**Lab 10: File search based on metadata**

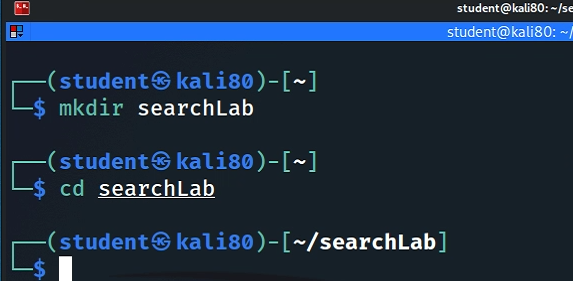
**What You Need for this lab**

* + 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+
* A USB image

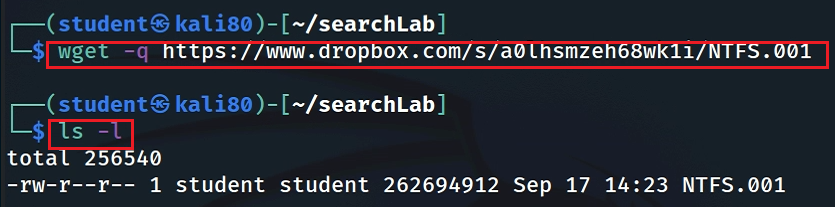
<https://www.dropbox.com/s/a0lhsmzeh68wk1i/NTFS.001>

