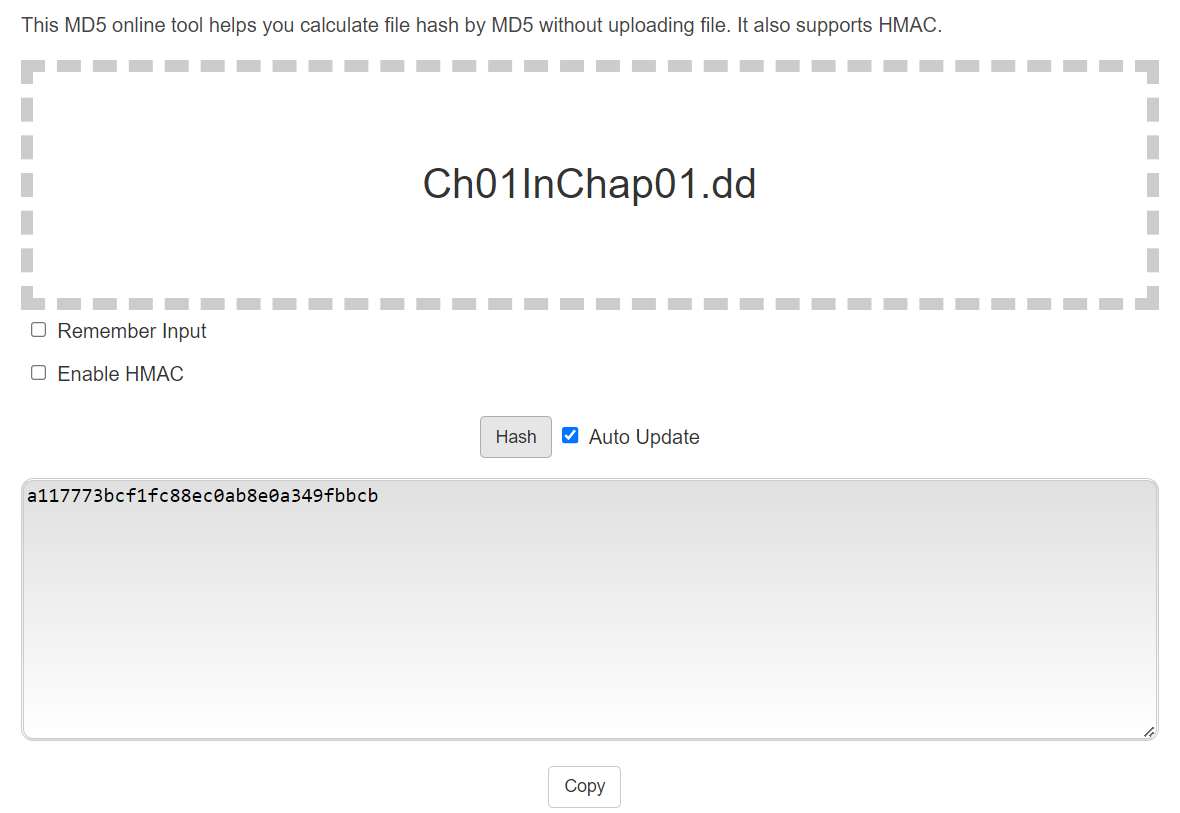
**Lab 1: Introduction to Digital Forensics – Autopsy software**

**What You Need for this lab**

* Windows 10
* Investigate a USB drive
  + Owned by George Montgomery
* Assume we have the image file
  + <https://www.dropbox.com/s/nw23q14vzsykyup/Ch01InChap01.dd>
  + (from book Guide to Computer Forensics and Investigations. Sixth Edition)
* Software
  + Autopsy : <https://www.autopsy.com/download/>
* Tasks
  + Recover Word files, images
  + Search key words

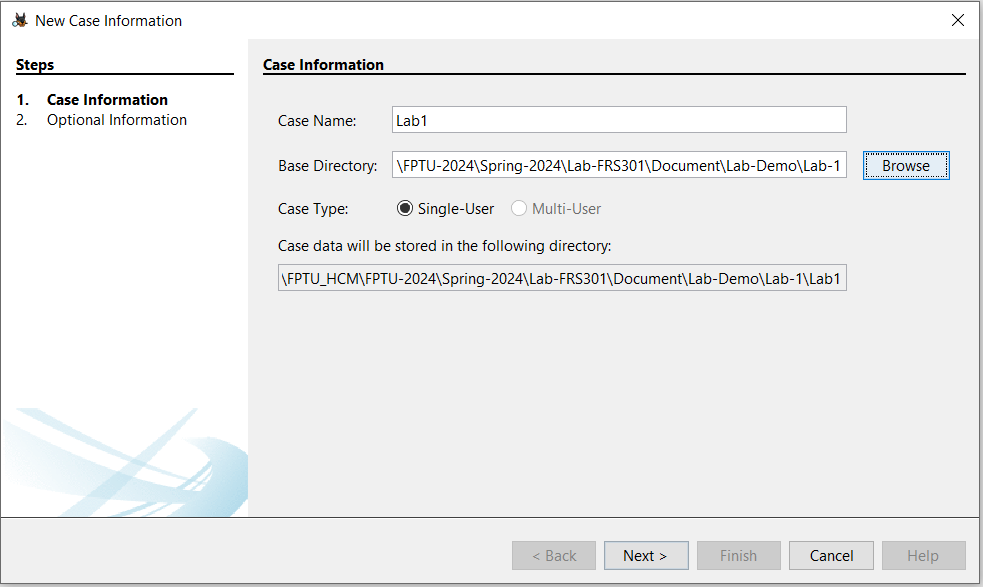
**Step 1.**

Check hash code online : <https://emn178.github.io/online-tools/md5_checksum.html>

