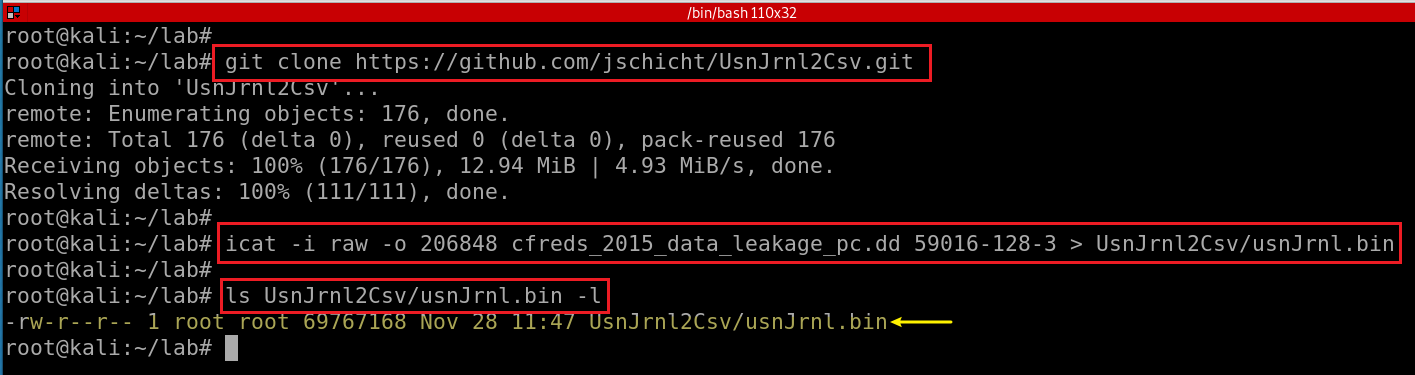
**Lab 6: Update Sequence Number (USN) Journaling**

**What You Need for this lab**

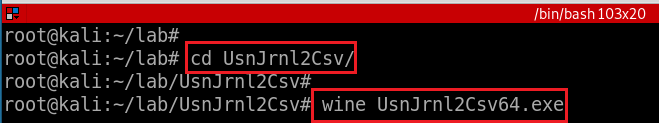
* + Install Virtualbox : <https://www.virtualbox.org/wiki/Downloads>
  + Install Kali 2021.4. : <https://old.kali.org/kali-images/kali-2021.4/>
    - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+
* <https://www.dropbox.com/sh/3lyzpi7vyod0pfs/AADh2b3TnmMqWZHB1Uzv9_ma?dl=0>
* <https://ubaltmy.sharepoint.com/:f:/g/personal/id31ga53_ubalt_edu/EoJThlUPE85Hm7592HB5sjIBGo4Ht9drLxt9XnwDdnf3PA?e=4Okj4m>
* <https://github.com/jschicht/ExtractUsnJrnl>
  + Image .dd from Lab 5

