**Lab 13: The Sleuth Kit**

**What You Need for this lab**

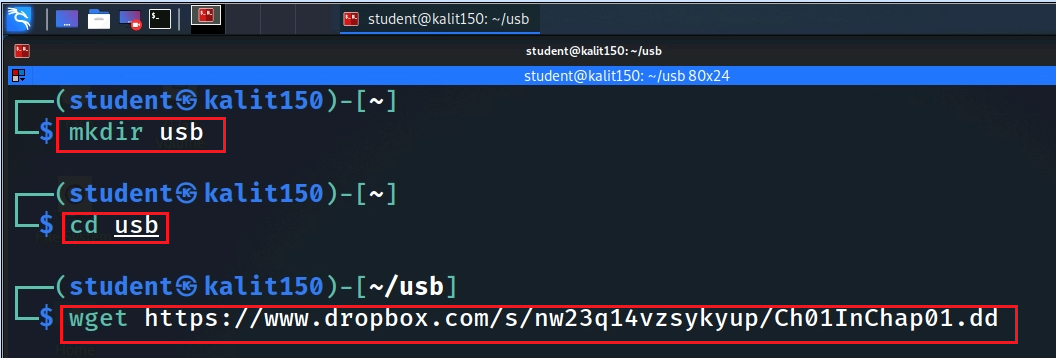
* + Install Virtualbox : <https://www.virtualbox.org/wiki/Downloads>
  + Install Kali 2021.4. : <https://old.kali.org/kali-images/kali-2021.4/>

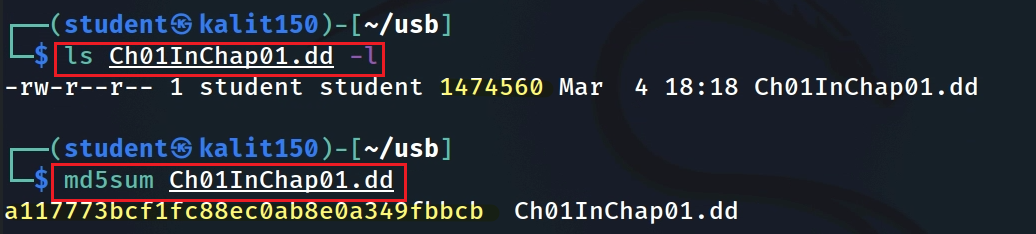
Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+

* + The Sleuth Kit
  + Assume we have the image file
  + <https://www.dropbox.com/s/nw23q14vzsykyup/Ch01InChap01.dd>