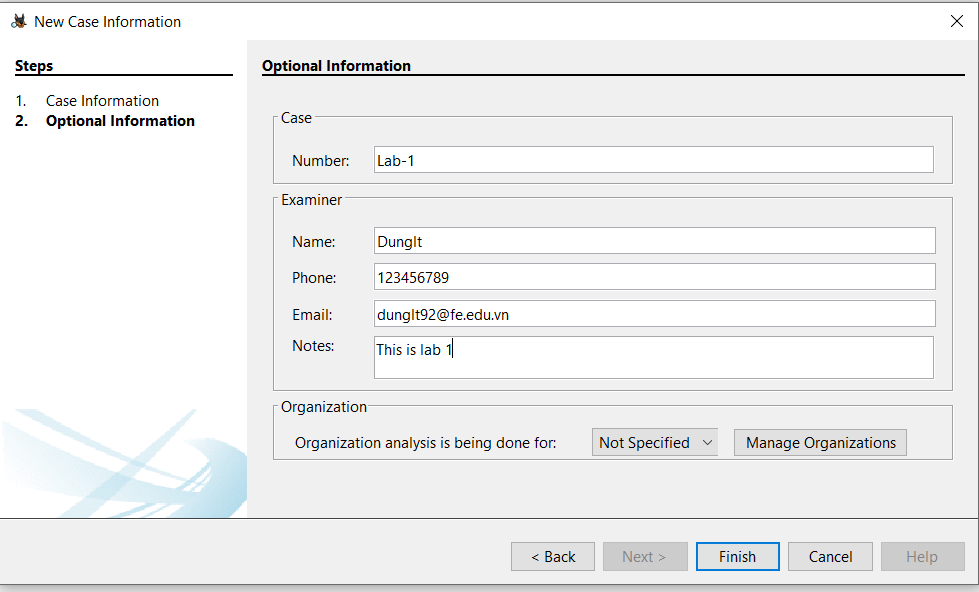


**Step 2.**

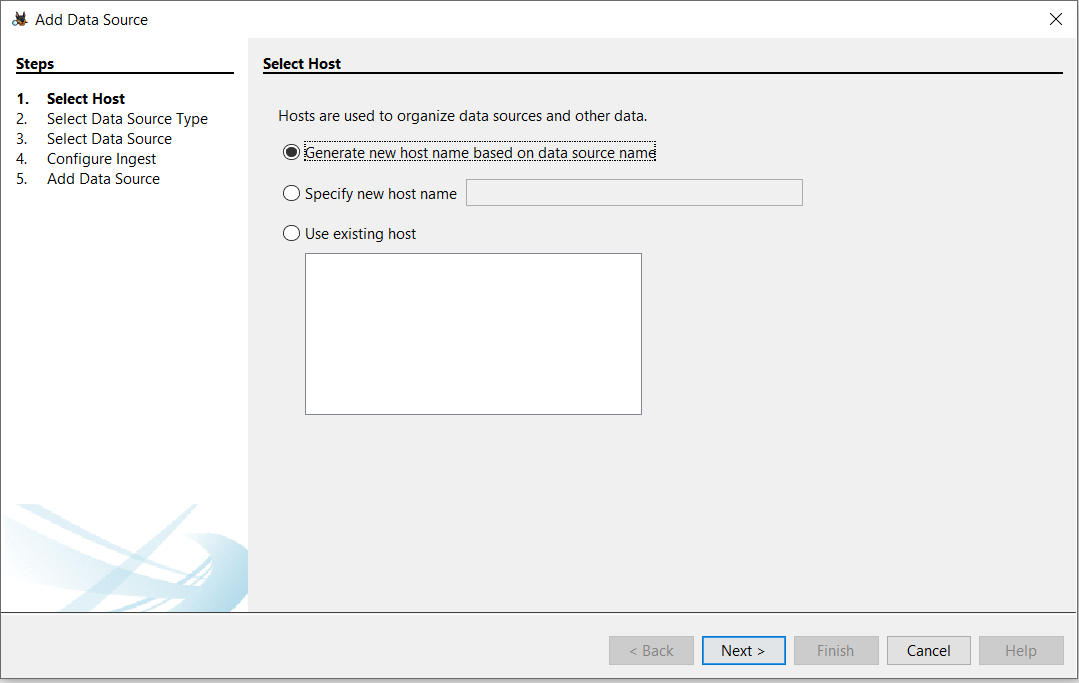
Create a case with name



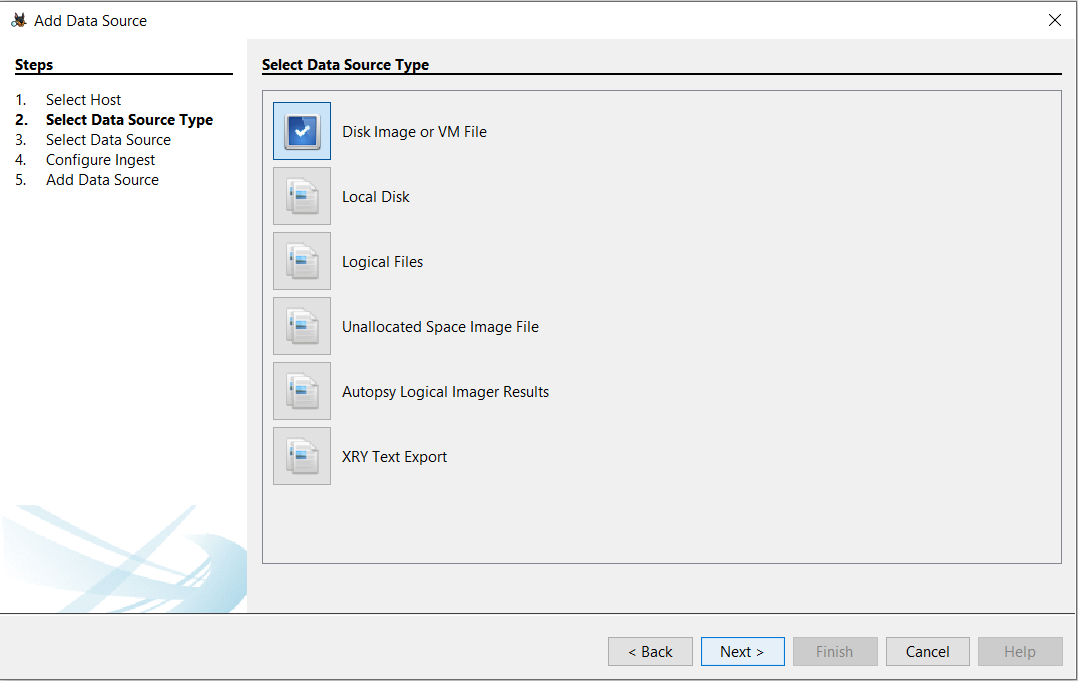