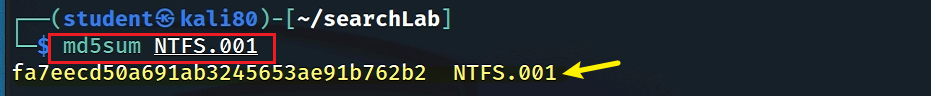
**Step 1.**

* Create a working folder

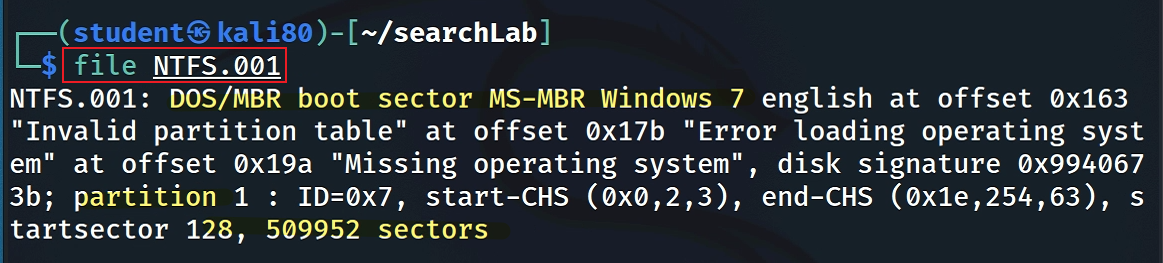


* Download a USB image



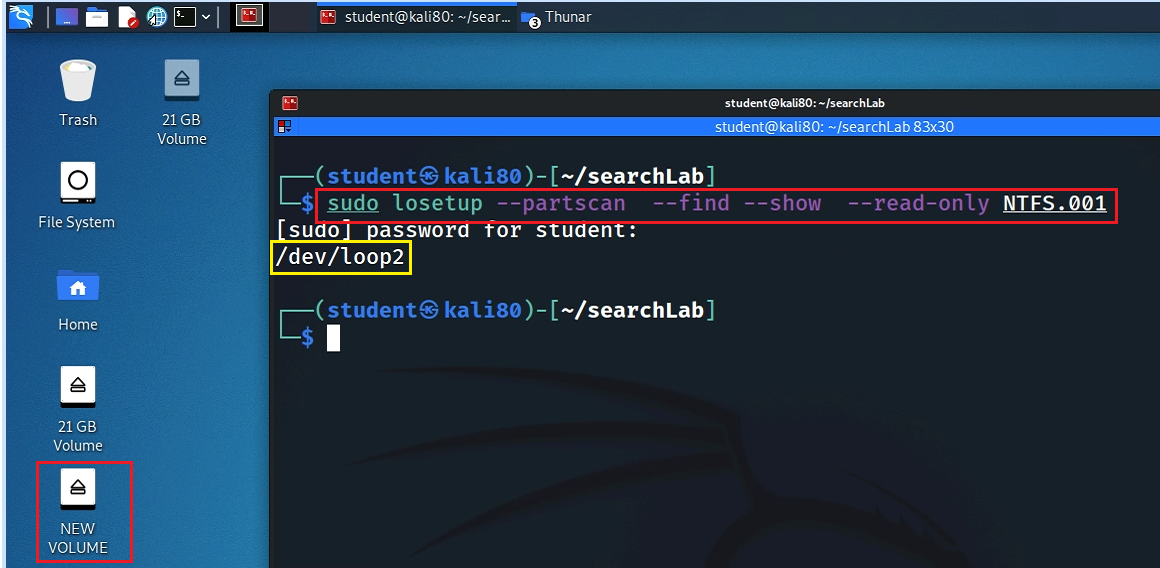


* Show image information



**Step 2.**

Mount the USB to Linux as a read-only loop device

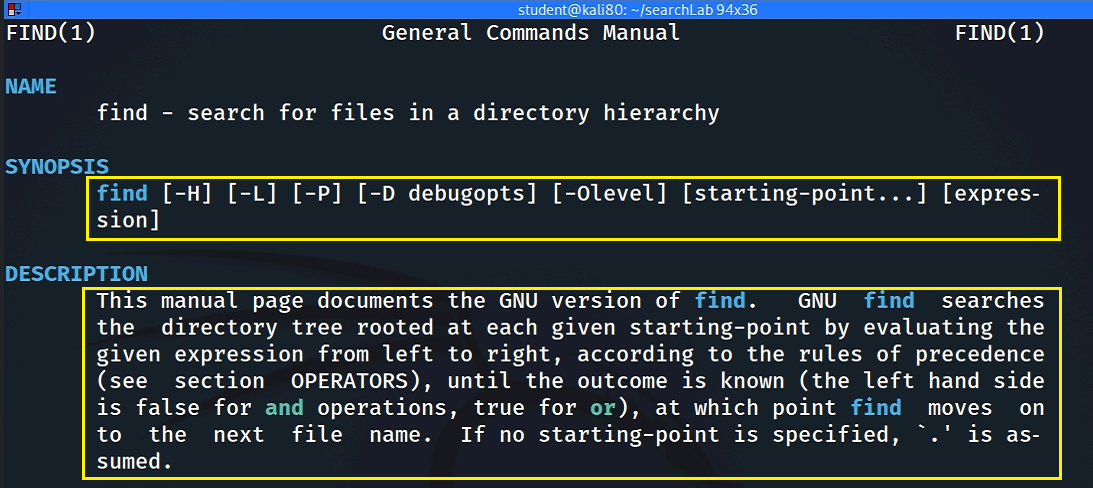


* View file structure

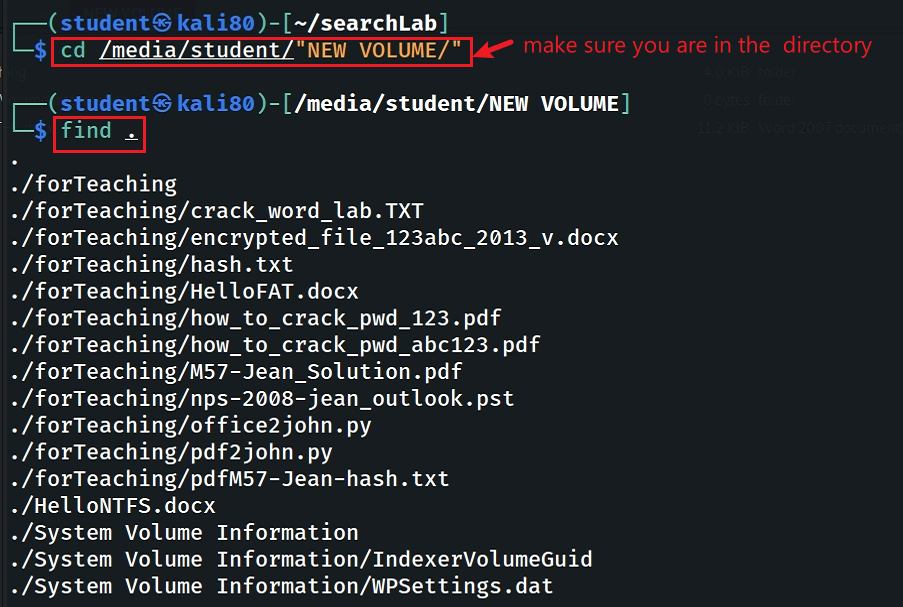


* Syntax

*$ find [where to start searching from] [expression determines what to find]*

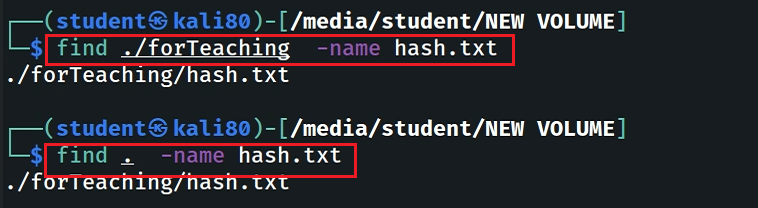


* Find Files/directories starts from Current Directory (recursively)

