Lab Assignment

Cybersecurity Professional Program

Digital Forensics &
Incident Response

Data Acquisition

DFIR-04-L3
Memory Capture

Lab Objective

Become familiar with the tools and methods used to capture memory data and examine it.

Lab Mission

Use the **FTK Imager** tool to capture the memory of a virtual machine and acquire basic information about it using **Volatility**.

Lab Duration

25–35 minutes

Requirements

- Basic knowledge of the Linux environment
- Knowledge of data acquisition

Resources

- Environment and tools
    - VirtualBox
        - Windows 10
            - **FTK Imager**
        - SIFT
- Extra lab files
    - ***pscp.exe***
    - ***SIFT-Workstation.OVA***
- Extra links
    - ***digital-forensics.sans.org/community/downloads***

Textbook References

- Chapter 4: Data Acquisition
    - Section 3: Advanced Capture Tools

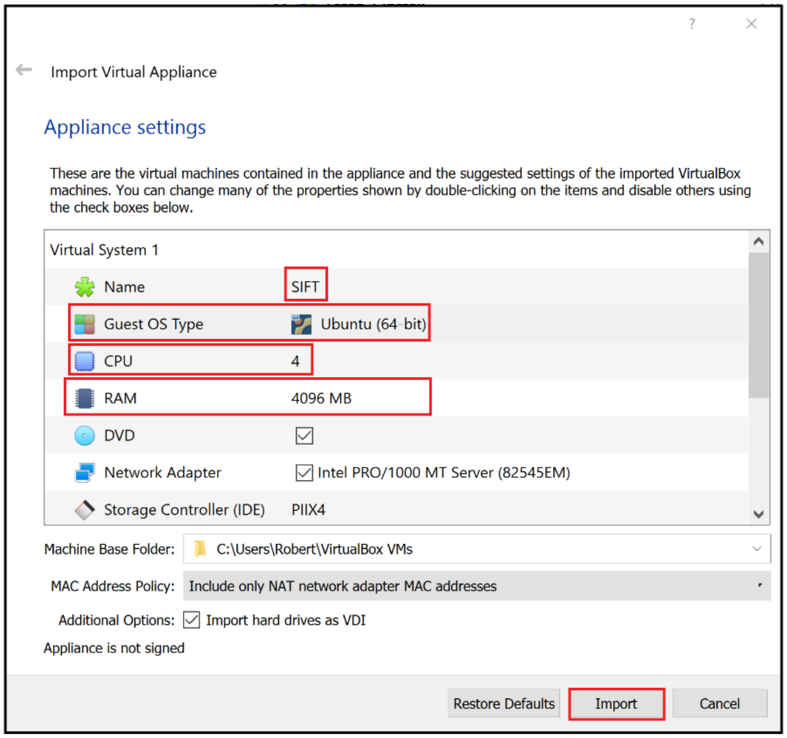
- Section 6: Memory Acquisition

Lab Task 1: Import SIFT

1 Go to digital-forensics.sans.org/community/downloads to create a SANS account and download the ***SIFT.OVA***. Be sure to write down the password and username from the website.

2 Double-click the ***OVA*** and make sure to change the name of the VM with ***Guest OS Type*** set as ***Ubuntu (64-bit)***. Once changed, import the VM.

Note: If there are fewer resources on the computer, consider lowering the RAM to 2 GB and the CPU to 2.



Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1

Name	SIFT
Guest OS Type	Ubuntu (64-bit)
CPU	4
RAM	4096 MB
DVD	☑
Network Adapter	☑ Intel PRO/1000 MT Server (82545EM)
Storage Controller (IDE)	PIIX4

Machine Base Folder: C:\Users\Robert\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☑ Import hard drives as VDI

Appliance is not signed

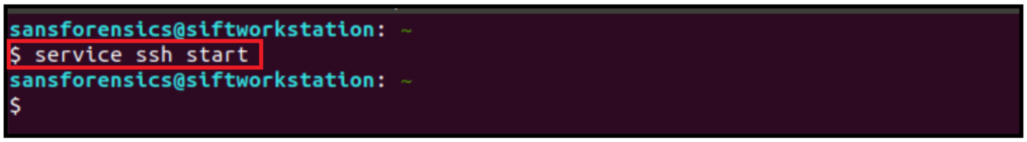
3 Ensure the VM's NIC is set to ***Internal Network***.

Lab Task 2: Data Acquisition

In this task, you will capture the Windows machine's RAM and examine it in SIFT.

1 Capture the machine's memory using **FTK Imager** by clicking the *capture memory* icon and selecting a file path for the ***memdump*** file.

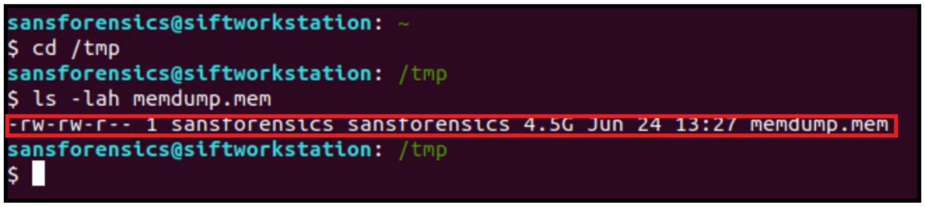
2 Set the SIFT's VM NIC to ***Internal Network*** and start the SSH service to transfer the file from the Windows 10 machine. Open the terminal in the SIFT machine and run ***service ssh start***
Note: You may need to set a manual IP address for both machines to communicate.



```
sansforensics@siftworkstation: ~
$ service ssh start
sansforensics@siftworkstation: ~
$
```

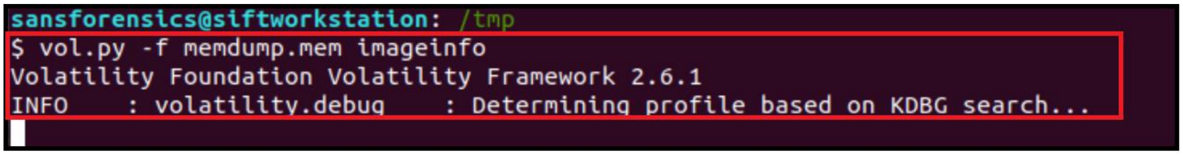
3 Transfer the capture from Windows to SIFT using the provided ***pscp.exe*** executable. Use the ***pscp.exe -P 22 memdump.mem sansforensics@[ip address]:/tmp*** command.
Note: This will transfer the file over SSH to the directory ***/tmp*** in the SIFT box.

4 Go to the ***/tmp*** directory in the SIFT box and check for the file.



```
sansforensics@siftworkstation: ~
$ cd /tmp
sansforensics@siftworkstation: /tmp
$ ls -lah memdump.mem
-rw-rw-r-- 1 sansforensics sansforensics 4.5G Jun 24 13:27 memdump.mem
sansforensics@siftworkstation: /tmp
$ 
```

5 Test the capture using ***vol.py -f <image> imageinfo*** to identify information about the file.



```
sansforensics@siftworkstation: /tmp
$ vol.py -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
```

Hints

Lab Task 2

- The VM's RAM options are in its settings.
- In **FTK Imager**, click the small *RAM* icon to start the memory capture.
- Access SIFT's network settings by clicking the *spinning network* icon and selecting ***Edit Connections***.
- The wired connection is the one to configure.
- The ***pscp.exe*** file is run via the CMD. The command to transfer a file is ***pscp.exe -P <port> <file> user@IP:/tmp***