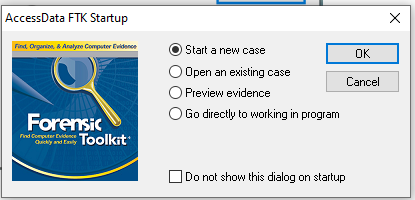
FTK & Autopsy

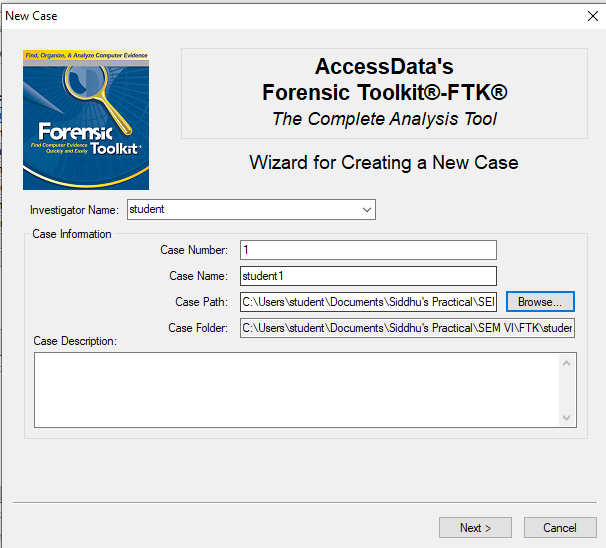
**Q.1]** Use FTK tool

**Steps:**

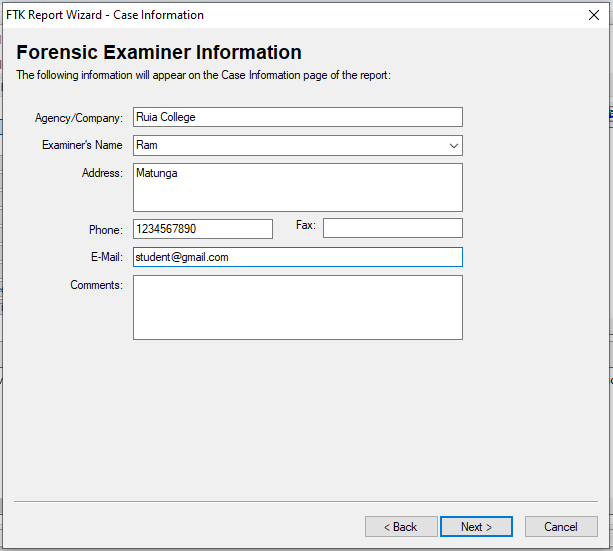
1. Install FTK and after that choose start a new case



