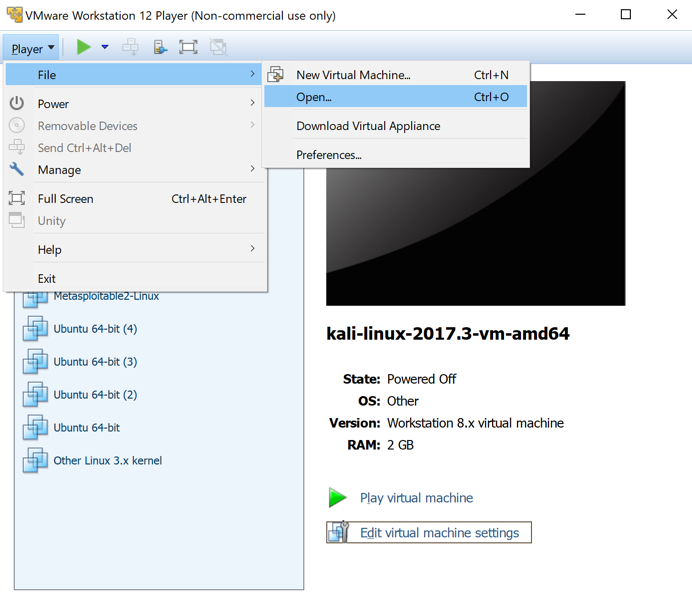
**SCY486 Lab exercise Five: RAM Analysis -Windows**

1. **Installing the Kali VM**
2. **Create a VM folder**
   1. Go to “This PC”. Find Documents folder, and look for Virtual Machines folder. In a there create a new folder called “YOUR Name VMs”.
   2. Download WinRAR from the Share. WinRAR is an unzipping tool.
   3. Download the Kali VM zipped file from the Lab1 Images folder from the Share (NOT THE iso) and unzip it into the directory you just created on the VMs folder.
3. **Starting your Kali Virtual Machine**

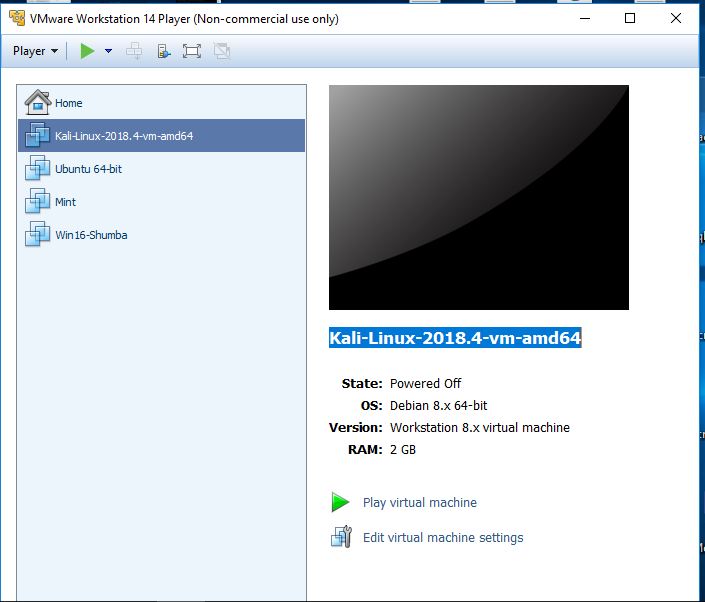
In VMware Player, at the top left, click Player, File, Open..., as shown below. Navigate to the Kali-Linux-2018-vm-amd64 folder and click on the file that displayed.



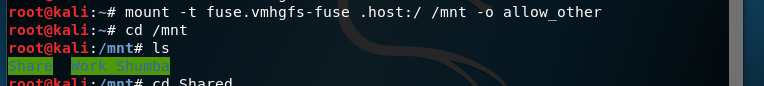
Log in to Kali with the username **root** and a password of **toor**.