**Scenario 1**

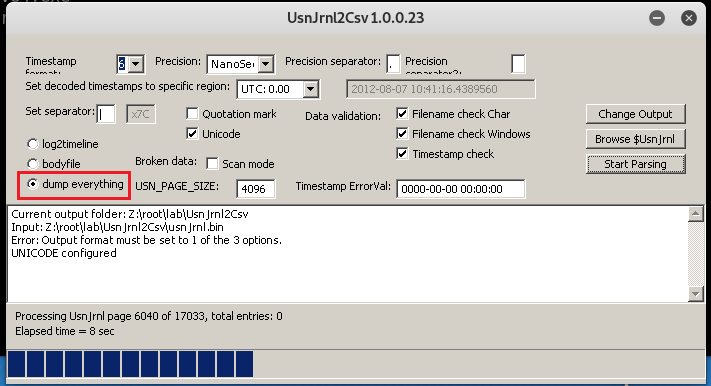
* Install *UsnJrnl2Csv* tool



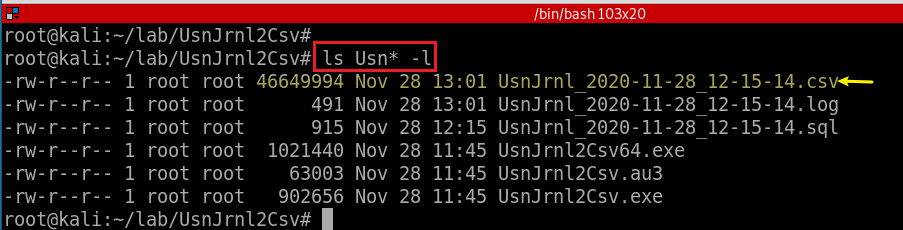
* Run *UsnJrnl2.exe* to covert *UsnJrnl.bin* to .csv

