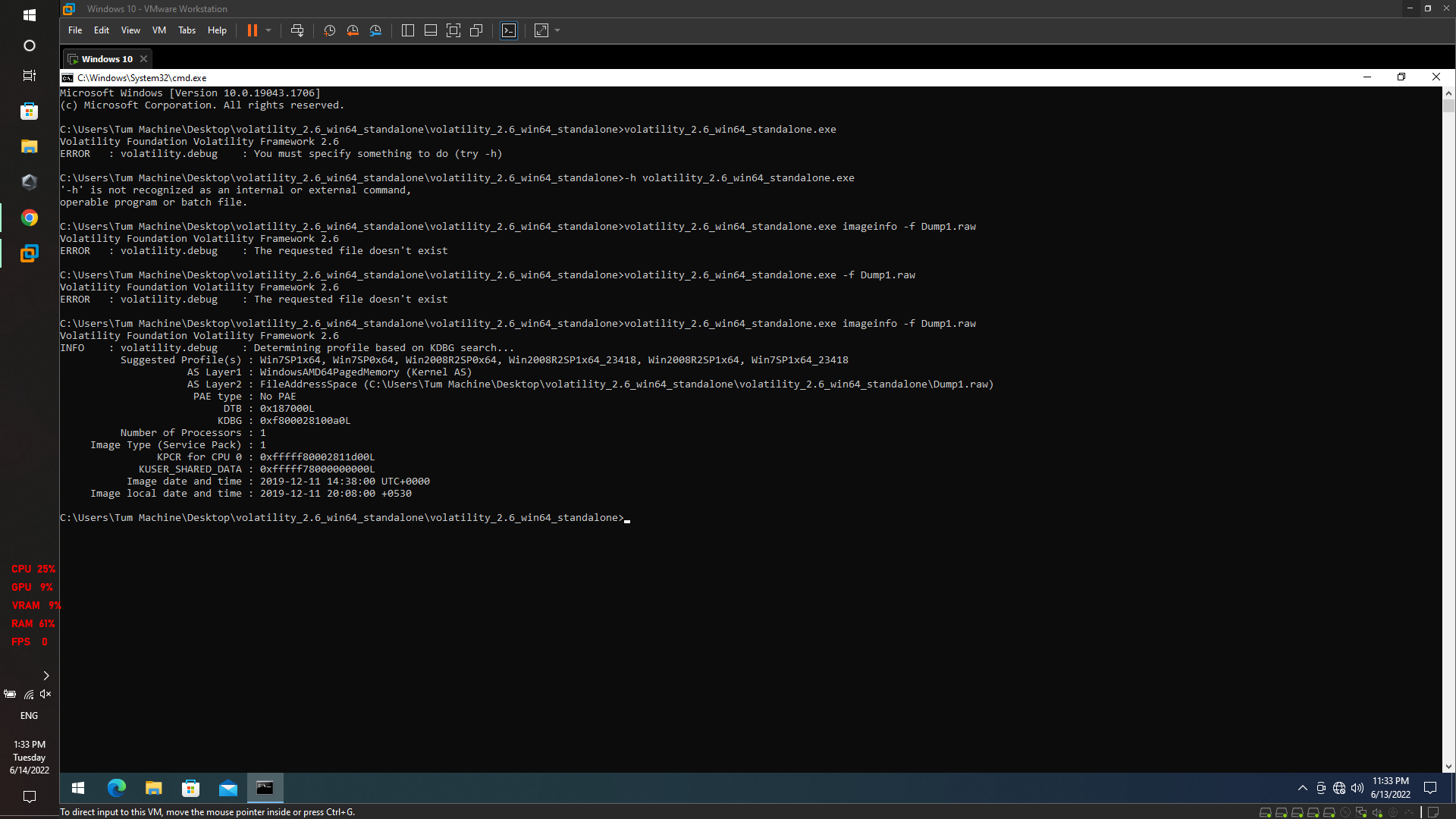
PROGRESS 1

Nguyễn Thanh Hoài Lộc – SE151250

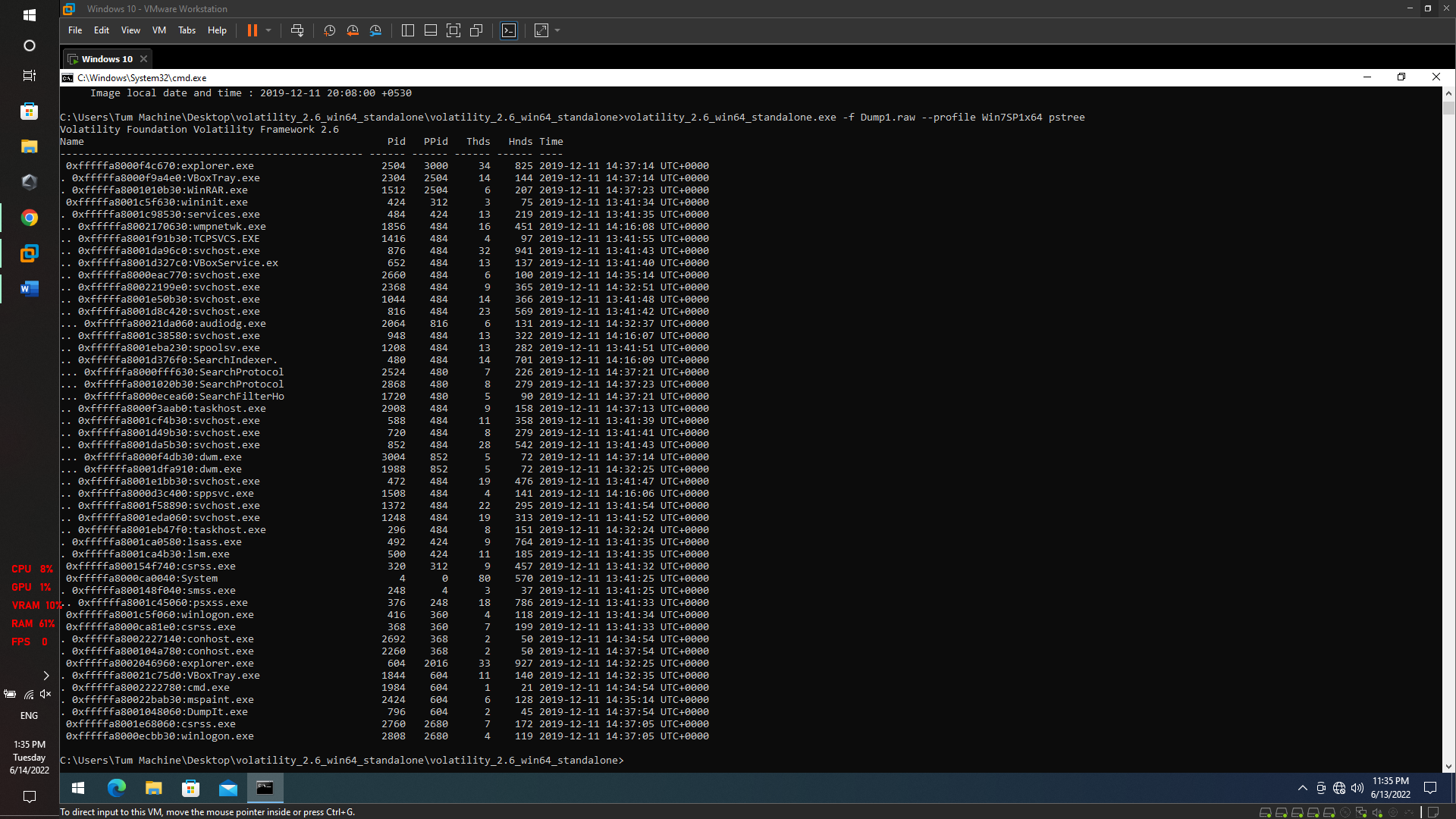
The first thing we do with a RAM dump file is identify the operating system, which we do using the imageinfo plugin.

* Volatility offers a number of choices for the profile, but generally the first one is enough.

