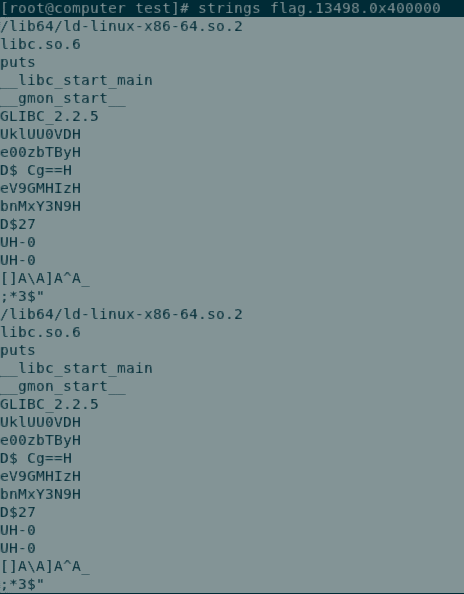
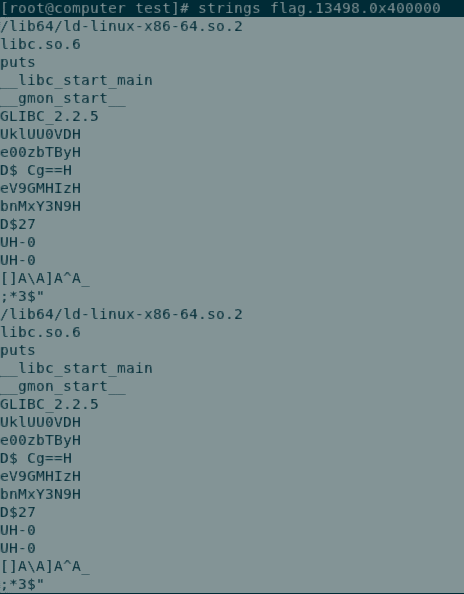
Easy Memory Forensics Write-up:

1. Get the image
   1. <https://s3.amazonaws.com/ritsec-ctf-files/memorydump>
   2. Should have a description of what operating system the image is from (CentOS 7.5) as the imageinfo command works very poorly for linux images.
2. Get volatility
   1. `git clone <https://github.com/volatilityfoundation/volatility.git>`
      1. This should probably be installed in /opt
      2. All commands from here out will assume user is in /opt/volatility
   2. `git clone <https://github.com/volatilityfoundation/profile.git>`
      1. This contains the memory profiles. They will need the `Centos7-3.10.0-862.el7.x86\_64.zip` profile from this repo.
      2. The profile goes in `./volatility/plugins/overlays/linux/`
         1. Don’t unzip the zip file
         2. Check that the profile is loaded with:
            1. `python2.7 vol.py --info | grep Profile`
            2. Ensure the following line in that output

`LinuxCentos7-3\_10\_0-862\_el7\_x86\_64x64 - A Profile for Linux Centos7-3.10.0-862.el7.x86\_64 x64`

1. List the running processes from the dump file:
   1. `python2.7 vol.py -f /home/zach/Documents/memorydump --profile=LinuxCentos7-3\_10\_0-862\_el7\_x86\_64x64 linux\_pslist`
   2. One of these processes is named `flag` and has PID 13498
2. Dump this files memory
   1. `mkdir /opt/outfile\_dir`
   2. `python2.7 vol.py -f /home/zach/Documents/memorydump --profile=LinuxCentos7-3\_10\_0-862\_el7\_x86\_64x64 linux\_procdump -p 13498 --dump-dir=/opt/outfile\_dir/ --output-file=output.dump`
3. Strings this file. Output of command is:
   1. 
4. Reconstruct the base64 encoded string from the dump as follows
   1. 
   2. `UklUU0VDe00zbTByeV9GMHIzbnMxY3N9Cg==`
5. Decode the base64 string to get the flag
   1. `RITSEC{M3m0ry\_F0r3ns1cs}`