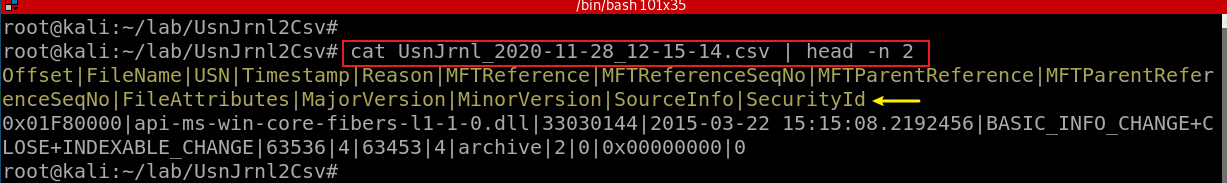


* Set configuration: Browser to *usnJrnl.bin*

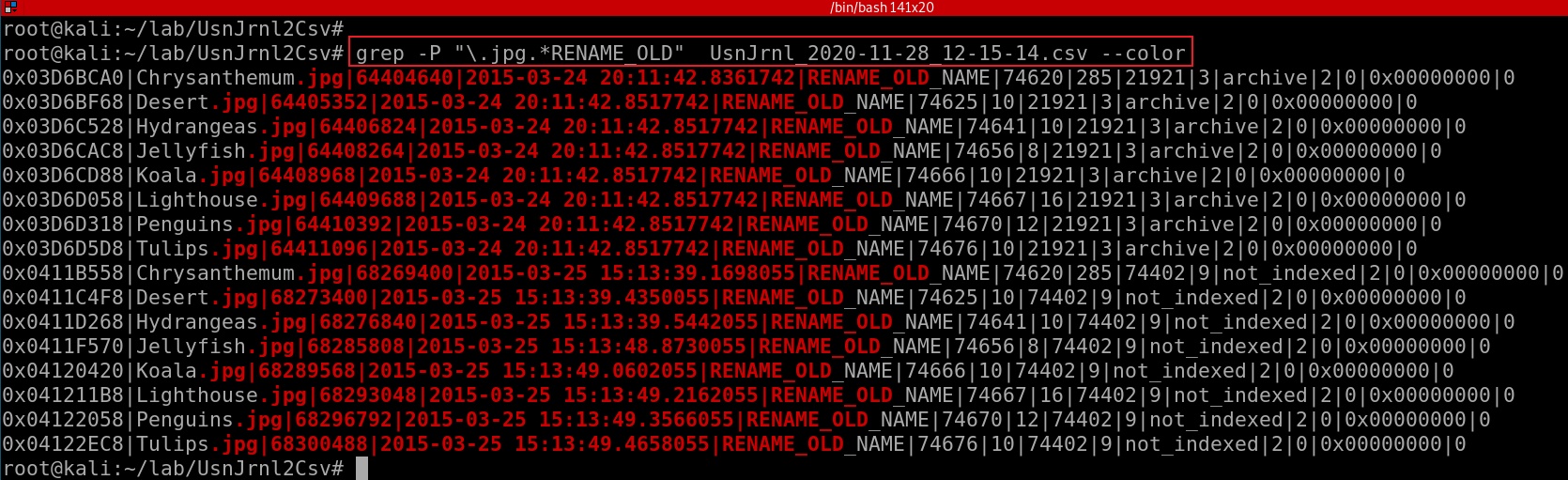
****

* Show the extracted USN journal file

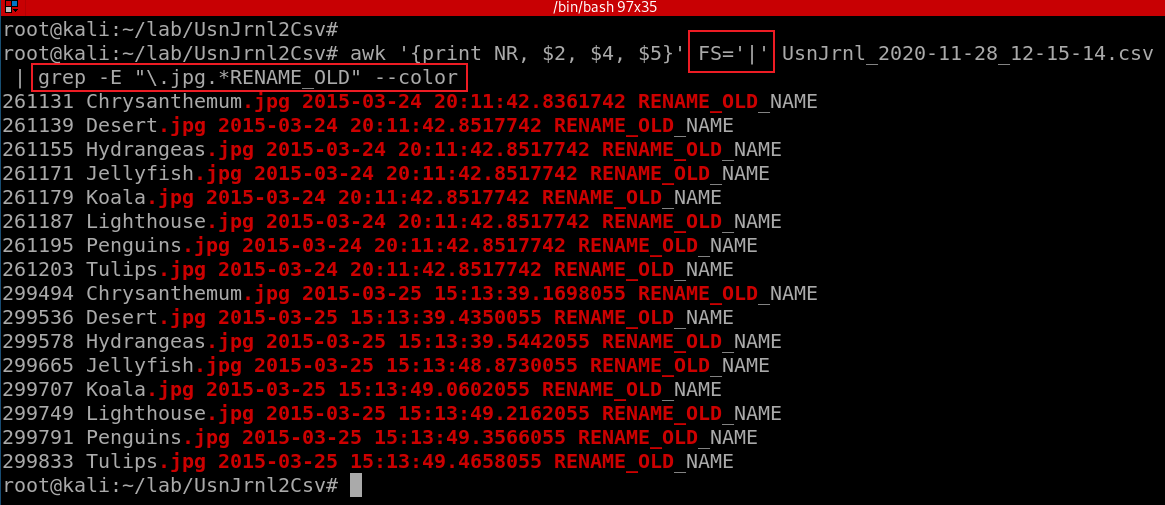
****

****

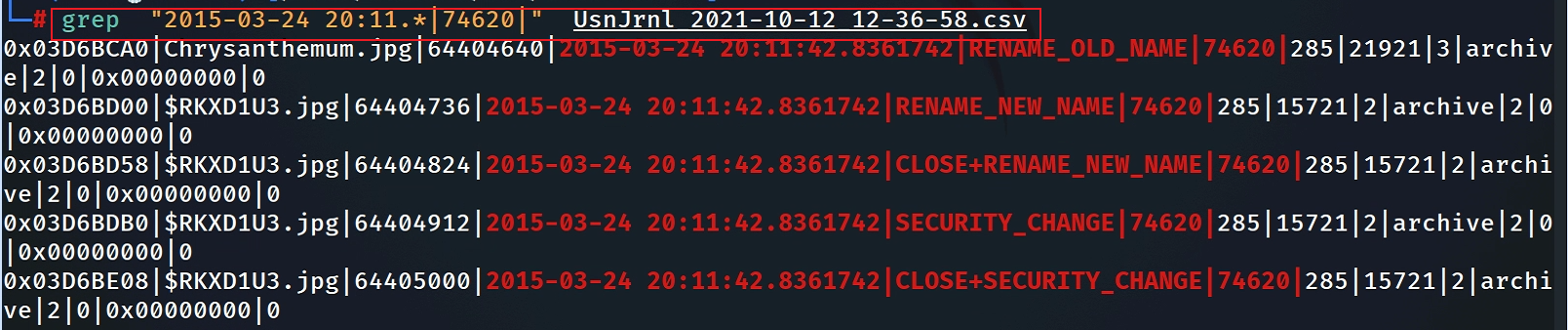
* Only show “*RENAME\_OLD*” information of any .jpg files