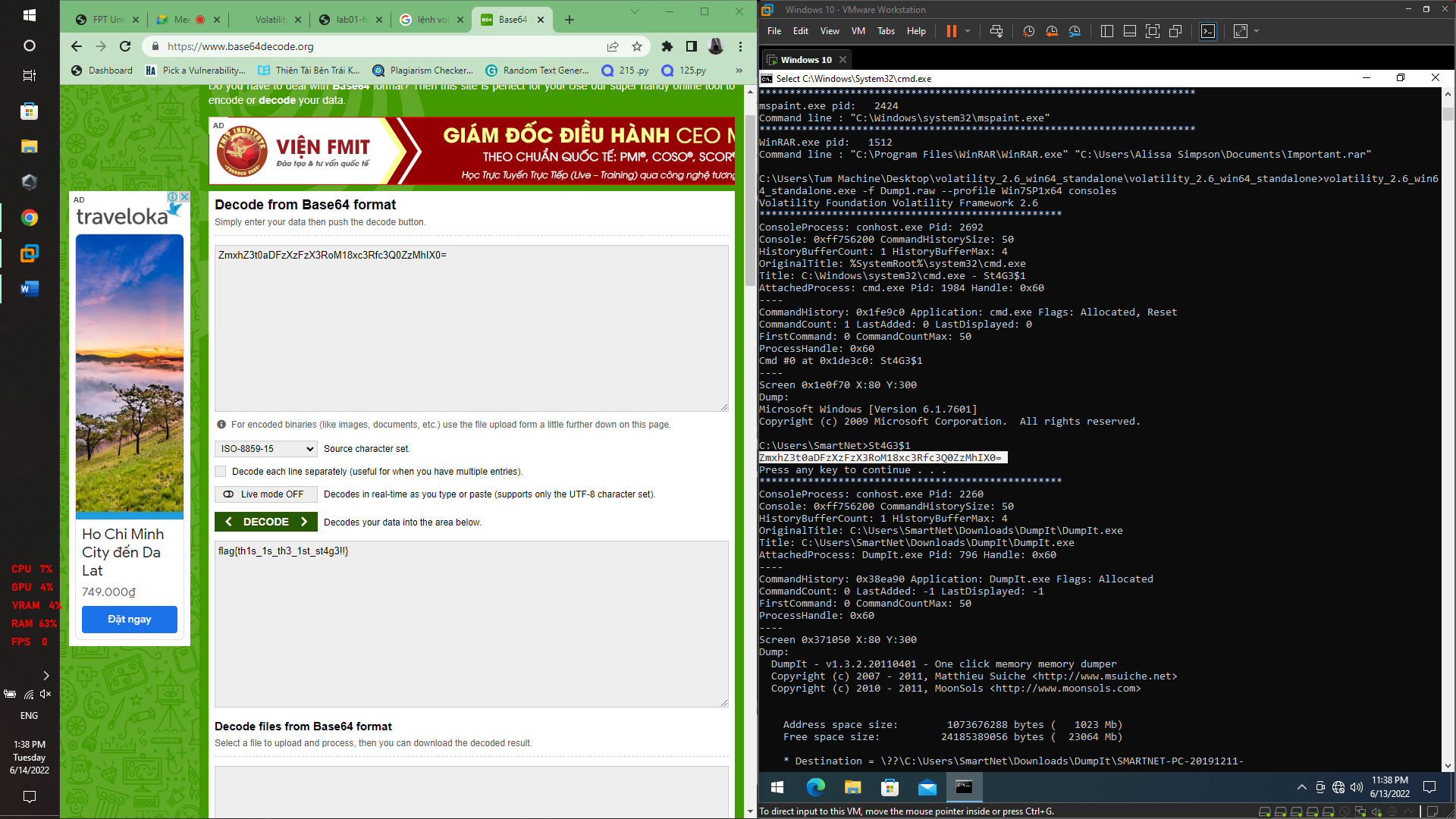


The running processes are then checked using the pstree plugin.