**Now shutdown the Kali VM**

1. **Sharing folders between Windows and Kali**
2. Create a folder called “Images” on your host desktop to share with Kali.
3. Download a zipped file memdump.7z from the Memory\_Analysis folder, Shared drive into the created Images file.
4. With the Kali VM powered off, in VMWare Workstation, select the Kali VM and click on “Edit virtual machine settings”, as shown below:



1. Click options
2. Scroll down and highlight “Shared Folders”
3. Select “Always Enabled” on the right, if it is not selected.
4. Click “Add” and go use the Wizard until you select your “Images” folder.
5. Click “OK “ to finish the process.
6. Now start your Kali VM and open a terminal and type in the command given in the screenshot below:



1. Now, still within your VM, click “Places” at the top of the Kali screen, then select Computer, then mnt and you should be able to see the mounted folder there, from your Windows machine.
2. Now copy the zipped image from “Images” to your Desktop and extract it there.
3. **Analyzing your memory dump using volatility**

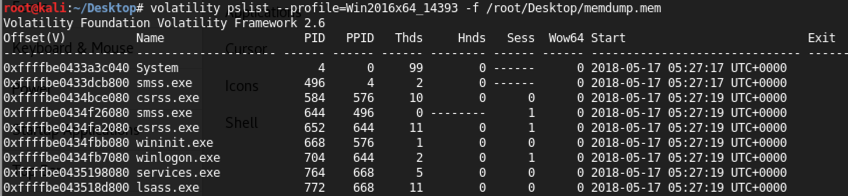
Assuming the path to your memory dump is **/root/Desktop/memdump.mem, l**et’s begin analyzing this RAM dump in volatility.

The syntax of running volatility is as follows:

1. To see the processes that were running on the machine when the RAM image was made, as shown below:

*volatility –plist profile=Win10x64\_15063 -f /root/Desktop/memdump.mem*

*{Please note that the preceeding profile are two underscores not one}*

**

1. To see the network connections on the Windows machine,

*volatility netscan --profile =<Win10Profile> -f /root/Desktop/memdump.mem*

***$volatility hivelist -f /root/memdump.raw –profile=Win7SP1x86 (Use double dashes in front of profile for some reason they are showing up as a single)***

1. We now have a list of where several key items are located in the memory dump. Next we will extract the password hashes from the memory dump. To do this it is necessary to find the starting memory locations for the SYSTEM and SAM keys. Look in the dump and copy the numbers in the first column that correspond to the SAM and SYSTEM locations. Then output the password hashes into a text file called hash.txt.

***$volatility hashdump -f /root/memdump.raw –profile=Win7SP1x86 -y 0x87c1a248 -s 0x8bfaa008 > hashs.txt (double dashes in front of profile)***

The hash values in hash.txt file can now be cracked with any password cracking tool.

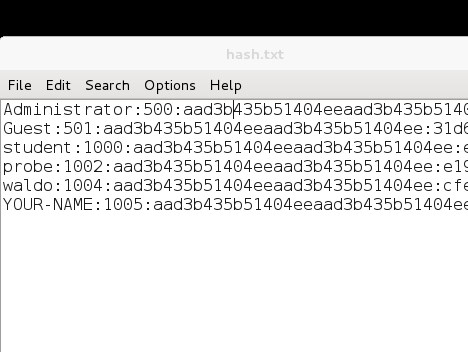
Record two accounts on the machine here **[4 points]**

**Please note the following:**

If you were using Windows XP, and have passwords shorter than 14 characters (LM passwords) –could use a password cracker- Online XP hash cracking program –LM passwords.

Windows 7 or XP with longer than 14 characters – stored in NTLM format) – take forever to crack – NTLM hashes can be used to log into a system

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



1. In addition to gathering hashes for SAM data, it is also possible to view processes that were running at the time of the memory dump. Enter the following command in order to display the running processes.