****

* Only show “RENAME\_OLD” information of any .jpg files. Only show three columns, FileName, Timestamp, Reason

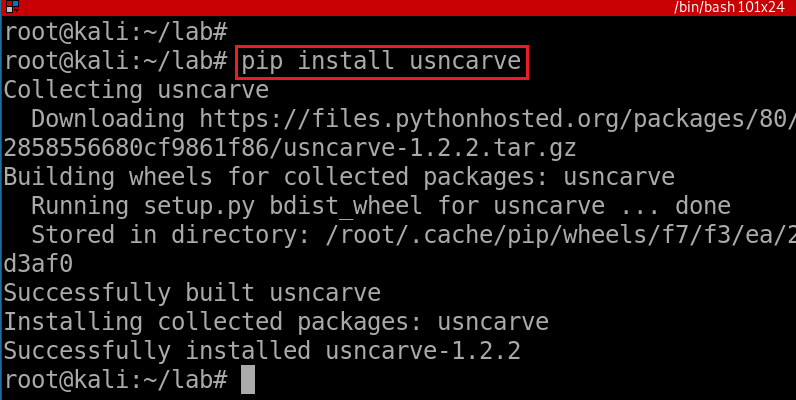


* Show what has happened around a specific time with the same MFT reference #

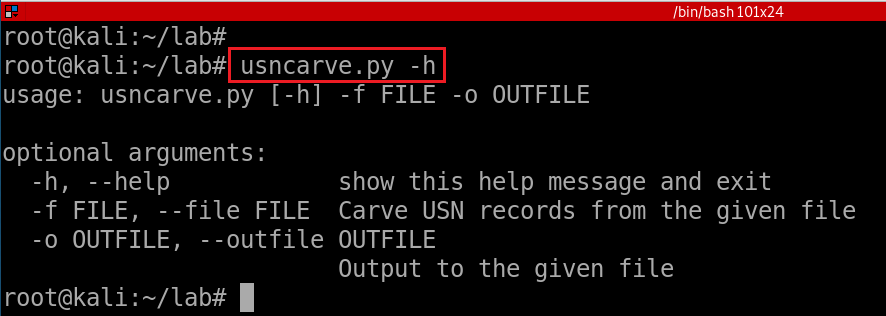


**Scenario 2**

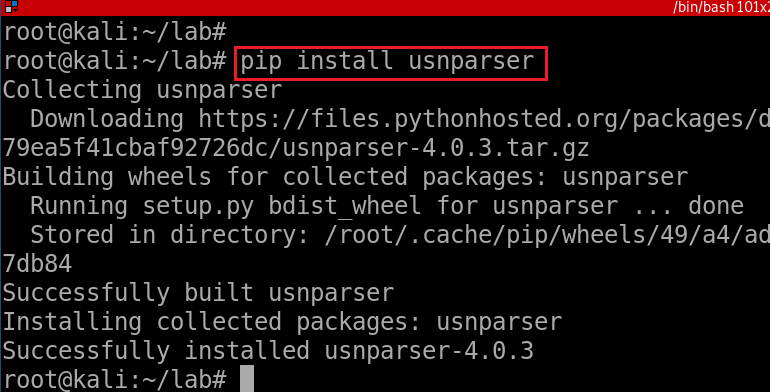
* Install *usncarve* tool (note we have changed the path)



