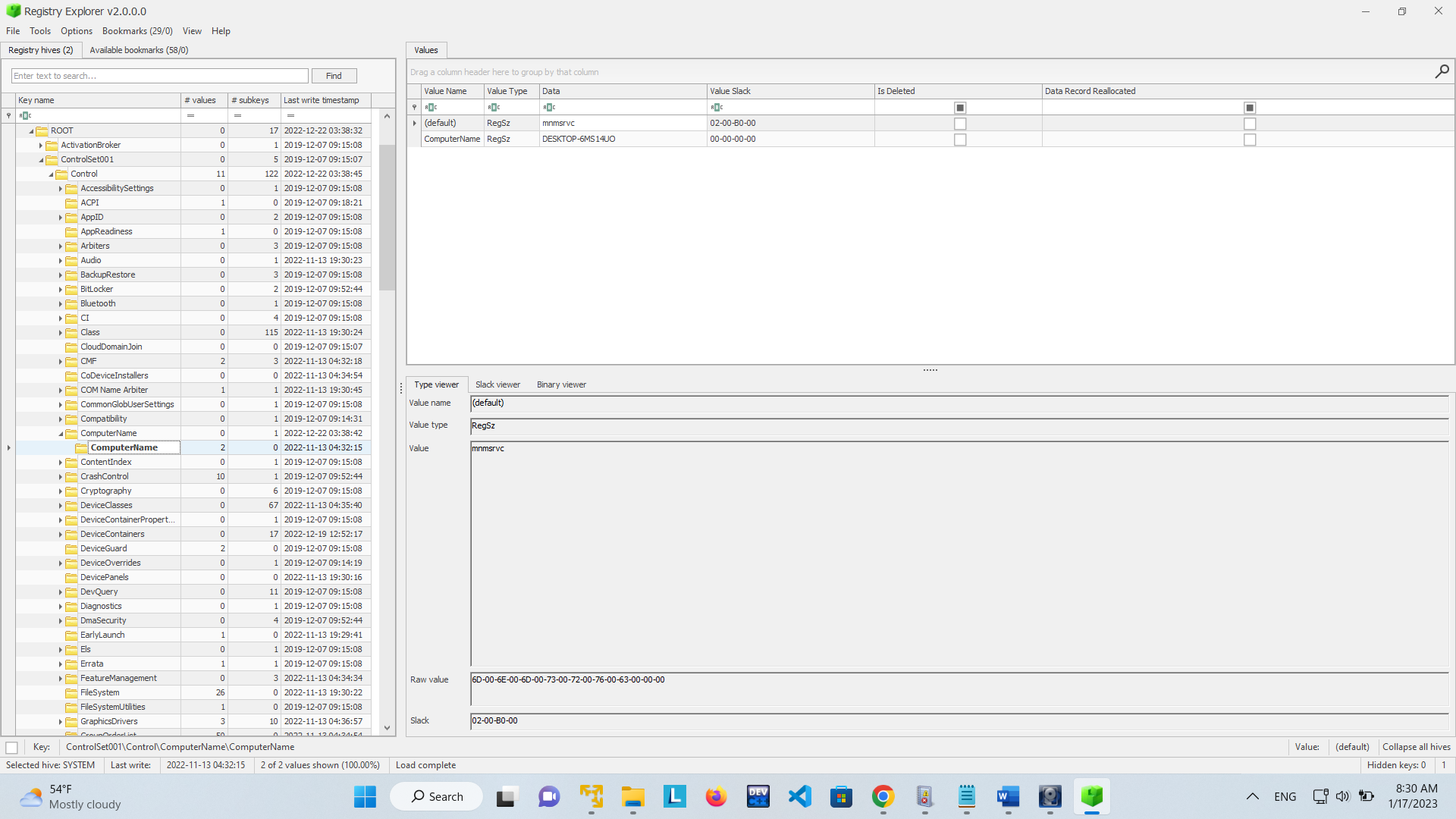
Description automatically generated

Do vậy thu được

Kaxeetxe-Cause\_I'd\_die\_for\_you\_You\_know\_I'd\_still\_die\_for\_you

Hint và spoil về hklm + phỏng đoán về file zip có tên registry explorer, em thử khởi động và thả file system vào phân tích, sau 2 lần ngu người mới đọc được bài này để sửa sai <https://sec.vnpt.vn/2021/04/windows-forensic-registry-analysis-part2/?fbclid=IwAR1SIPGadLxHaugdsA9upavuIOX11Y39CaqjE58aeVe-uSDNuLgMOVTGg5c>

Và thu được



Computer name là : 6MS14UO

Graphical user interface, text, application

Description automatically generated

Timezone có ghi SE Asia Standard Time em lên gg search có kết quả là UTC +8

Flag:KCSC{6MS14UO\_ Kaxeetxe-Cause\_I'd\_die\_for\_you\_You\_know\_I'd\_still\_die\_for\_you\_UTC8}

(em quên mất cái gạch nối giữa 3 cái như nào rồi :v)