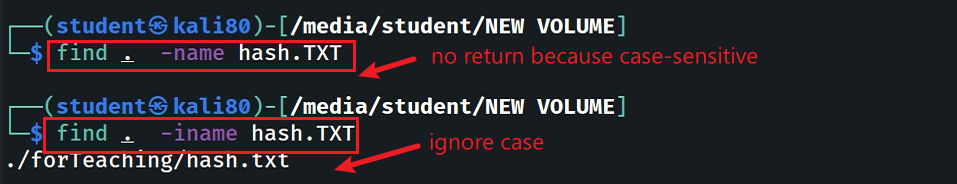


*-name* and *-iname*: find file/directory names

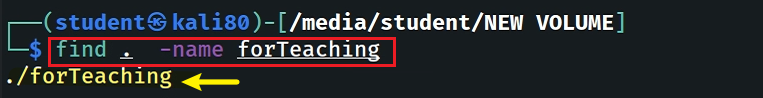
* find a file



* find a file and ignore case

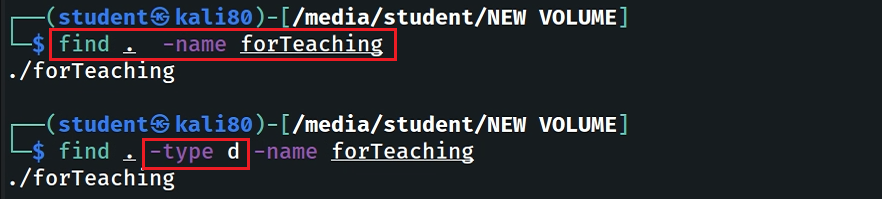


* find a directory

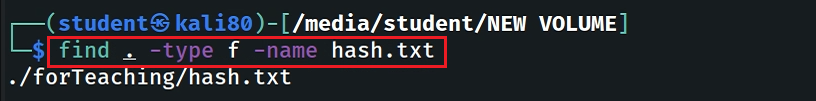


*type*: specify string types

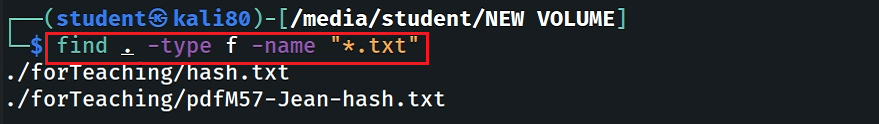
* Specify the search type *d: directory*



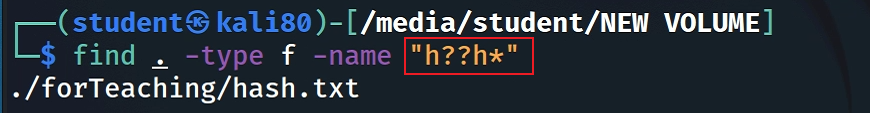
* Specify the search type *f: file*



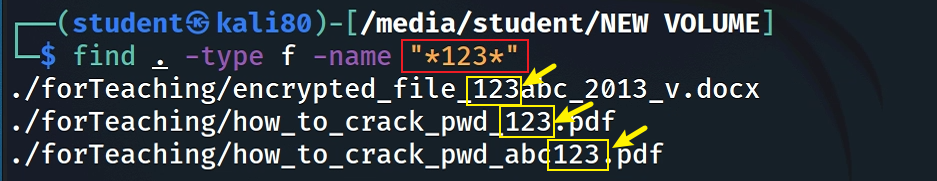
* Search all files with extension *.txt*