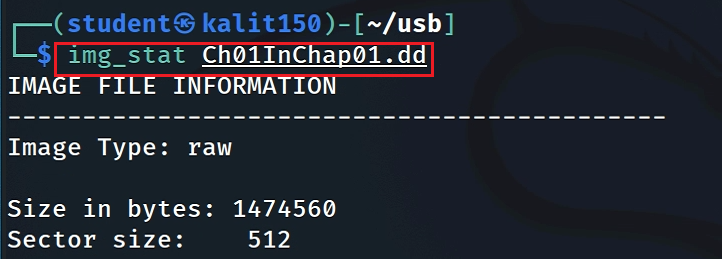
**Step 1.**

* Download a USB image

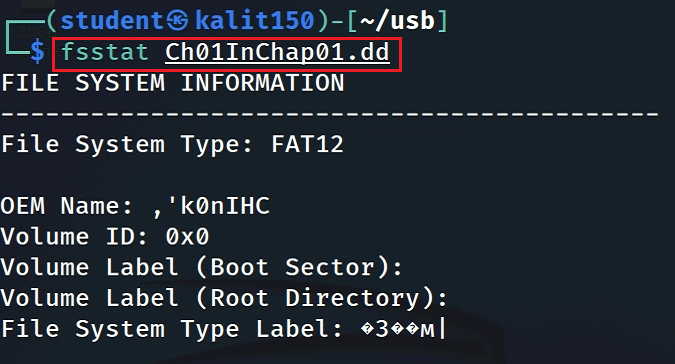




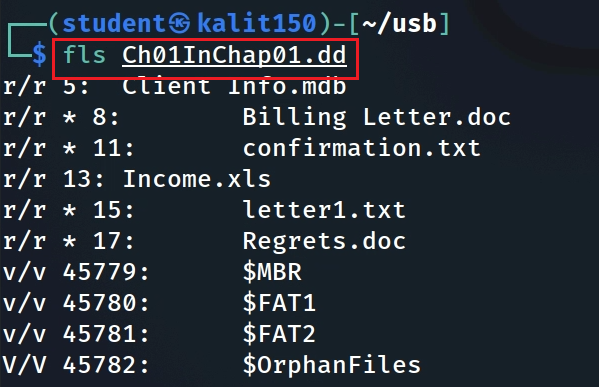
* Tool will show the details of the image format



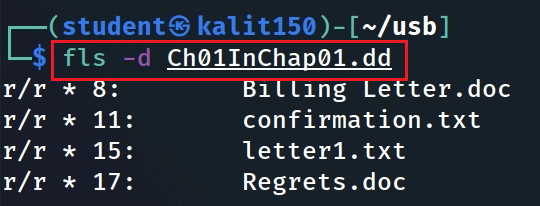
* Show file system details and statistics including layout, sizes, and labels.



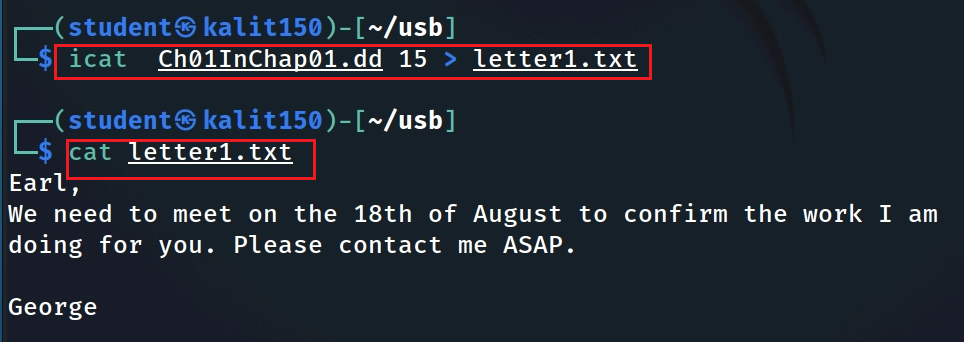
* List allocated and deleted file names in a directory