* There are 3 interesting processes here



We can use consoles plugin to see the output

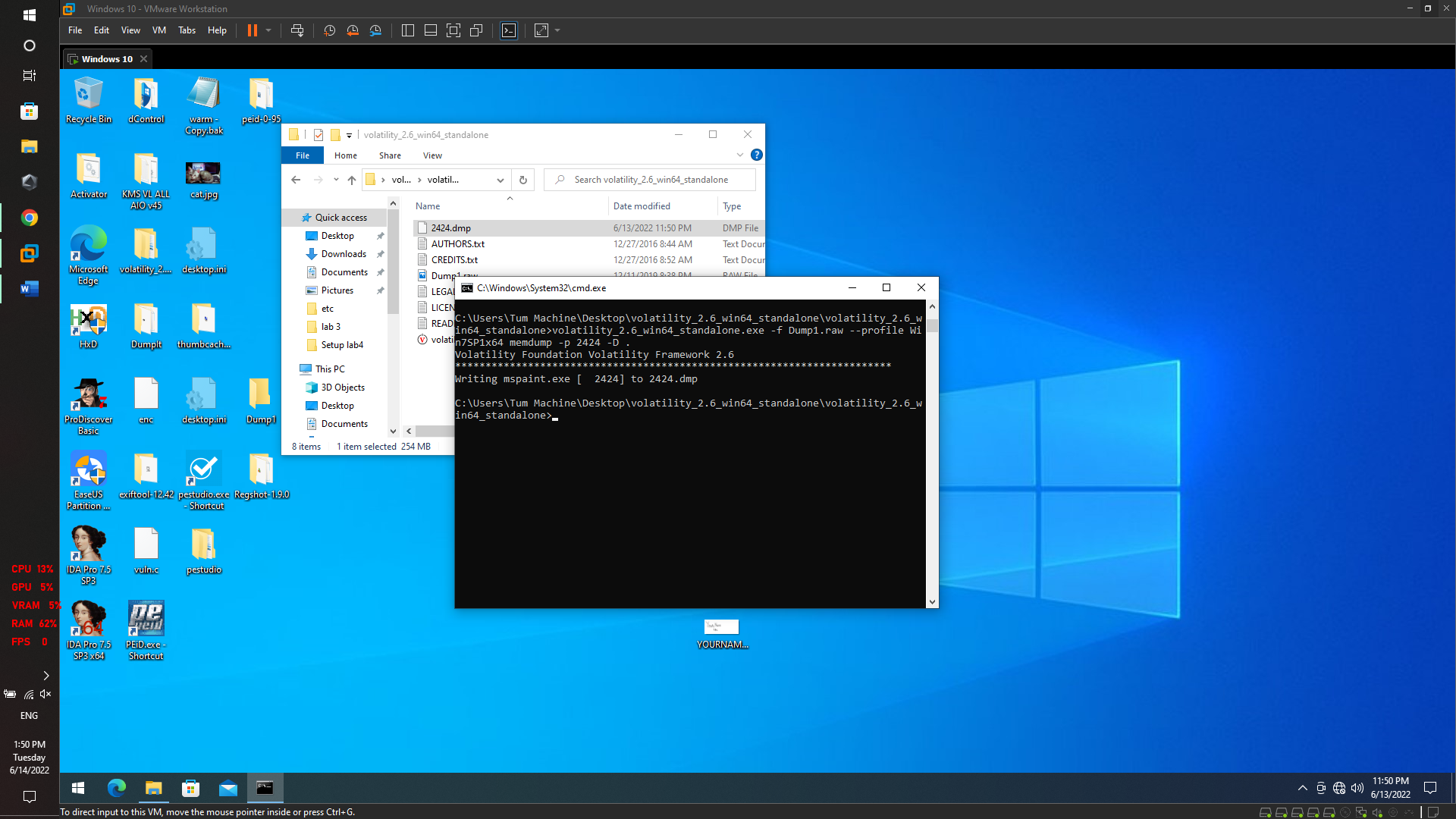


* **flag{th1s\_1s\_th3\_1st\_st4g3!!}**

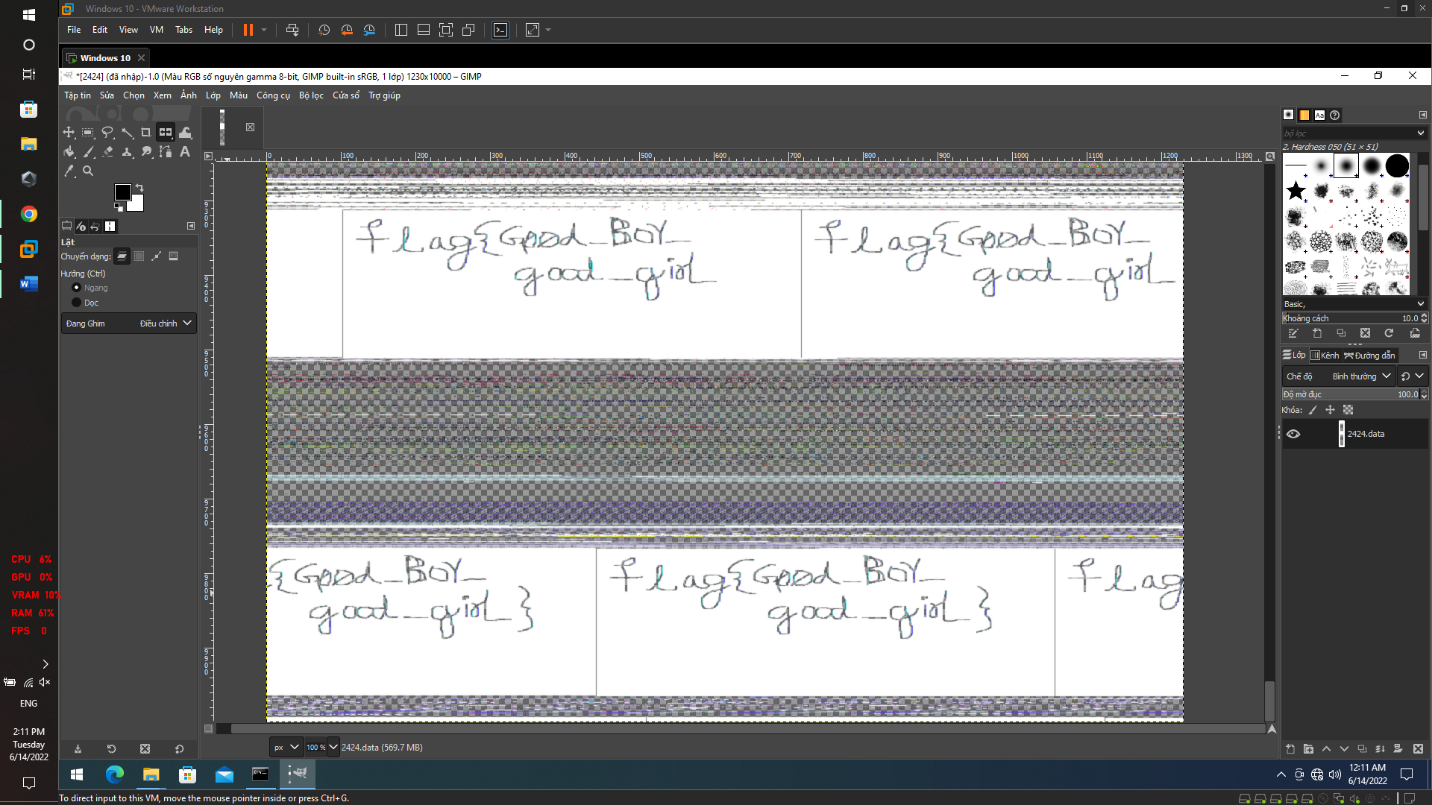
**----------------------------------------**

Next we will focus on the second interesting process, which is mspaint.exe. The PID of this process is 2424.

If you go back to the challenge description, we can see that the user was drawing something (using mspaint of course).



The output is written to 2424.dmp, we need to rename it to 2424.data to be able to open it in Gimp.