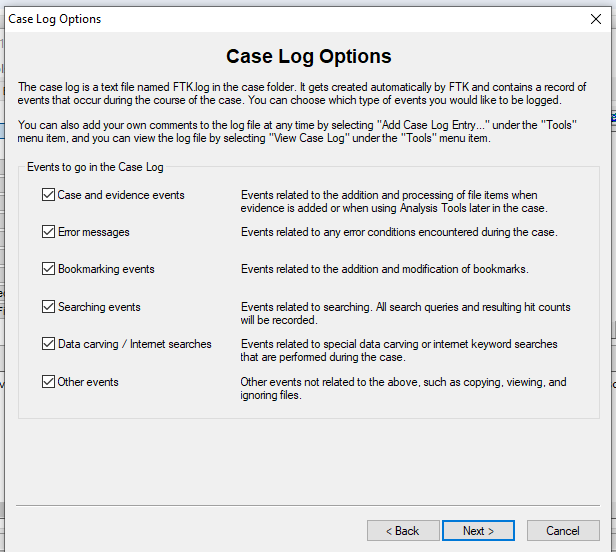
1. Enter the case detail



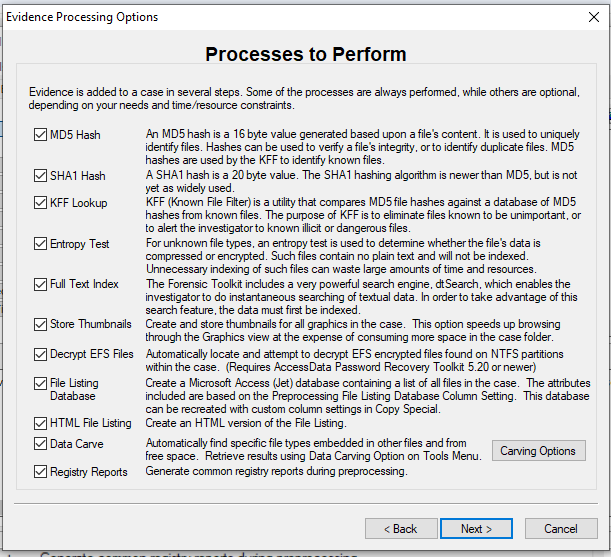
1. Enter the following details



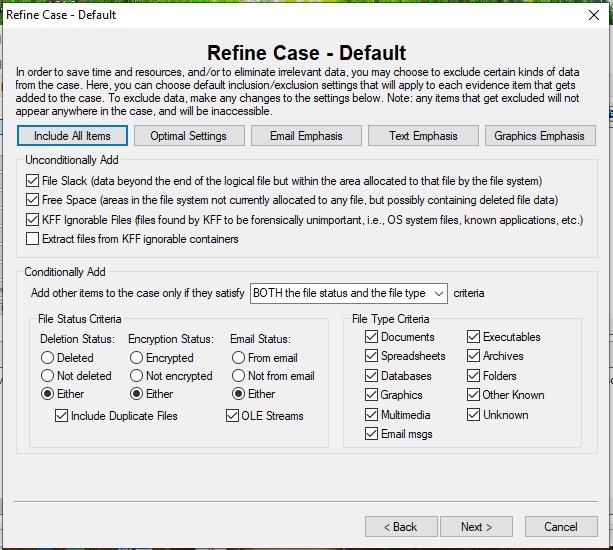
1. Click Next



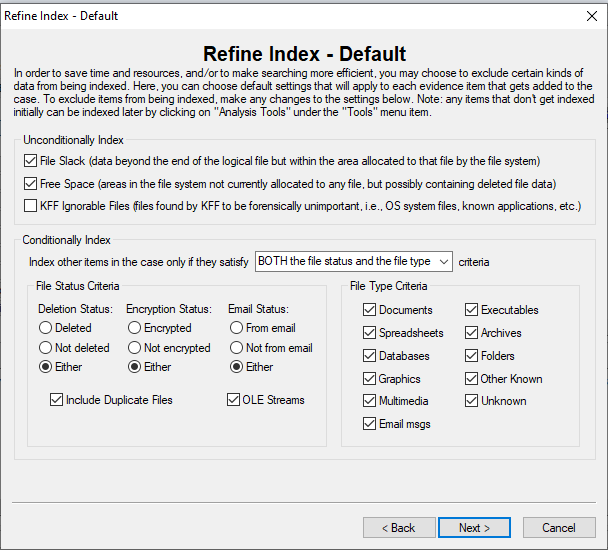