*$****volatility pslist --profile=Win2008SP1x86 -f /root/memdump.raw (double dashes in front of profile)***

Note the following columns:

Offset: The location in RAM of the process, in hexadecimal

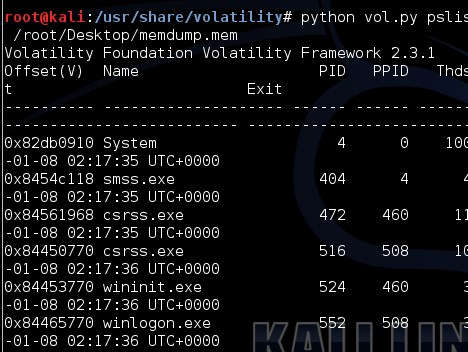
Name: The process name, as it would be shown in Task Manager

PID: The process ID

PPID: The parent process ID – that is, the process that launched this process.

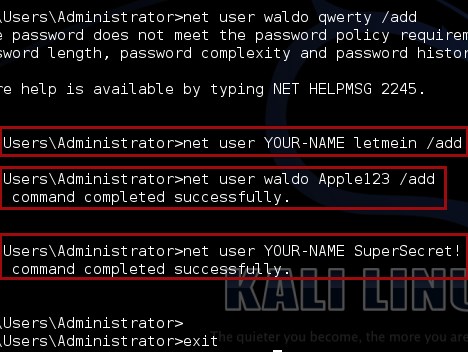
Record any **three** processes that were running at the point the dump was captured:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_[ 6 points]**



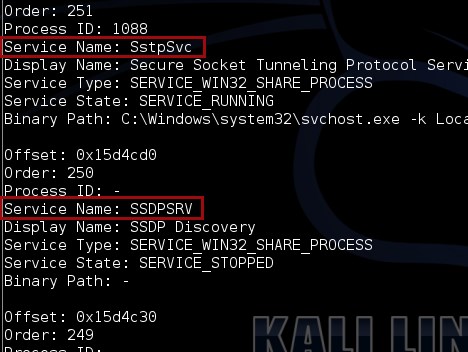
1. It is also possible to see any recent console commands that have been executed. Though this may not always be useful, in this case we can see that there were some console commands recently run that contain information about user accounts recently created, along with the passwords that were set for those users. Run the following command to display this information. Record two commands that were executed:

***$volatility consoles --profile=Win2008SP1x86 -f /root/memdump.raw***



1. Finally, it is also possible to see the services that were running at the time of the memory dump. This can be used to identify malware or other malicious programs running at the time of the memory dump. Run the following command to display the services.

***$volatility svcscan --profile=Win2008SP1x86 -f /root/memdump.raw***



1. List four challenges associated with RAM acquisition **[10 points]**
2. It is possible that you encounter a locked computer, which is on, and you would like to do a RAM acquisition. Do some research on how you as an investigator can handle this? **[5 points]**