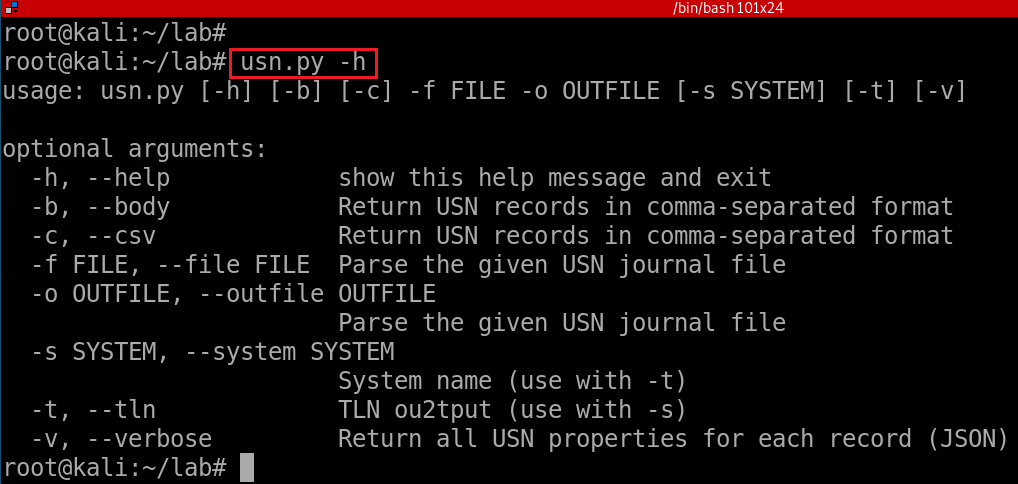
* Verify installation



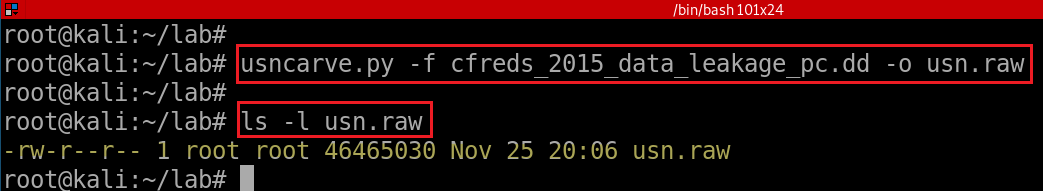
* Install usnparser tool



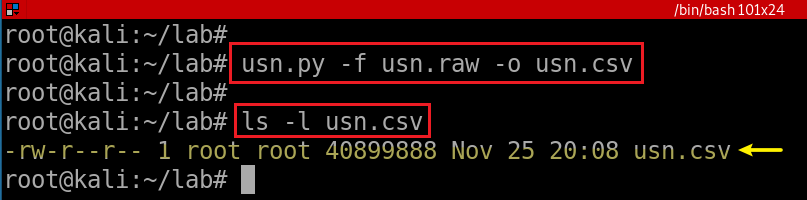
* Verify installation



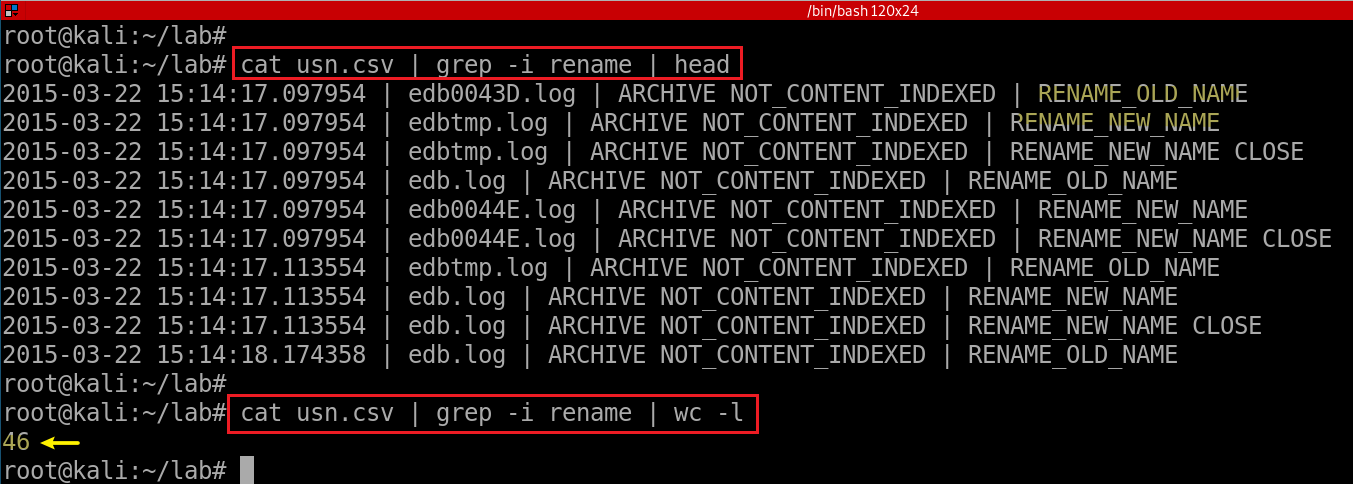
* *usncarve.py -f* input file *-o* output file