Details of the case



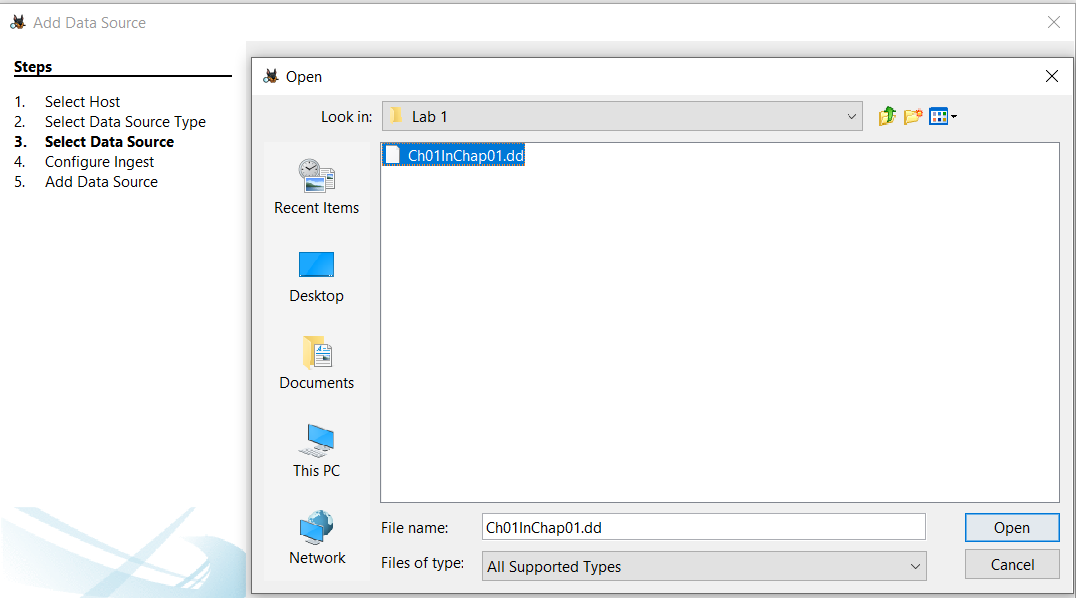
Choose Data Format

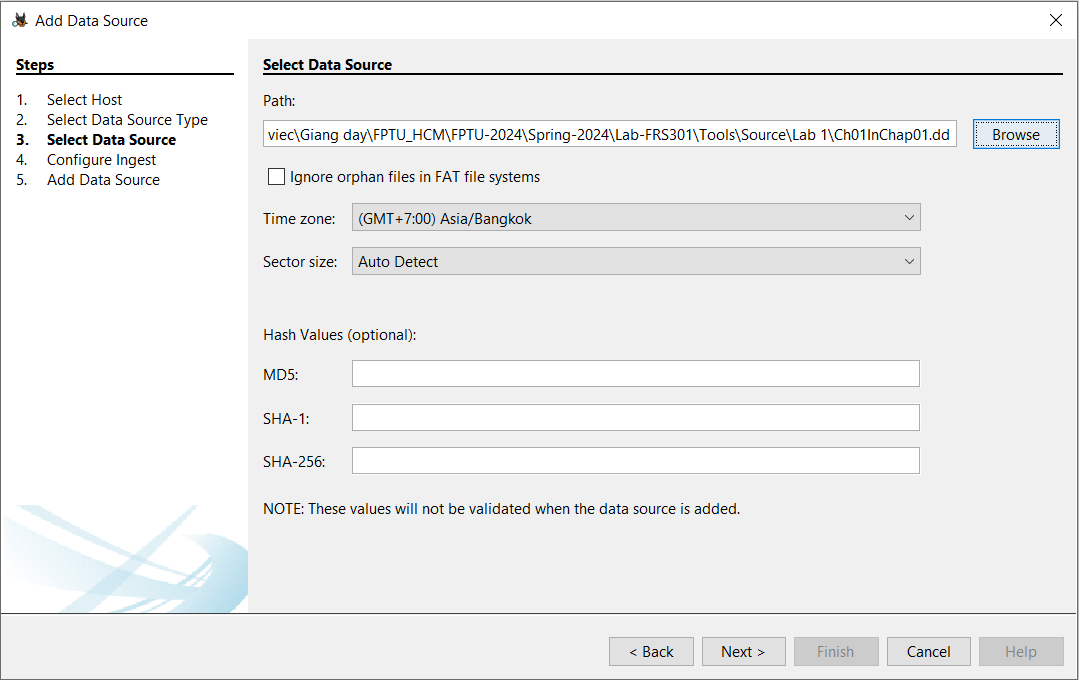