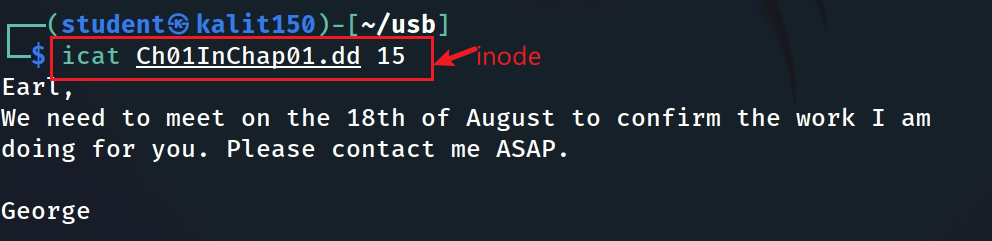
-d Display deleted entries only



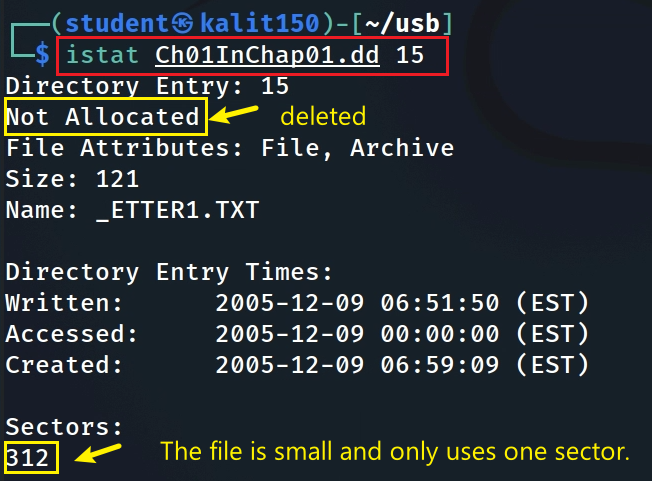
* Recover deleted file using inode



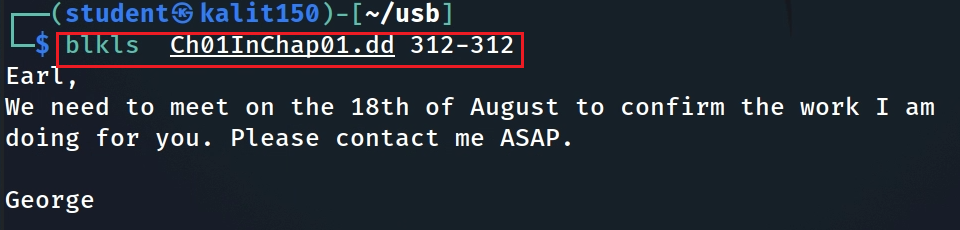
* Extract the data units of letter1.txt (inode15)



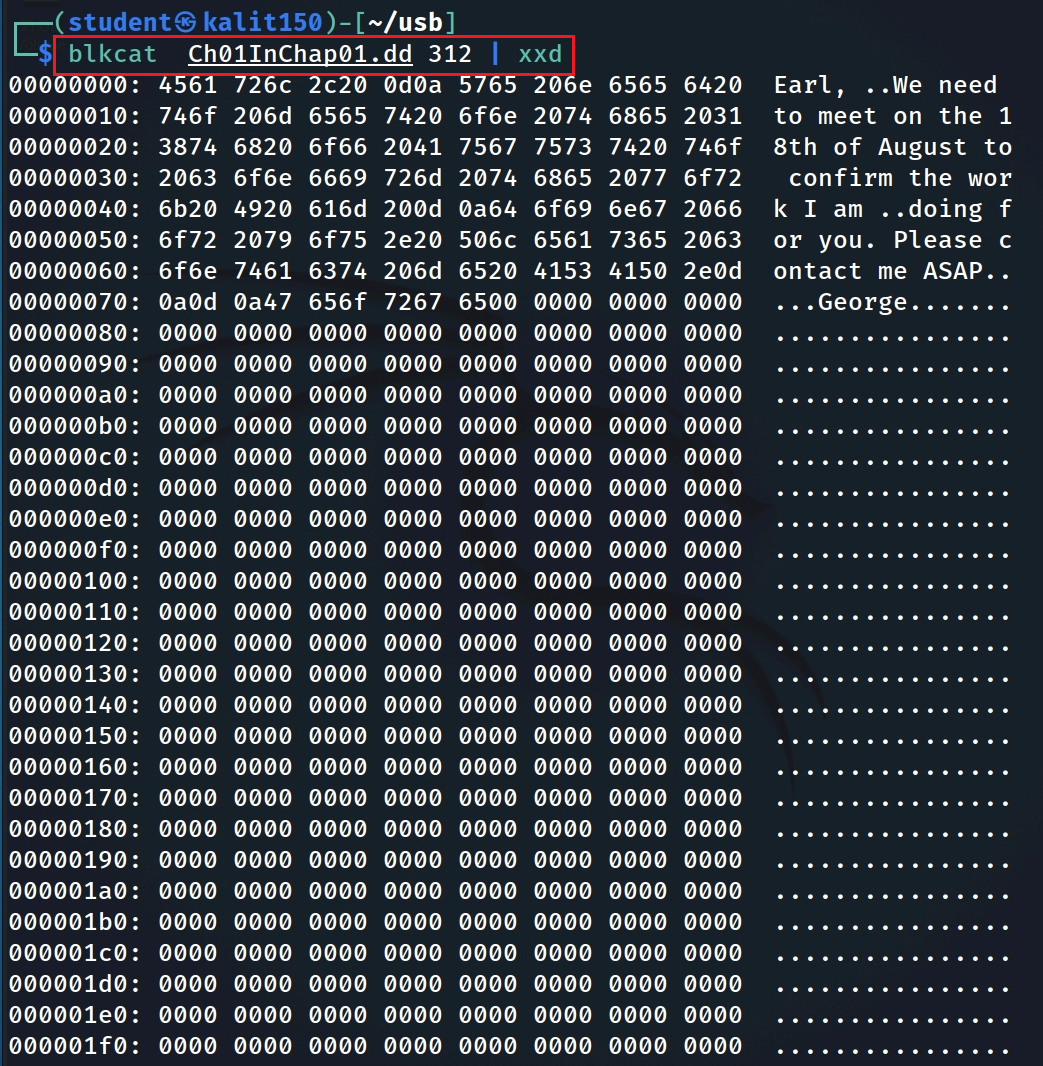
* Display the statistics and details about a given meta data structure



