<u>Premise</u>

Flag: RC3-2016-aEv6riGd
Truecrypt Pass: CcnciaVWadkPBdJPoon6eNsJ4
This challenge is pretty difficult and it takes someone to

1. volatility -f WIN-31DSBDSOR6O-20161116-112442.raw imageinfo
   a. This will tell you the image may be windows 2008 or windows 7
   b. It's windows 7 spoiler alert :)
2. volatility -f WIN-31DSBDSOR6O-20161116-112442.raw --profile=Win7SP1x64 pslist
   a. You will see stikynote is running on PID 2724
   b. It has something you may wish to see
3. volatility -f WIN-31DSBDSOR6O-20161116-112442.raw --profile=Win7SP1x64 memdump -p 2724 -D dump/
4. Strings 2724.dmp | grep truecrypt
   a. The note should indicate that you need to get
      i. True crypt container in evidence drive(E) and password in Lastpass.
   b. Since this is a memory image the only way to pass a file is via RAMdisk
5. Get Ramdisk image
   a. volatility -f WIN-31DSBDSOR6O-20161113-015508.raw --profile=Win7SP1x64 modscan
      i. This will show all the kernel modules loaded. RAMdisk runs in the kernel
      ii. RAMDiskVE.sys
      iii. \SystemRoot\System32\Drivers\RAMDiskVE.sys
   b. volatility -f WIN-31DSBDSOR6O-20161113-015508.raw --profile=Win7SP1x64 filescan
   c. volatility -f WIN-31DSBDSOR6O-20161113-015508.raw --profile=Win7SP1x64 dumpfiles -D . -Q 0x000000013e949f20
   d. strings file.None.0xfffffa8005584260.dat

- Hints
  - Desktop stickey note
  -
  - https://github.com/VirusTotal/yara-python
  - https://github.com/kevthehermit/volatility_plugins
  - http://jessekornblum.livejournal.com/291418.html