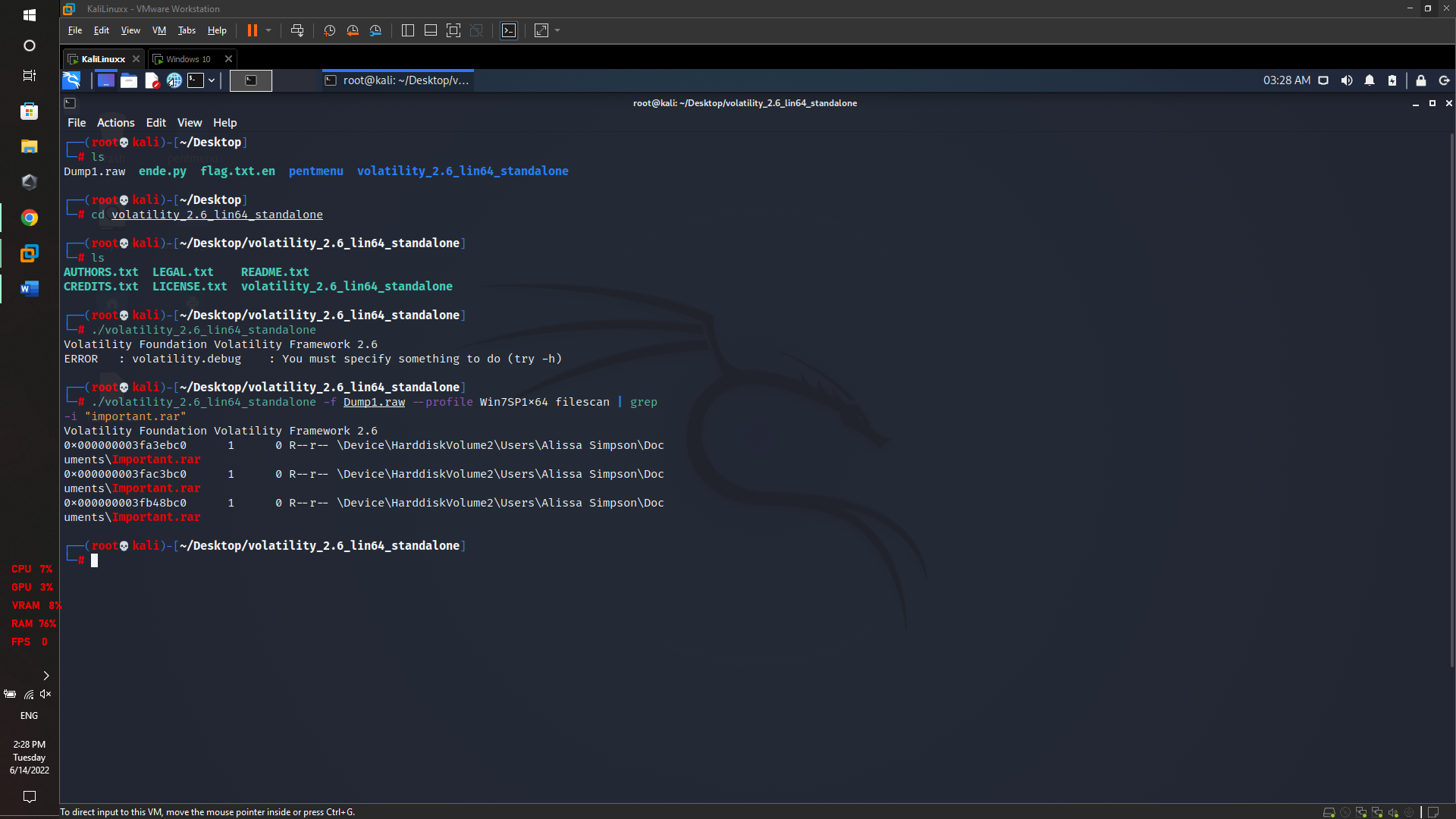
After playing a bit with the width and offset. I got an image which is somewhat flipped. I rotated it 180 degrees then flipped it horizontally

* **flag{G00d\_Boy\_good\_girL}**

**----------------------------------------**

We got the name of the rar file which is Important.rar (looks important).