Click Disk Image or VM File

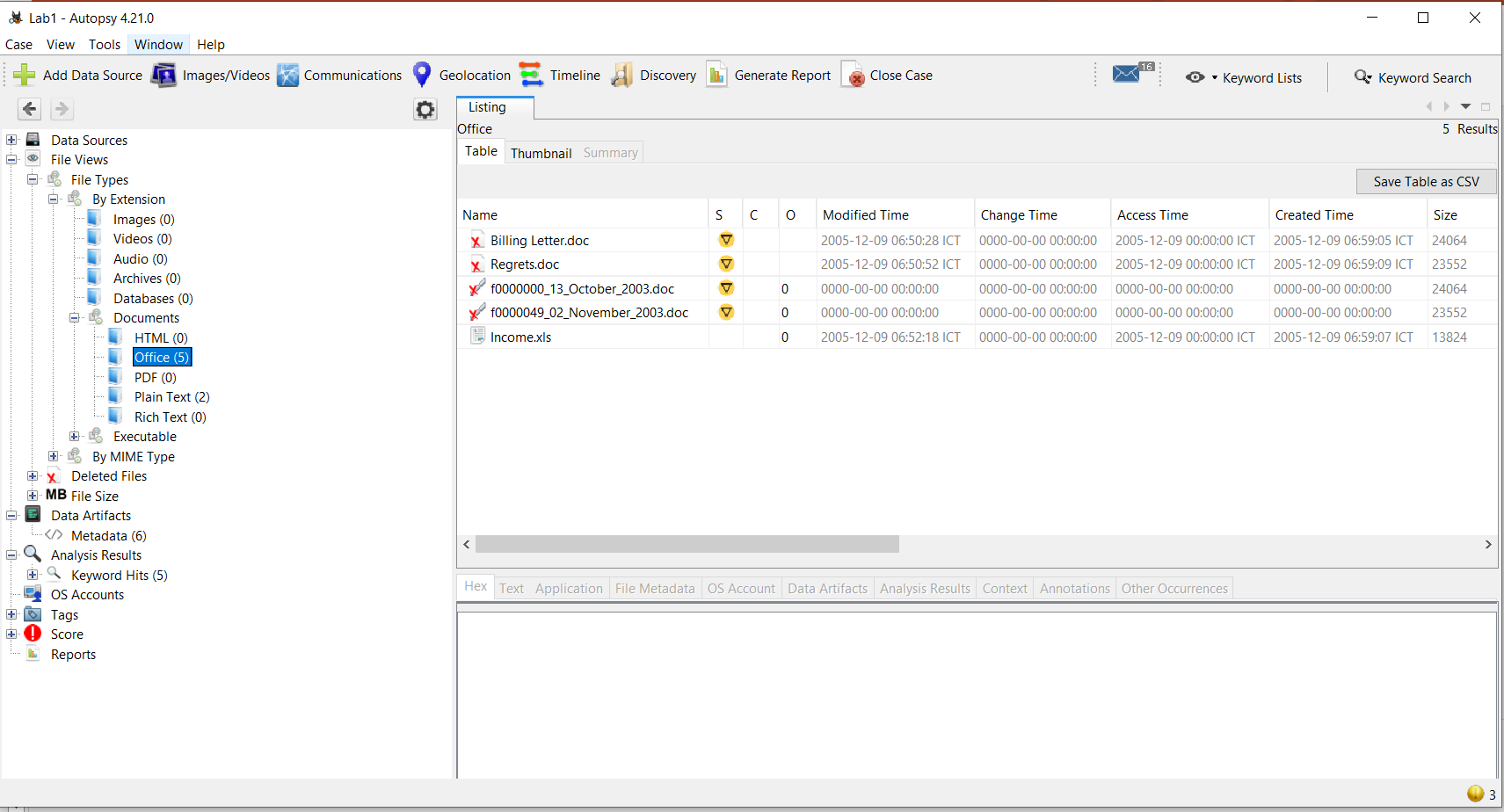


Choose the image file

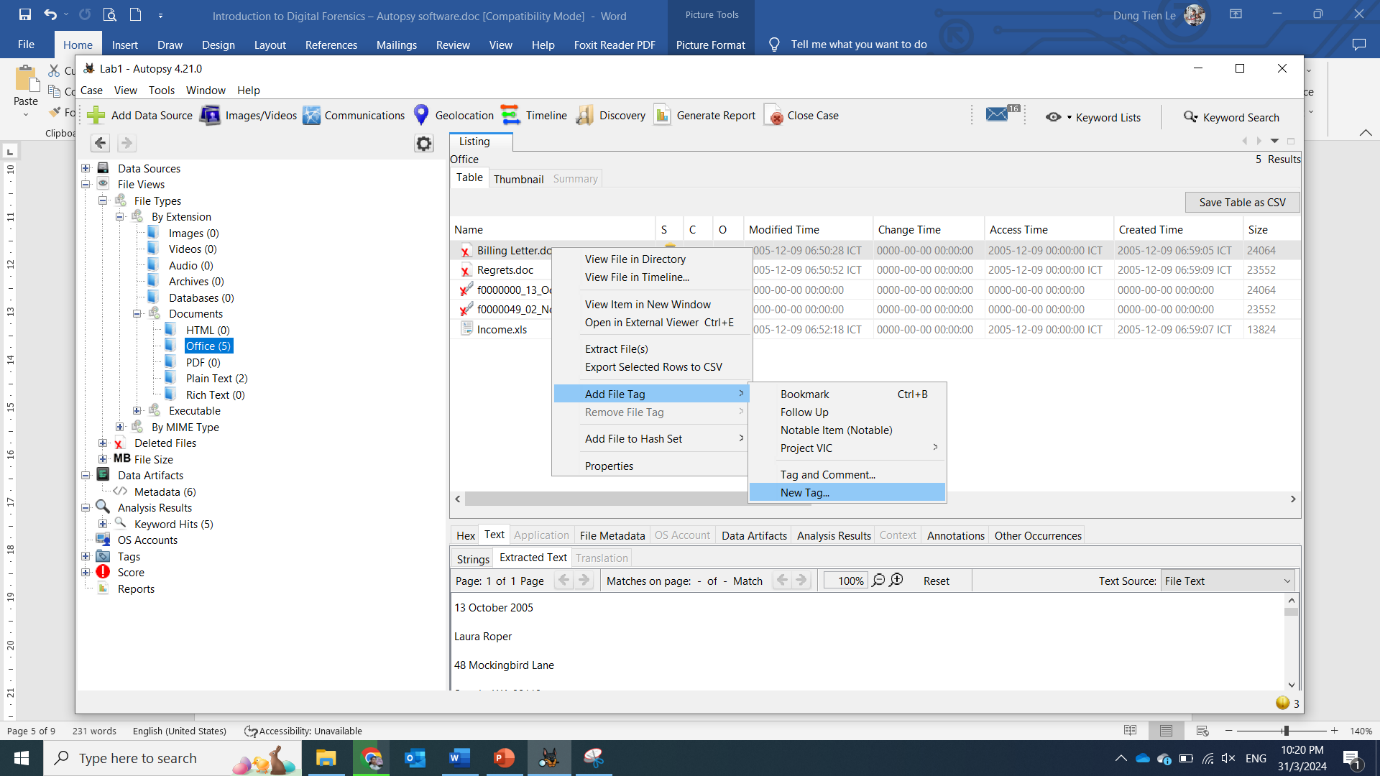




Find deleted files :