1. Select all options



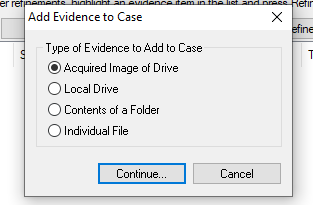
1. Click next

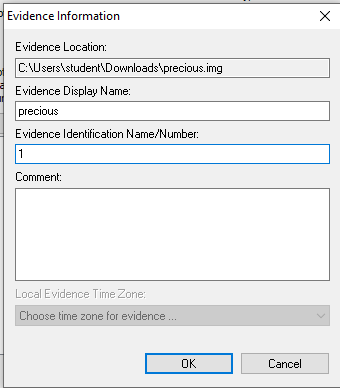


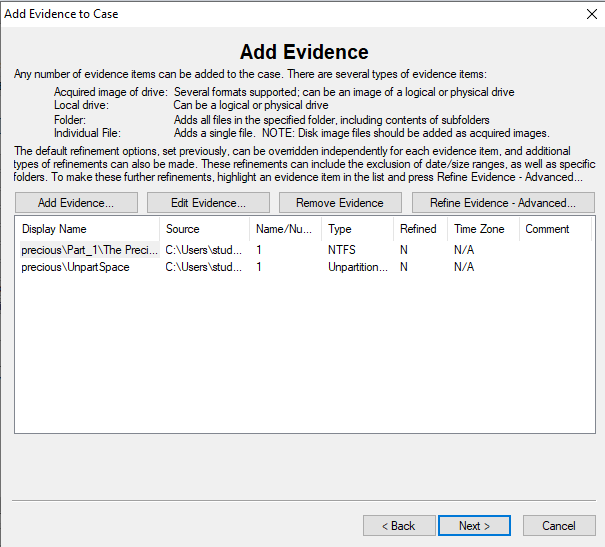
1. Click next

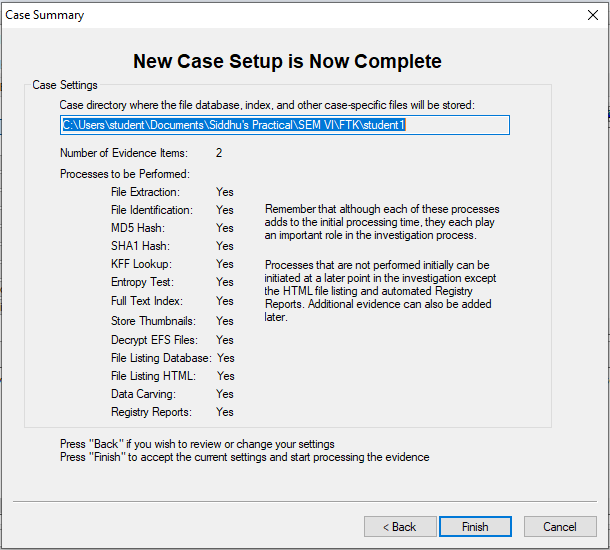