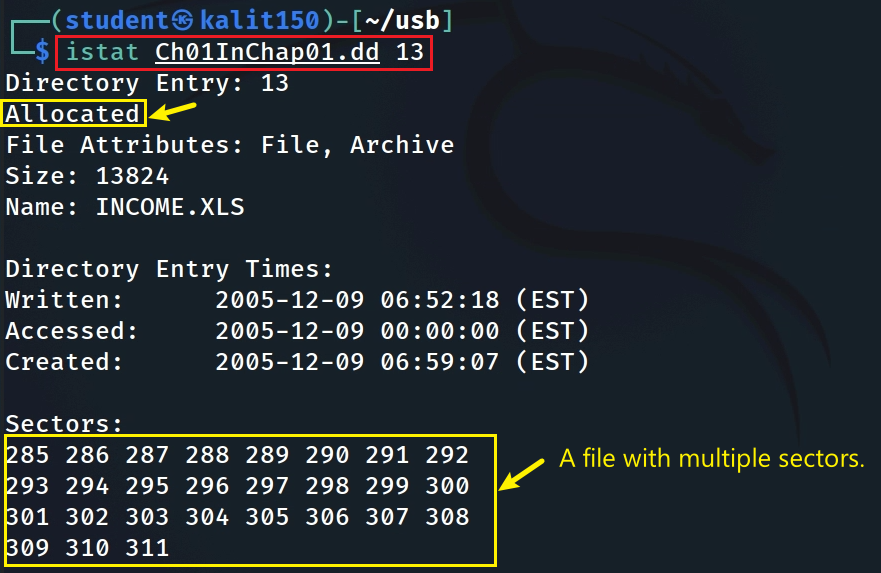
* List the details about data units and can extract the unallocated space of the file system