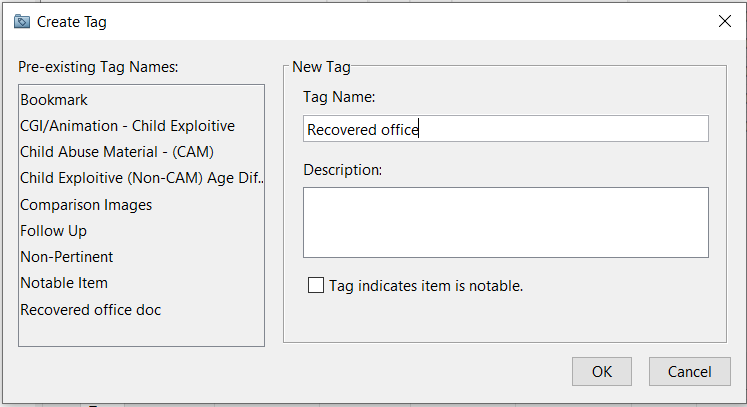


Tag the file: right click and click New Tag

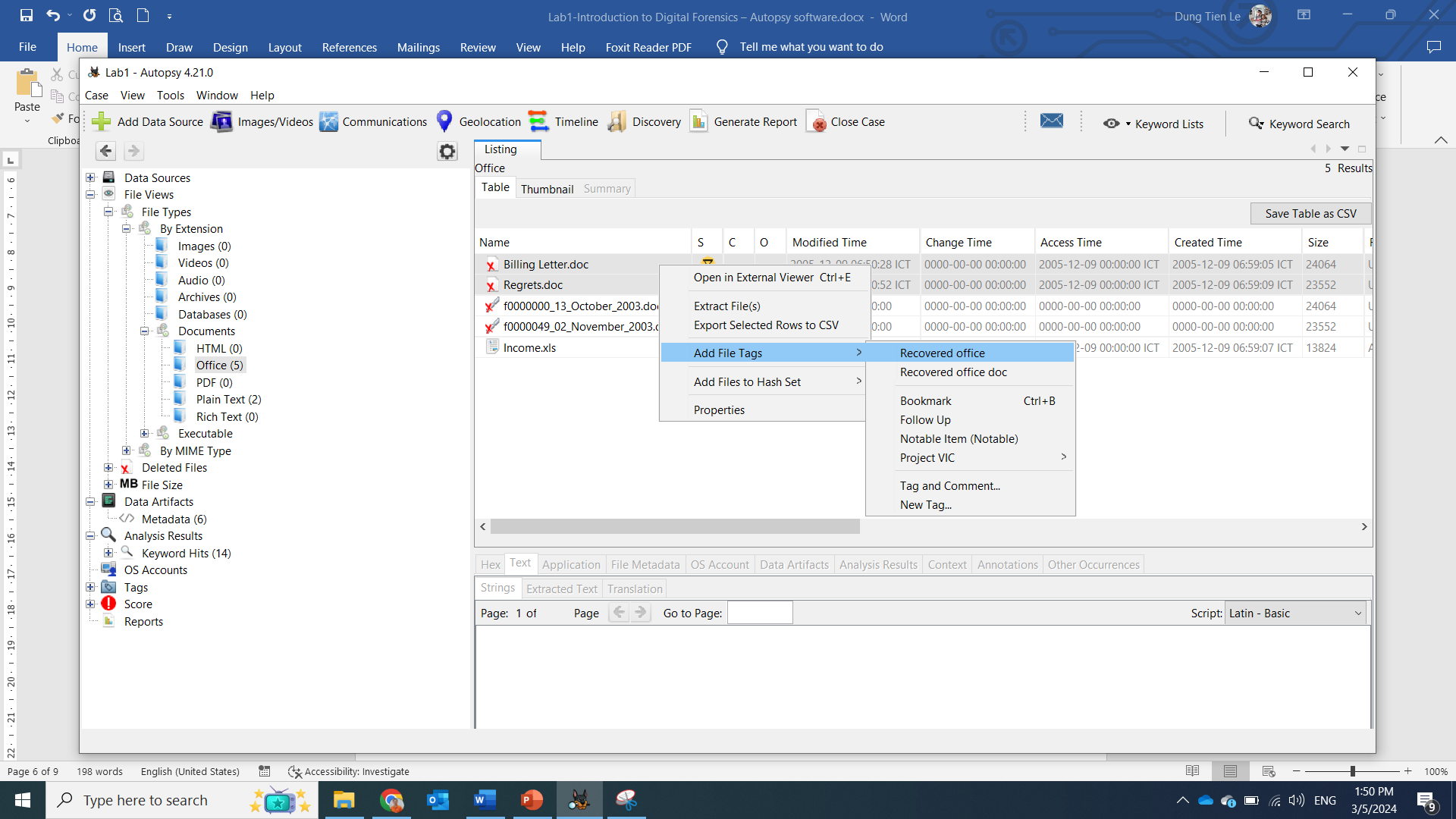


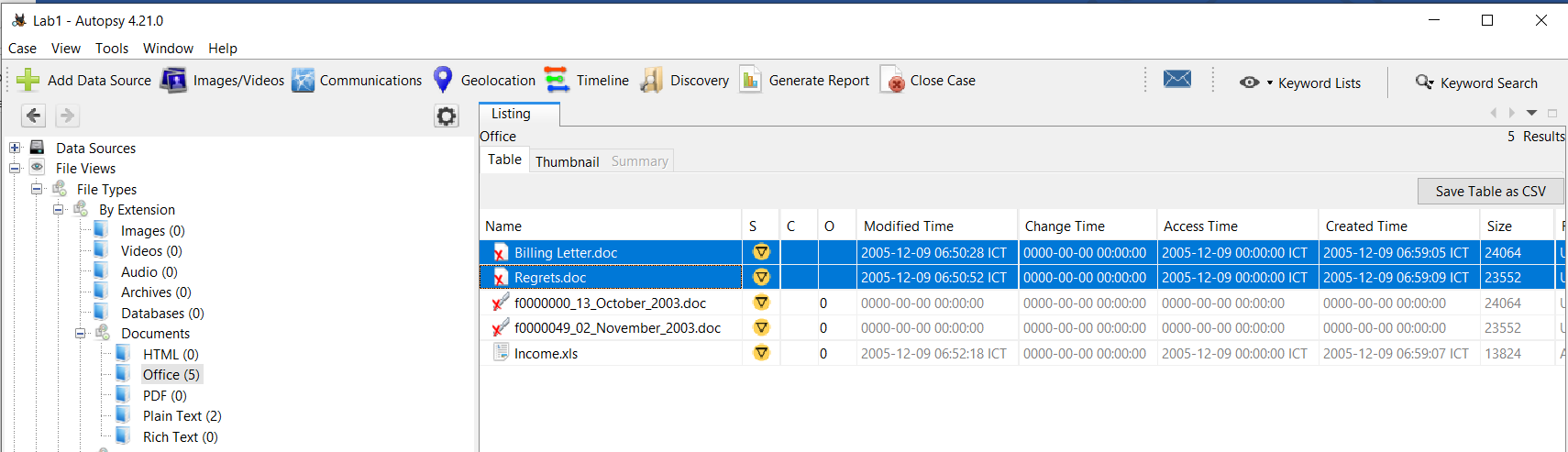
**Step 3.**

Create a tag for reporting