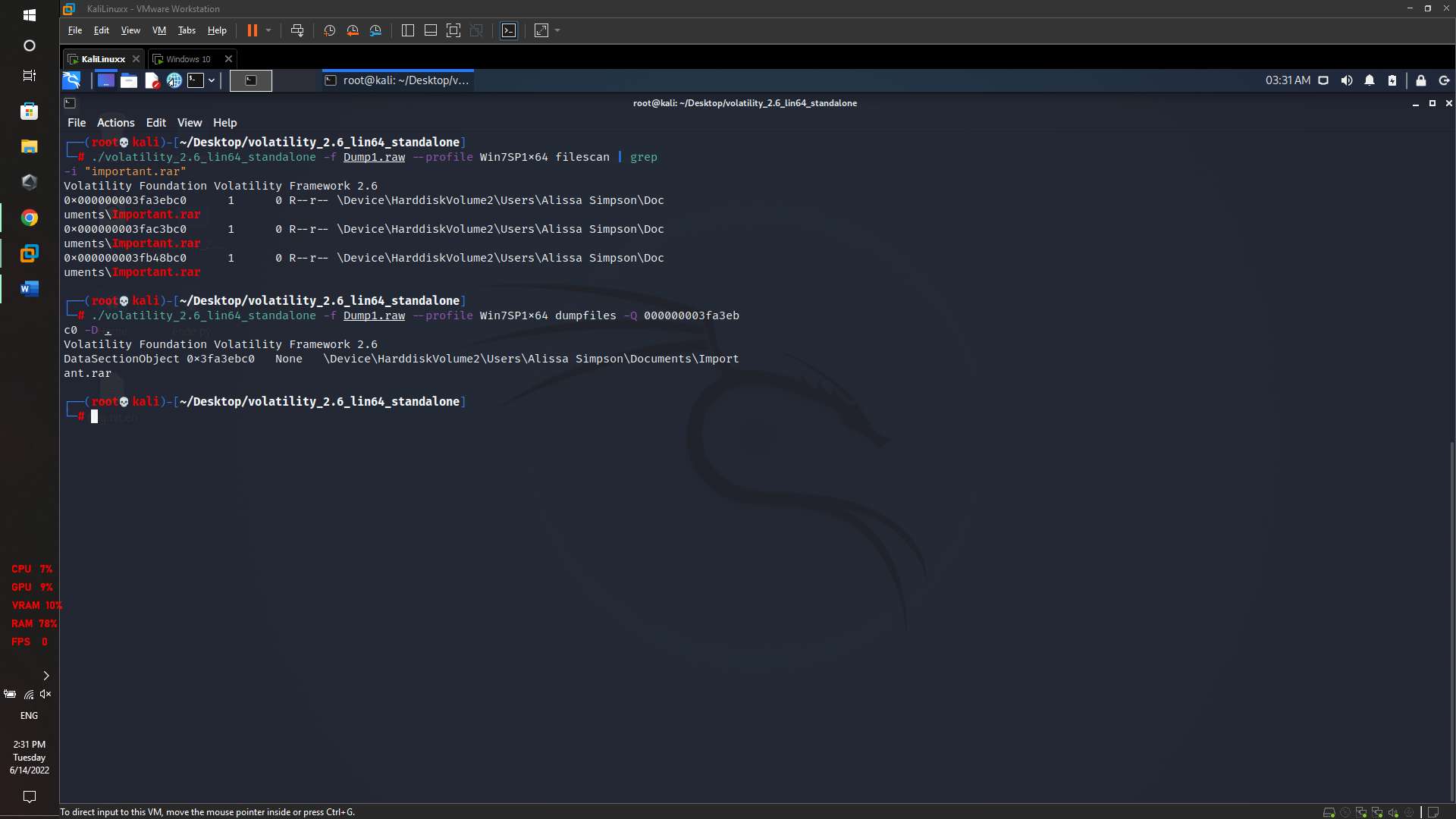
Next we can use filescan plugin to get the psychical offset of that file in memory.



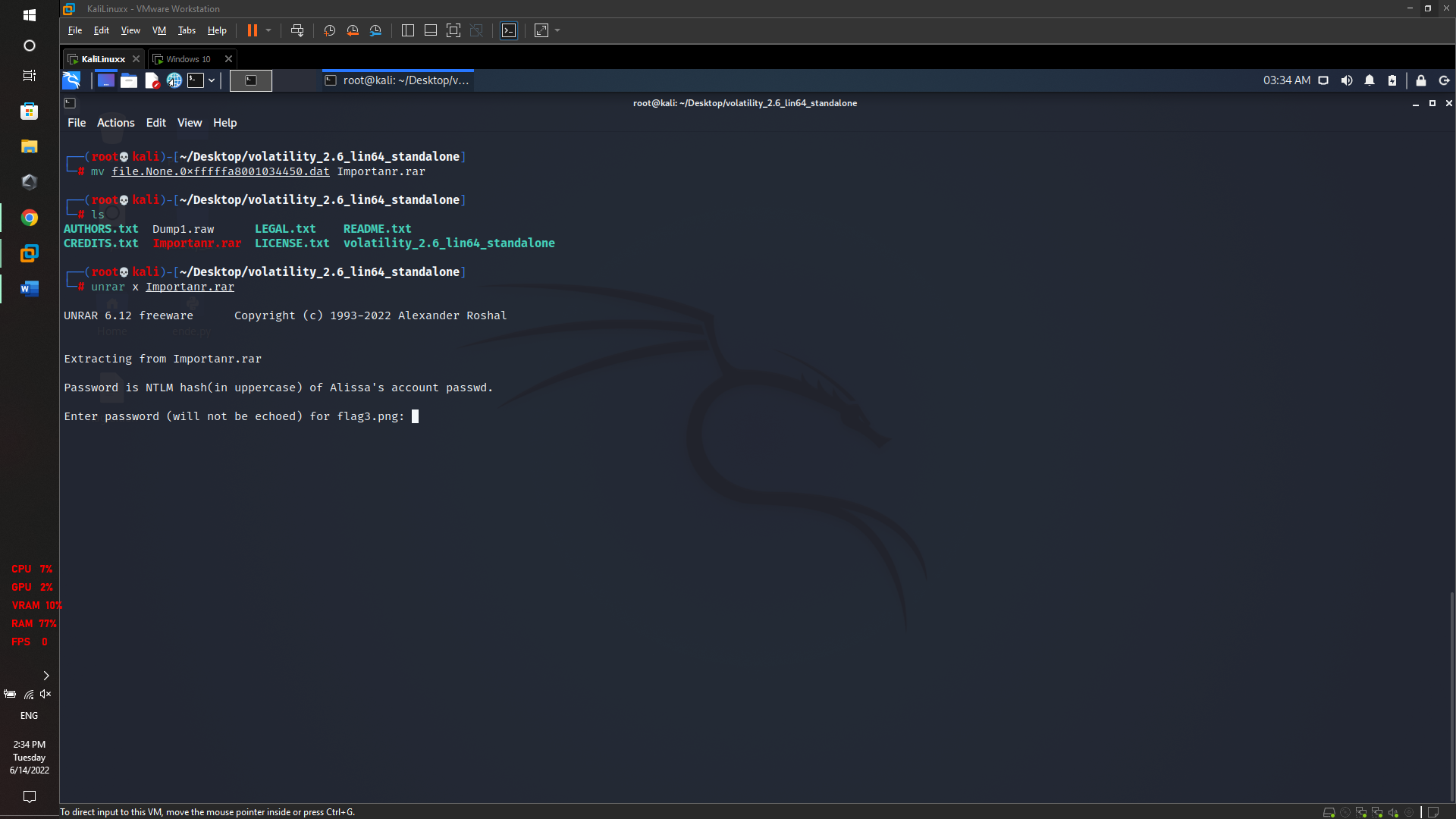
We can pick any of these offsets, To dump the file we can use dumpfiles plugin.

