

Autopsy Exercise

0. Download XP virtual machine -

<https://drive.google.com/open?id=0B-9qtJllxTEQjE1RHNxRTdPVE0>

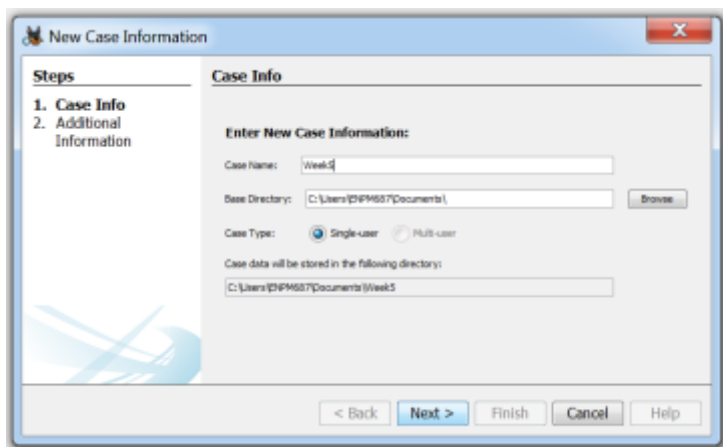
Place the VM in a location that is accessible to your copy of Autopsy, either directly if running Autopsy directly from your laptop or from the Windows VM you created to run Autopsy. For my example I am storing it in a directory called “Week5” on my Mac Desktop but it is known as “Z:\kts On My Mac\Desktop\Week5\” on my Forensics VM.

1. Open Autopsy
2. Select Create New Case



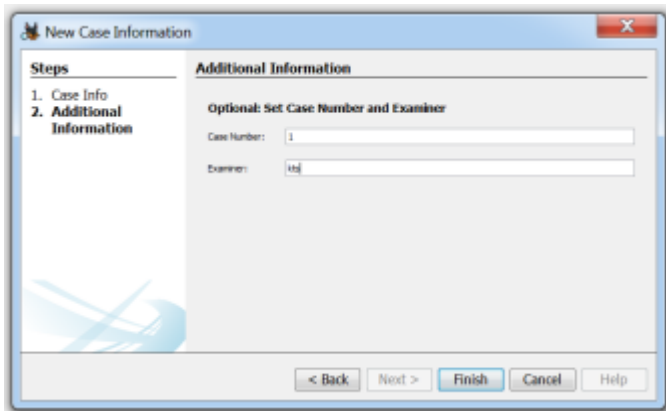
3. Enter case info

- Give the Case a name “ENPM687” “week 5”, etc.
- Base directory (standard is fine)
- Case type = Single-user



4. Click **Next**

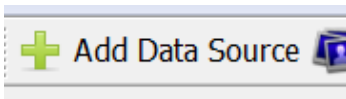
5. Enter Case information



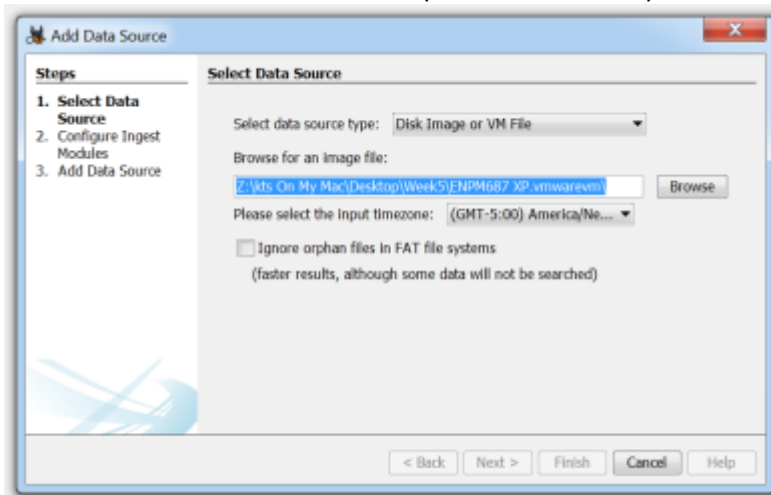
- Case Number: Whatever you want
- Examiner: Whatever you want

6. Click **Finish**

7. Click **“Add Data Source”** from the top left of the Autopsy application window



8. Enter location of the VM disk (Data Source info)



- Select data source type: **“Disk Image or VM file”**
- Browse and select the location of where you saved the VM
- **The file you want is “Virtual Disk.vmdk”**

(ex: on my system the image is Z:\kts On My Mac\Desktop\Week5\ENPM687 XP.vmwarevm\Virtual Disk.vmdk”)

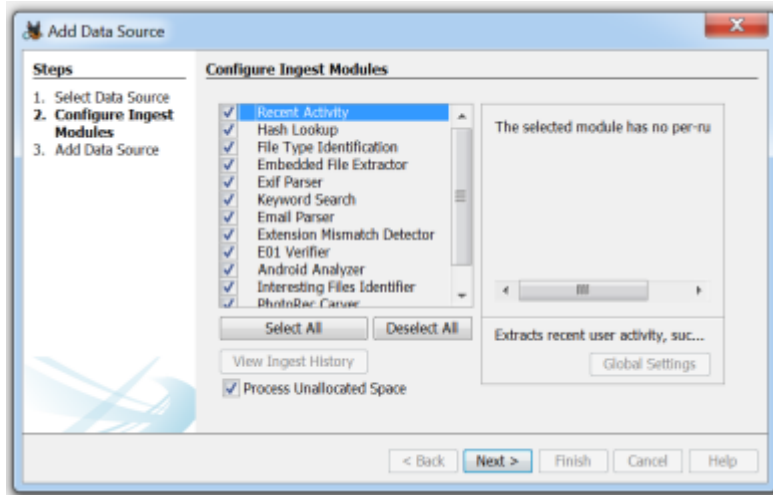
- The rest of the defaults are fine.

9. Select **Next**

10. Select all **Ingest Modules**

11. **Process Unallocated Space**

12. Select **Next**



13. Select **Finish**

You'll see Autopsy start to process the disk image and lots of data begin to be found!