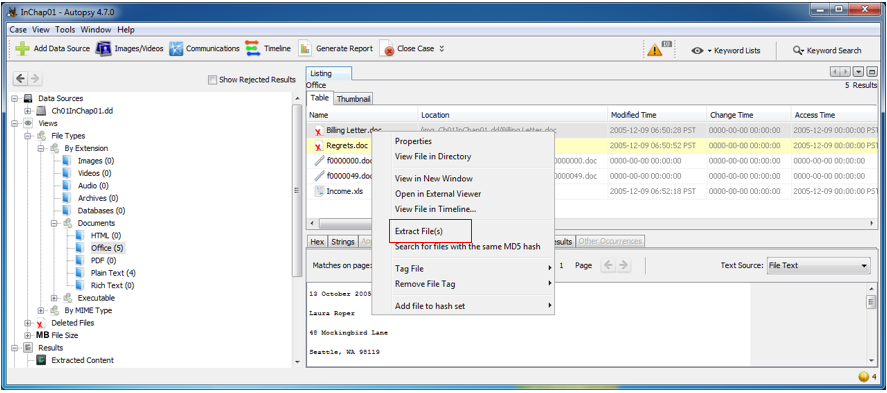
Tag both deleted files

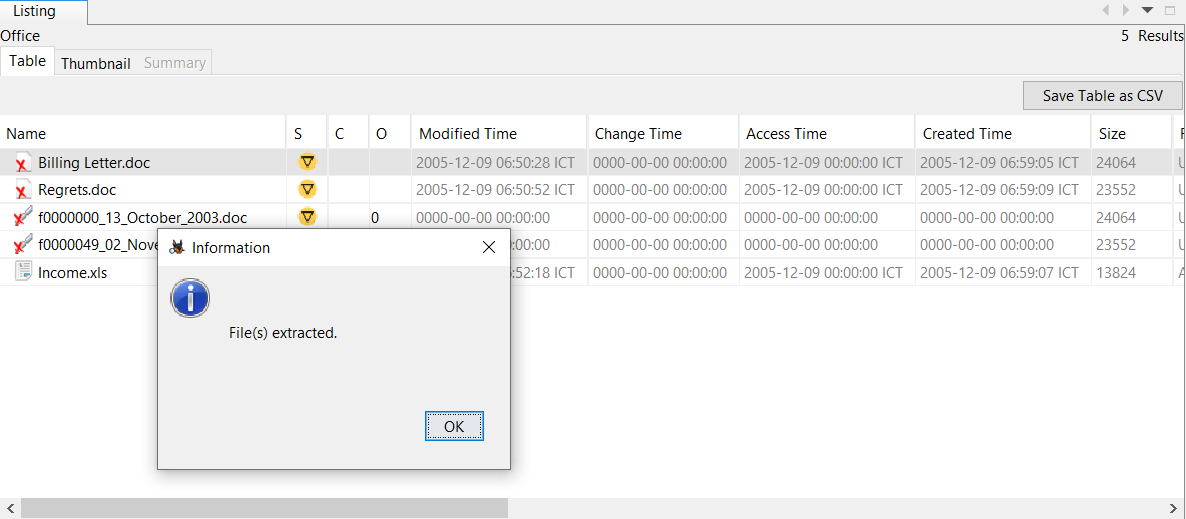




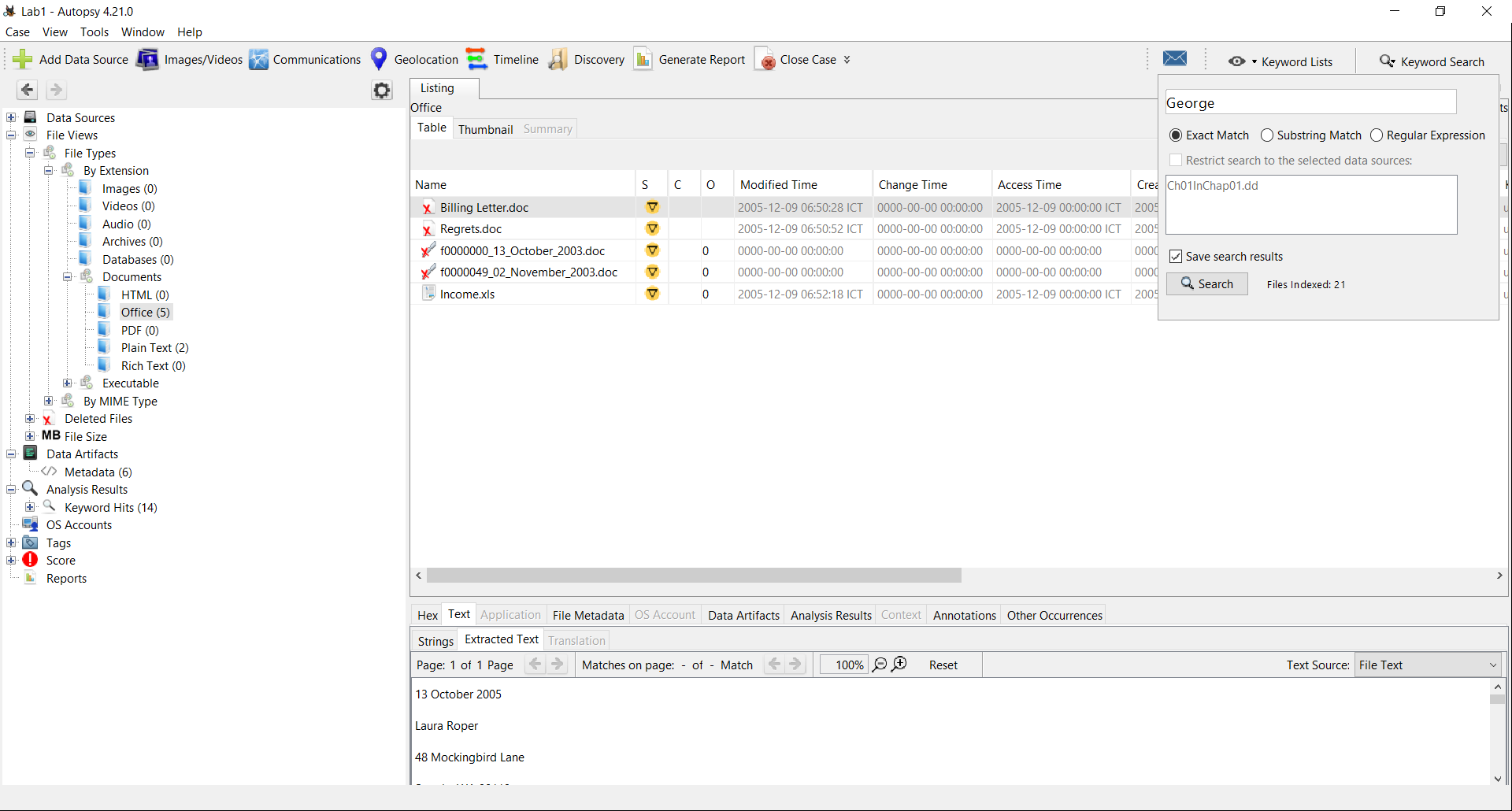
**Step 4.**

Recover deleted file

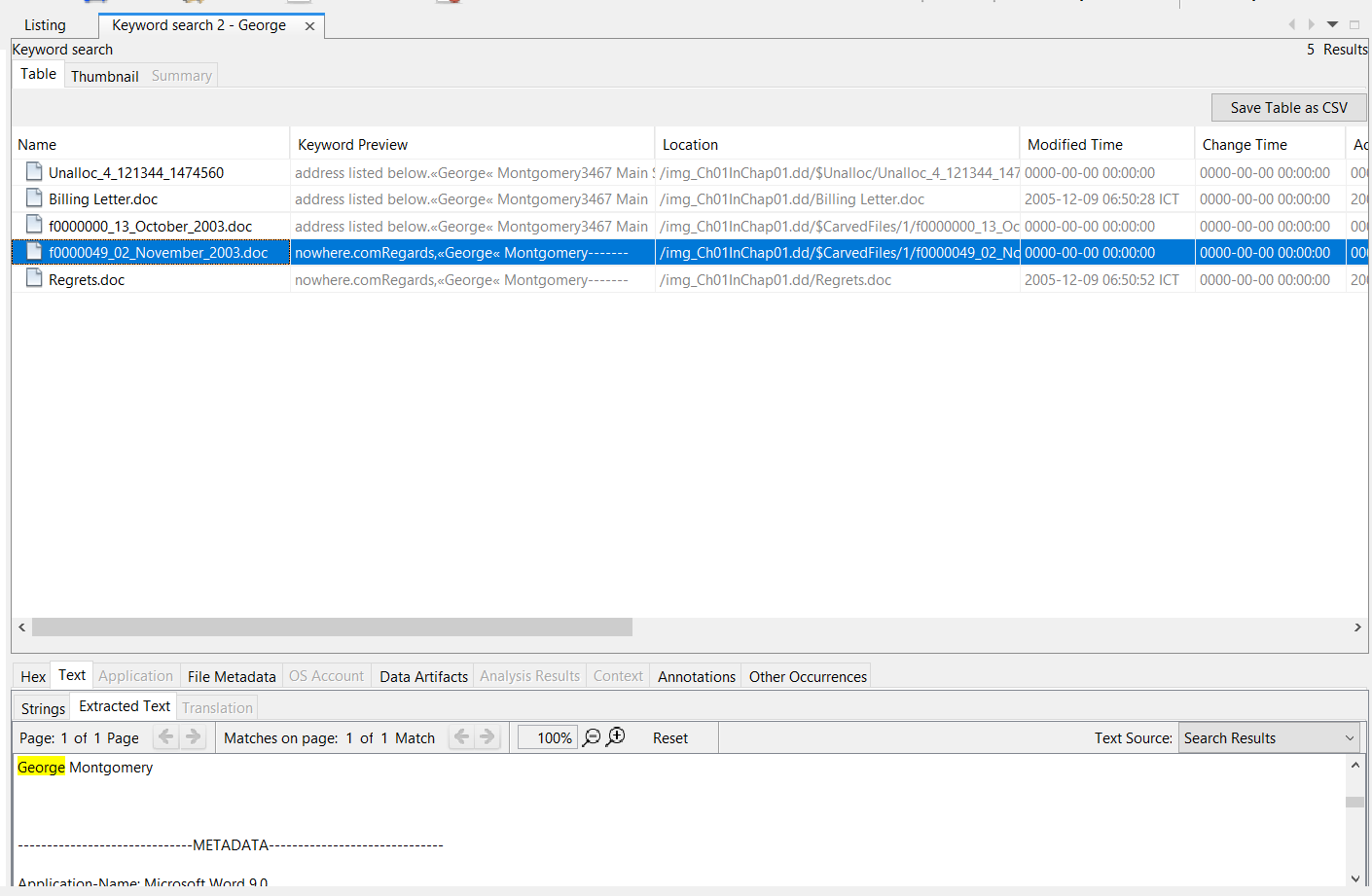