The file is dumped under the name file.None.0xfffffa8001034450.dat

rename and unrar it.

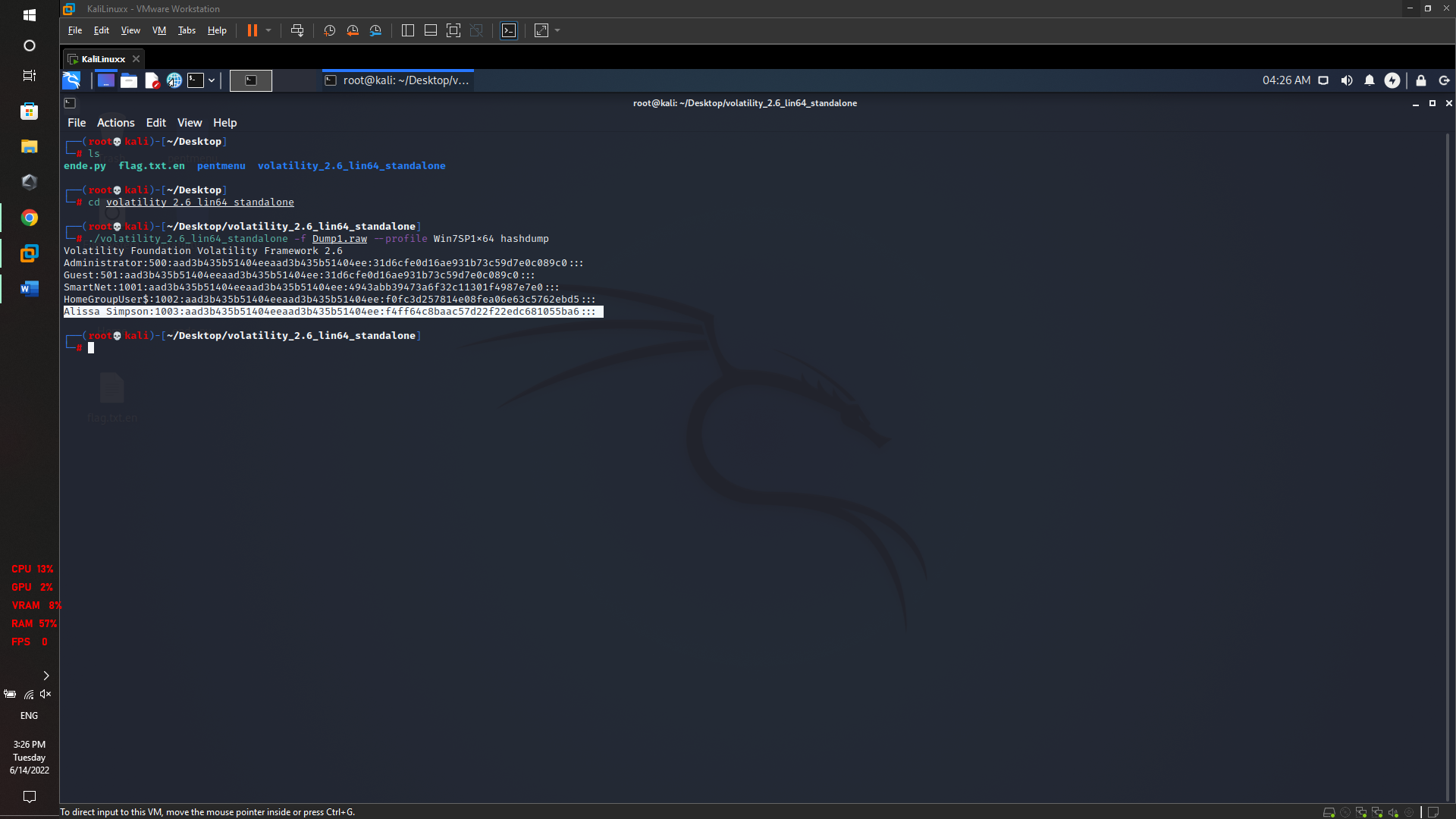


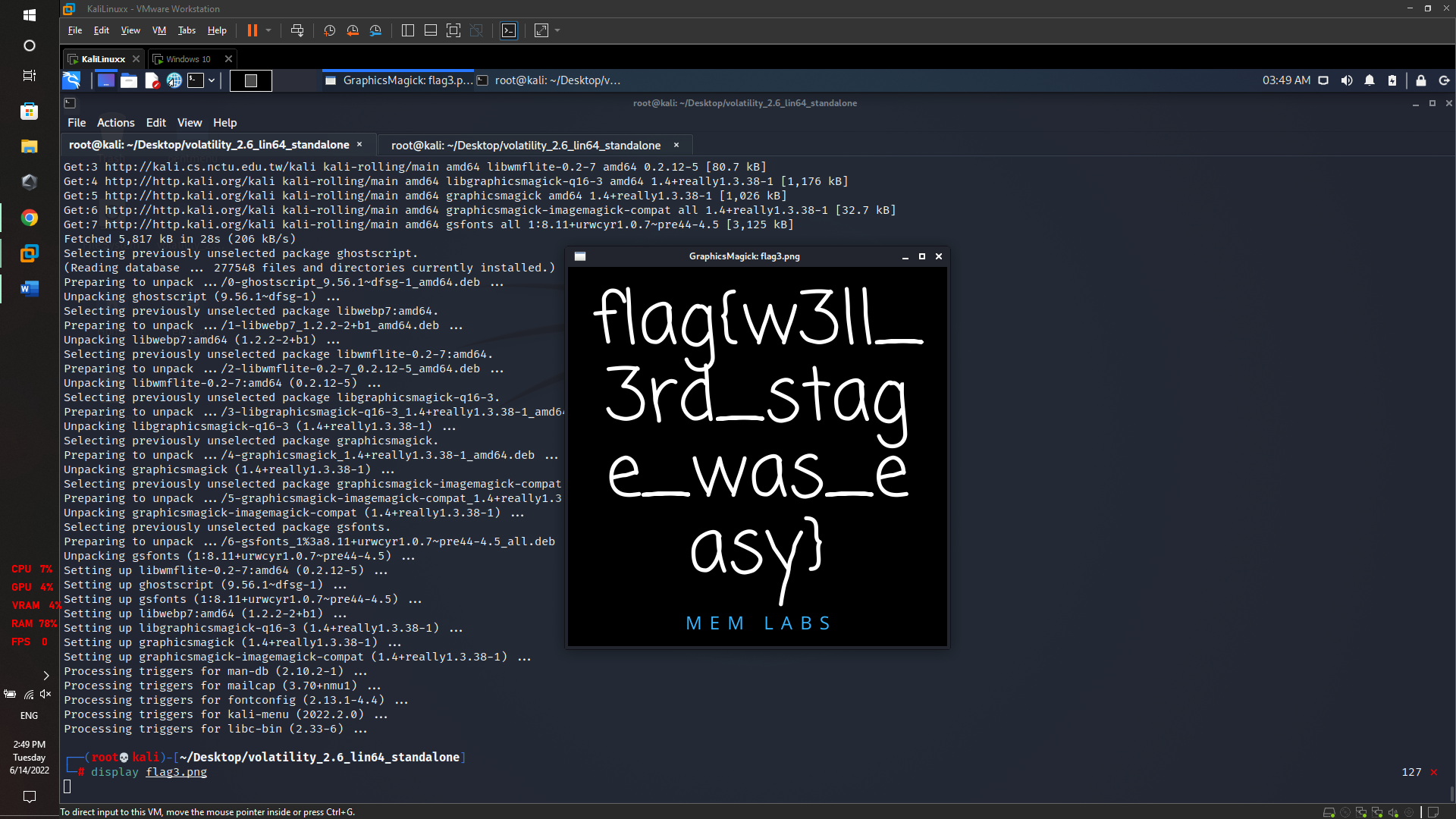
The file is password protected, but we can see a comment that says the password hash of Alissa’s account passwd.



To get the password hash, we can use hashdump plugin.

it must be in uppercase





* **flag{w3ll\_3rd\_stage\_was\_easy}**