1. Add evidence

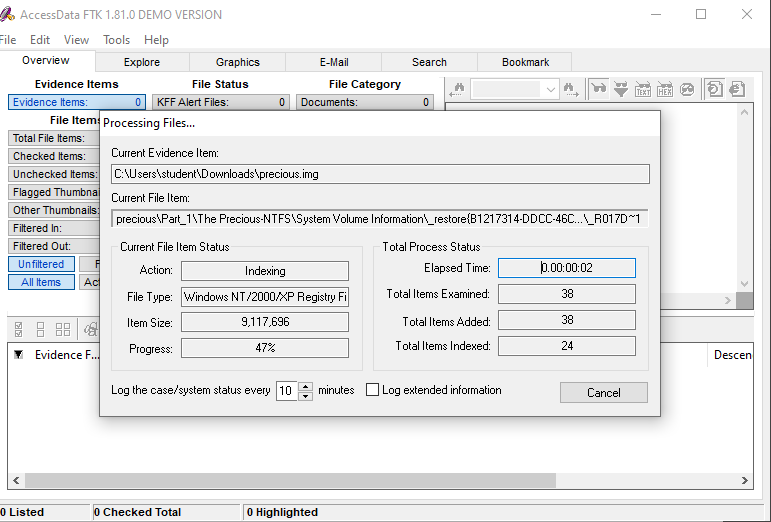




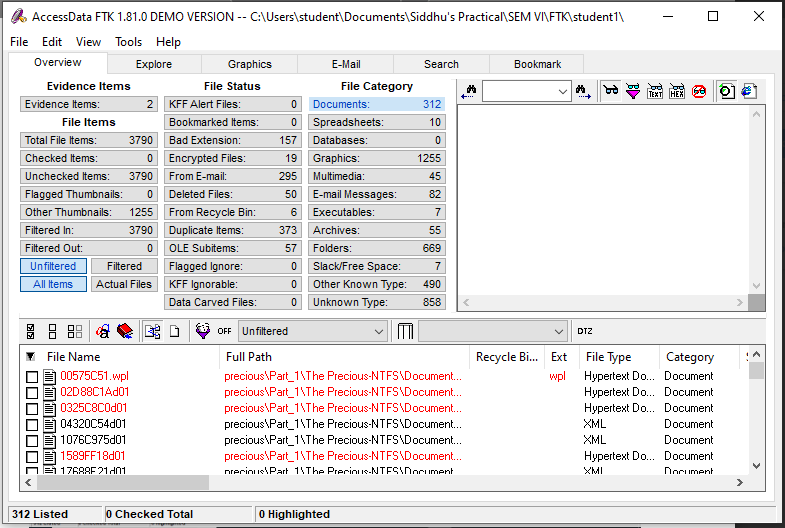




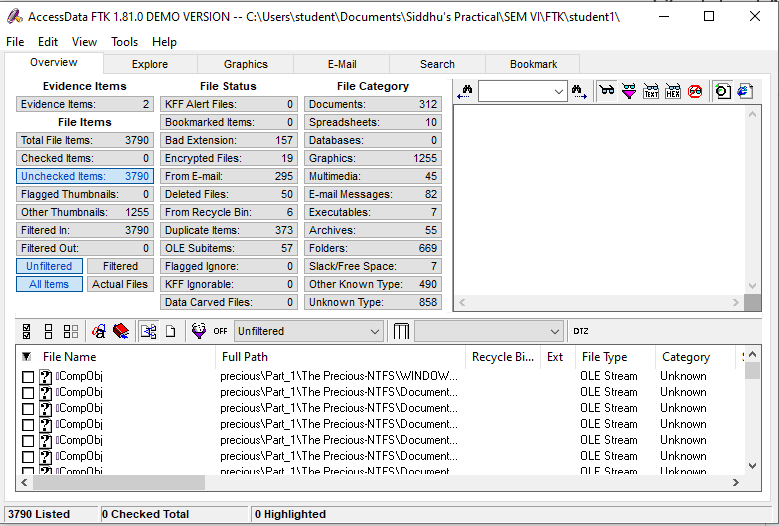
1. Click finish and it will take some time to analyze