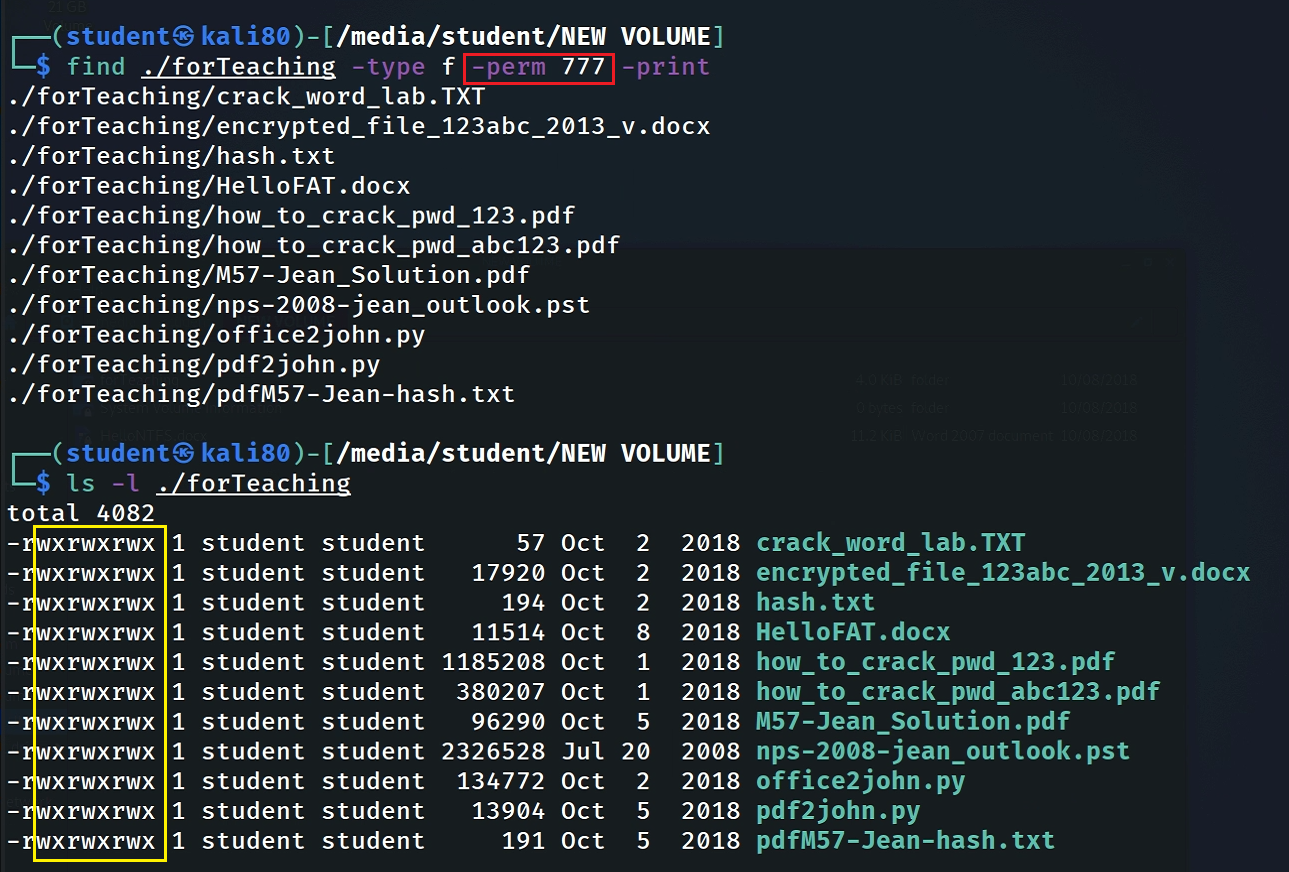
* Match all files which first and four letters are “*h*”



* Match all files contains “*123*” (in the middle of the file name)