Search keywords : **“George”**

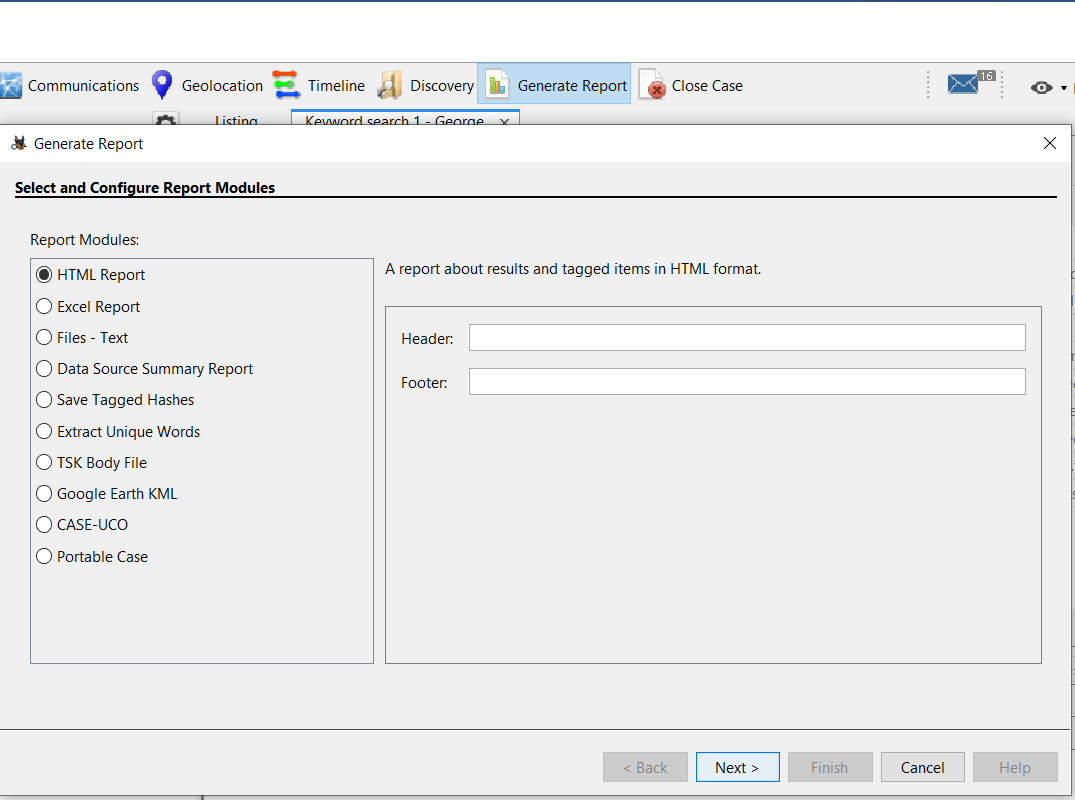


Search results

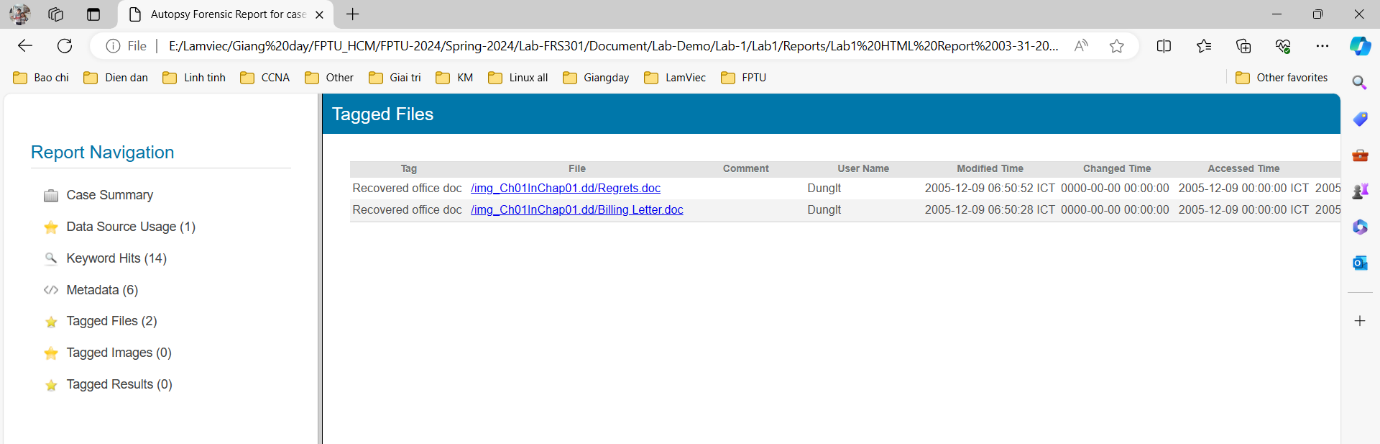


**Step 5.**

Generate reports



Open or Save as file doc is recovered.



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

Save the document with the filename "**YOUR NAME Lab 1.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 1 From YOUR NAME**", replacing "YOUR NAME" with your real name.