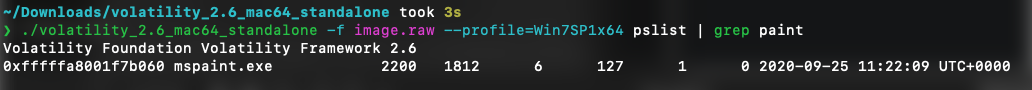
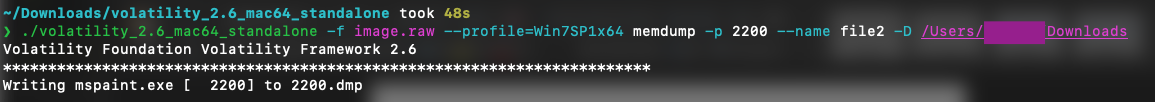
Mem 5 – Painted Masterpiece writeup:

From the description of the challenge, the author seems to be using MS paint.

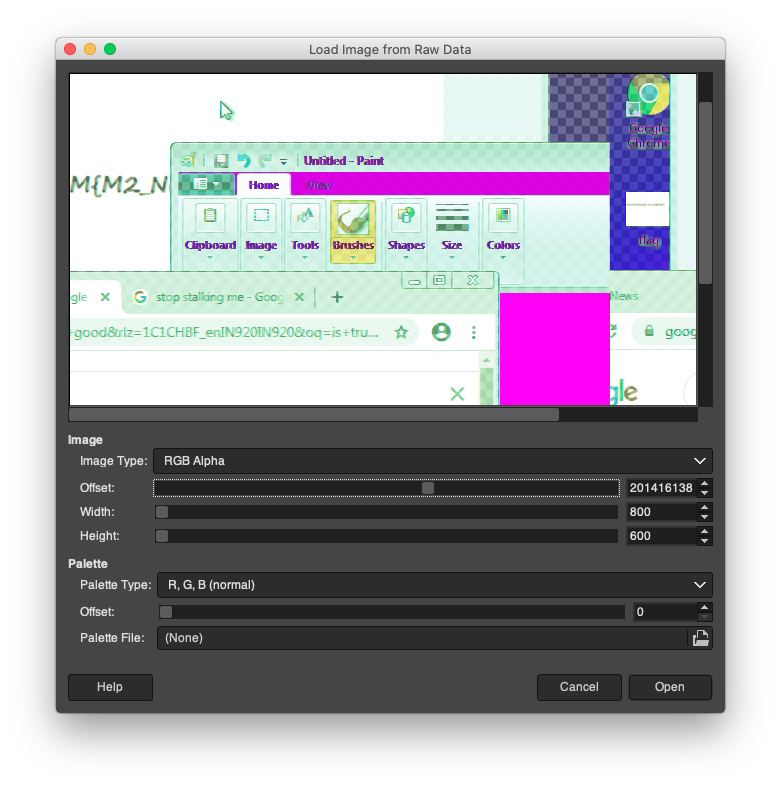
Using Volatility to grep out the process mspaint and its process ID:



Saving the memory dump of mspaint.exe to a .dmp file



Next, I rename the .dmp file to .data so that it can be opened using GIMP.



On GIMP, after setting the Image Type to RGB Alpha and setting a suitable height, I slowly change the offset using the up arrow. This took way longer than expected and after 45 minutes of playing around with the width and offset, I finally get the flag. AMCOM{M5\_M4$TER}