* Extract the contents of a given data unit in Hex

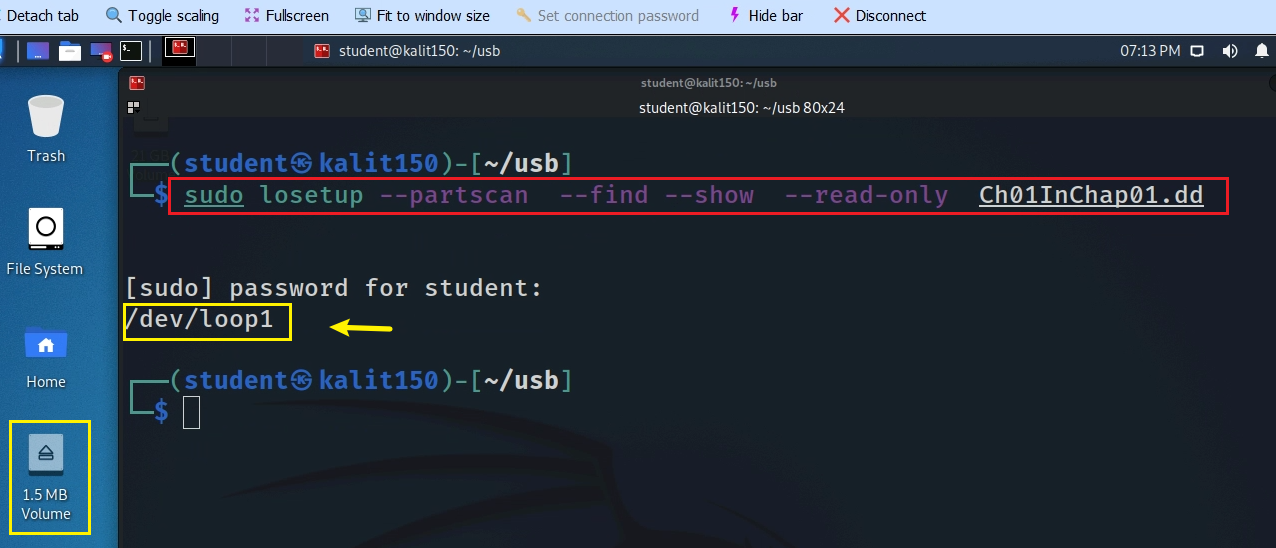


* Show A file with multiple sectors

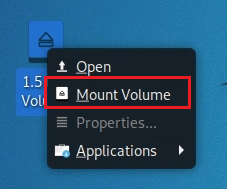


* + 1. **Assignment**

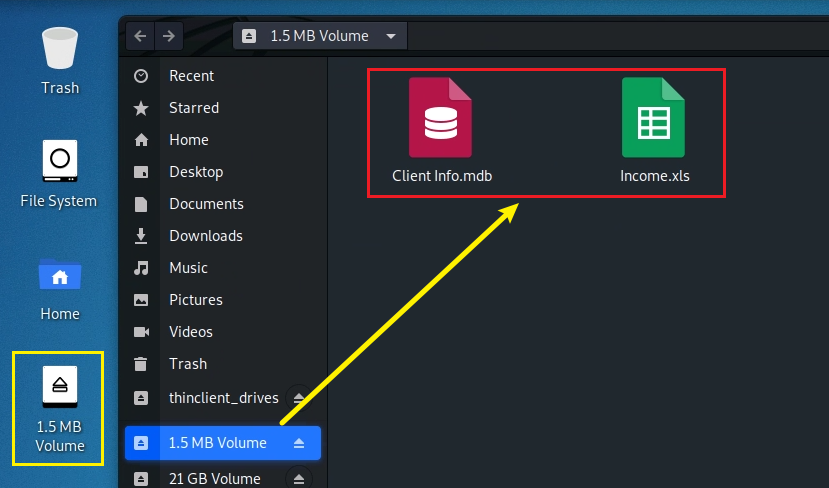
Mounting a USB image



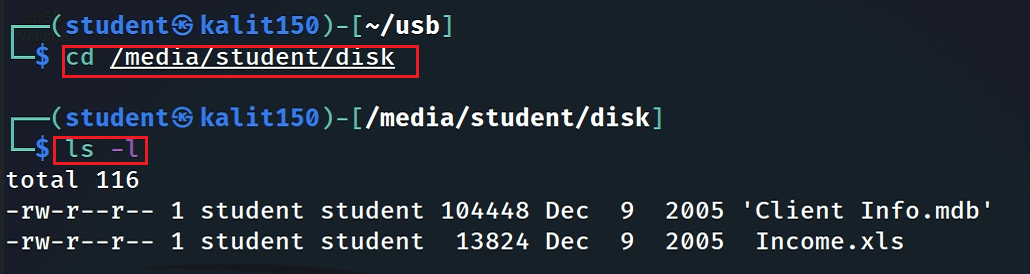
* Mount the USB image

****

* Show content

****

* Show the disk content

****

**Exercise**

1. Follow the DOCX and practice all Linux commands
2. How many deleted files in the disk image?
3. Recover all deleted files
   * Without mounting
   * Only using the commands introduced in this lecture

**YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!**

Save the document with the filename "**YOUR NAME Lab 13.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 13 From YOUR NAME**", replacing "YOUR NAME" with your real name.