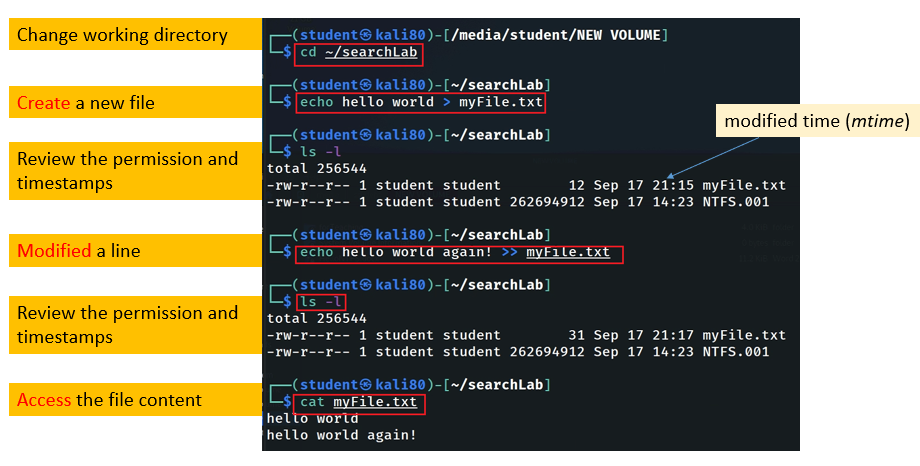


* Find Files With 777 Permissions

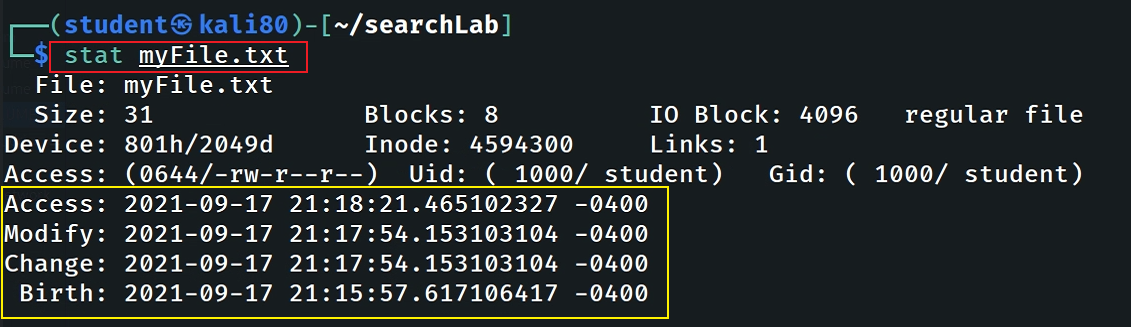


**Step 3.**

* **“atime”, “mtime” and “ctime”**



Can you recreate the file changing history? Answer and explaine

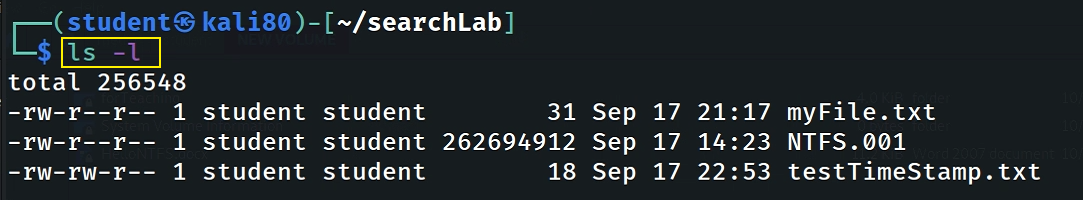


**Answer**

* Timestamp changes when changing permission

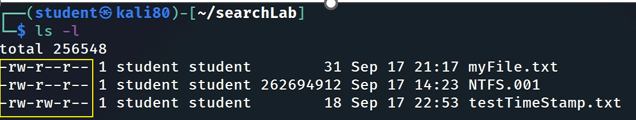


Find Files With “*–perm=664”* Permissions ?

****

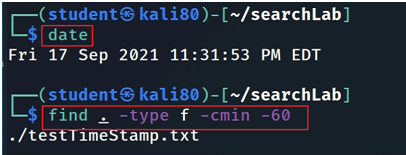
**Answer**

Find Files With */u=r /u=w /u=x* Permissions



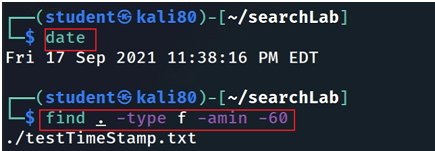
**Answer**

Find Changed Files in Last 1 Hour ?



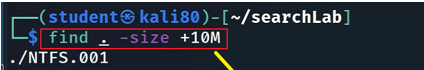
**Answer**

Find Accessed Files in Last 1 Hour ?



**Answer**

Find files that size that is great than 10MB ?



**Answer**

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

Save the document with the filename "**YOUR NAME Lab 10.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 10 From YOUR NAME**", replacing "YOUR NAME" with your real name.