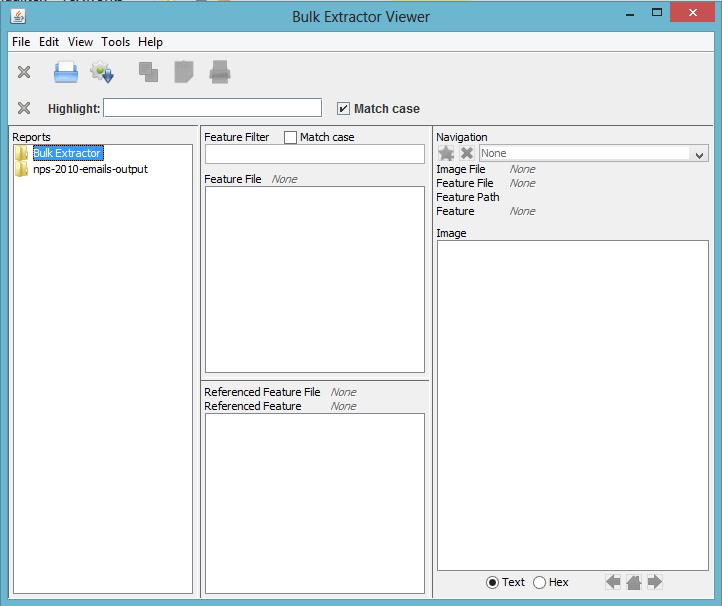
**Windows Environment**

Using a hex editor, HxD to analyze our image

* + 1. Download HxDSetup (from the Share) and install it on the host.
    2. In HxD, click File, Open. Open the "memdump.mem" file on your desktop.
    3. In HxD, press Ctrl+F. Search for Notepad or any other processes that you ran for your evidence creation.
    4. Search for any possible information in this image
    5. Record what you found

Using Bulk Extractor to analyze our image

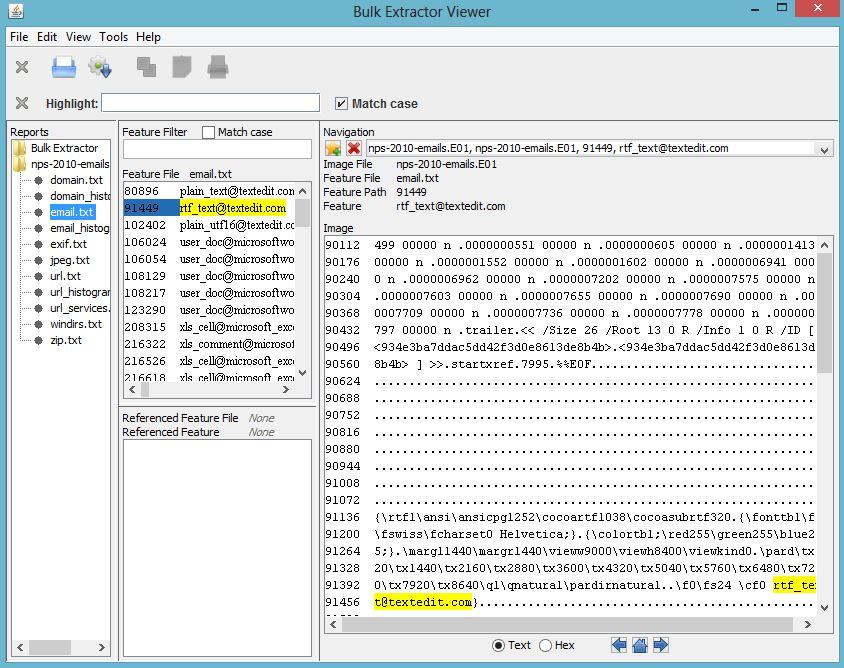
1. Download and Install Bulk Extractor



1. To run bulk\_extractor, click on the icon that looks like a gear with a down arrow. It is next to the Print icon below the Tools menu. Clicking on this icon will bring up the “Run bulk\_extractor” Window as shown below.
2. Select the image file and the output directory – use your logical drive from yesterday.

## 

1. When the run is complete, a dialog will pop-up indicating the results are ready to be viewed. Click the “Close” button which will return you to the main Bulk Extractor Viewer window to view the results of the run. The “Reports” window on the left will now show the newly created report. Clicking once on this report name will expand the report and show all of the files that have been created.
2. Clicking on one of the files will bring that file up in the “Feature File” window in the middle of the screen. In the example, the user clicked on email.txt to view the email feature file. Clicking on one of the features, in this case rtf\_text@textedit.com, shows the feature in context within the feature file on the right hand side of the window.



## The user can also view histogram files in the Bulk Extractor Viewer. Clicking on the file, email\_histogram.txt in the Reports window on the left hand side will bring up the contents of the histogram file in the middle window. It will also display the referenced feature file in the window below the histogram file. In this case, the referenced feature file is email.txt. Clicking on a feature in the histogram, in this example [rtf\_text@textedit.com](mailto:rtf_text@textedit.com), will display the feature in context as found within the feature file on the right hand side of the screen as shown

## 