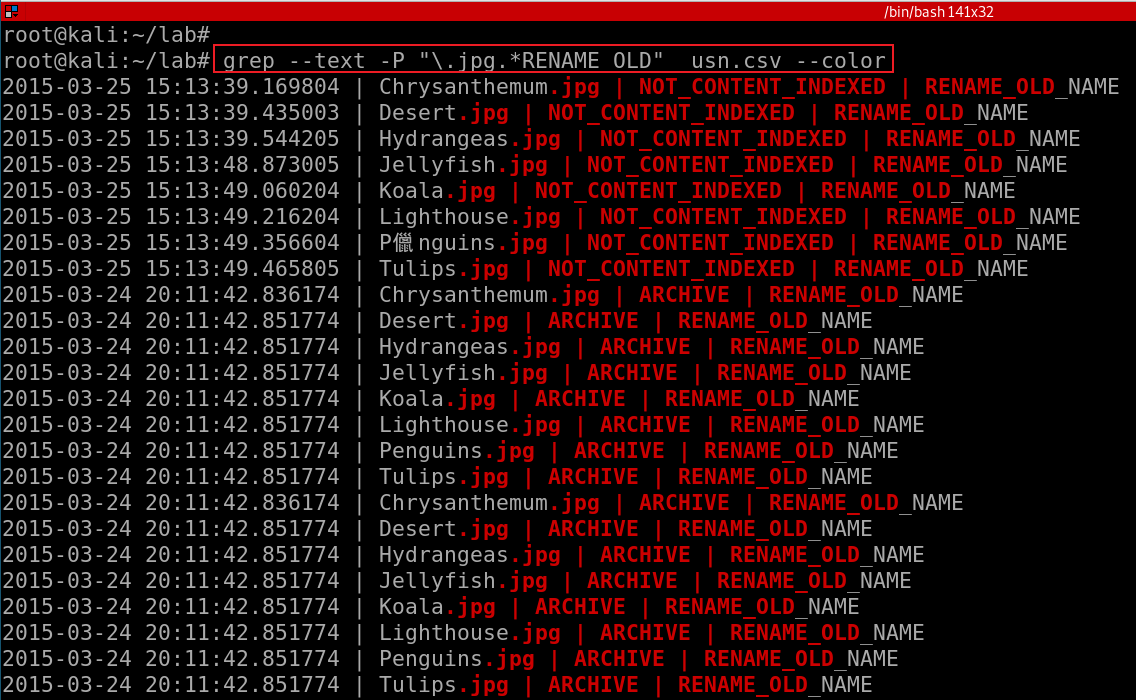


* *usn.py -f* input file *-o* output file



* View renamed files





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

Save the document with the filename "**YOUR NAME Lab 6.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 6 From YOUR NAME**", replacing "YOUR NAME" with your real name.