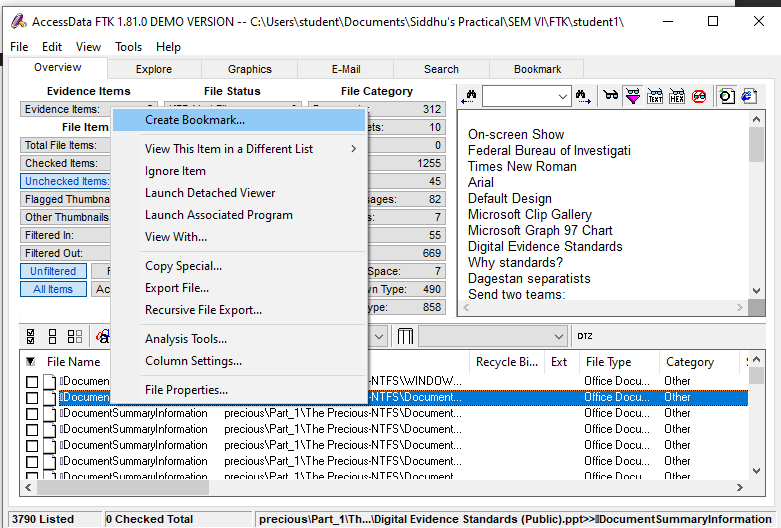
1. Click on documents

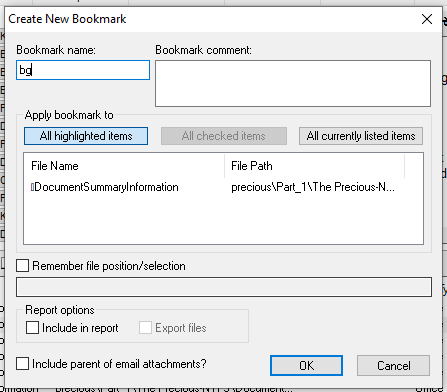


1. Click on unchecked items

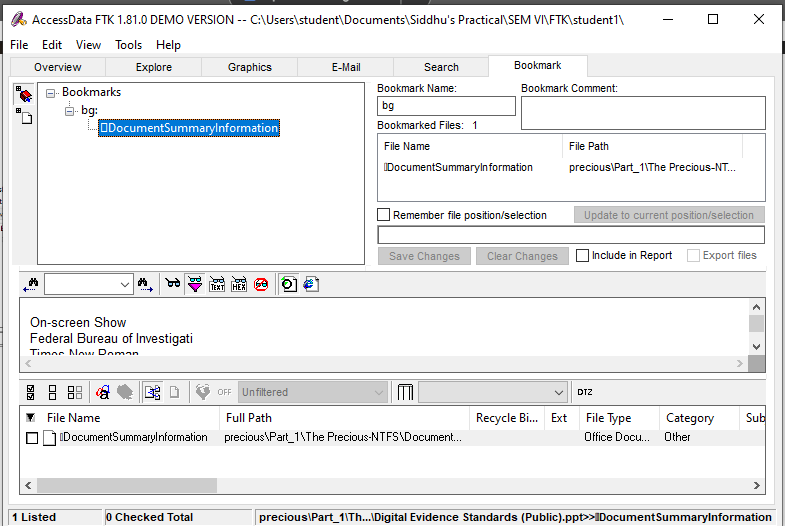


1. RIght click any file > create bookmark

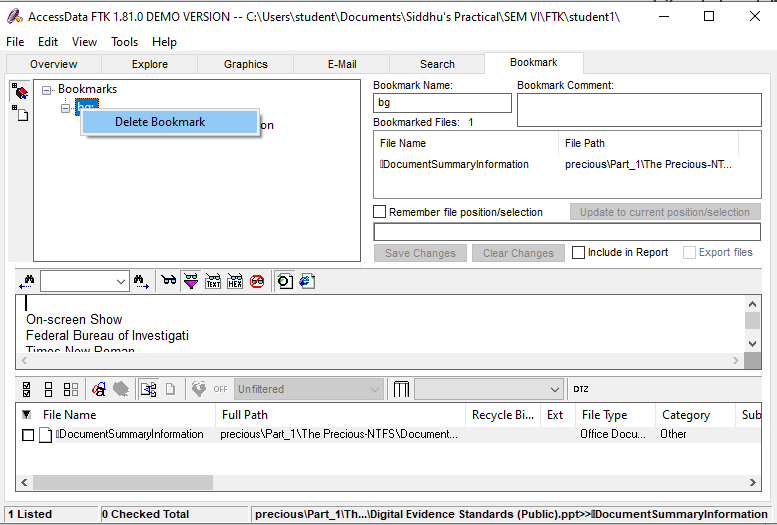


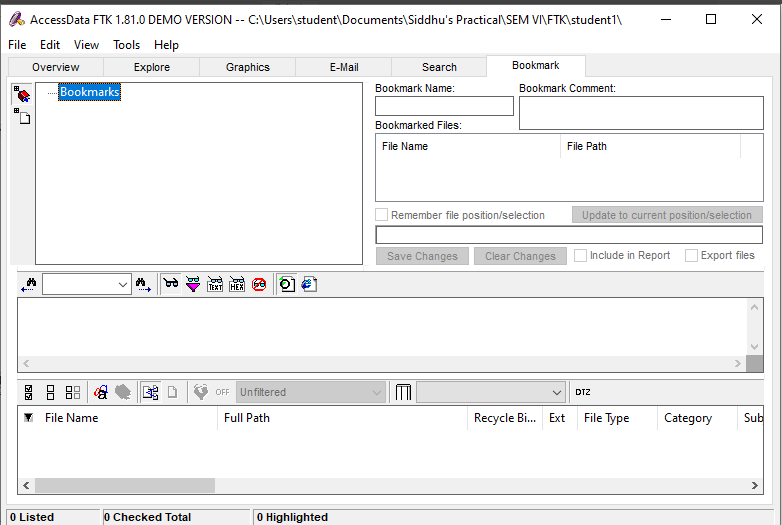


1. The bookmark will be added, click bookmark tab

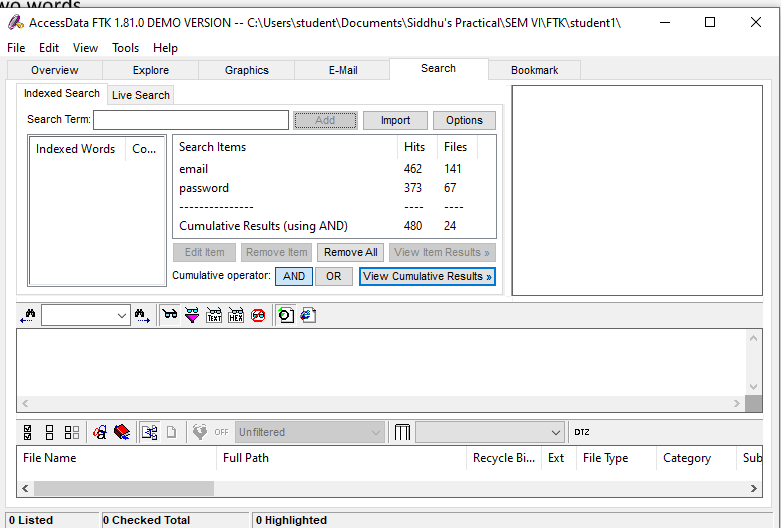


1. Right click the bookmark to delete it

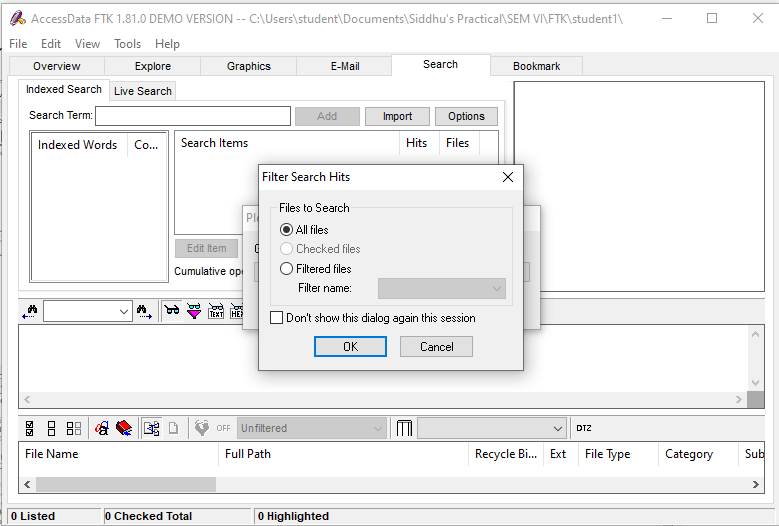


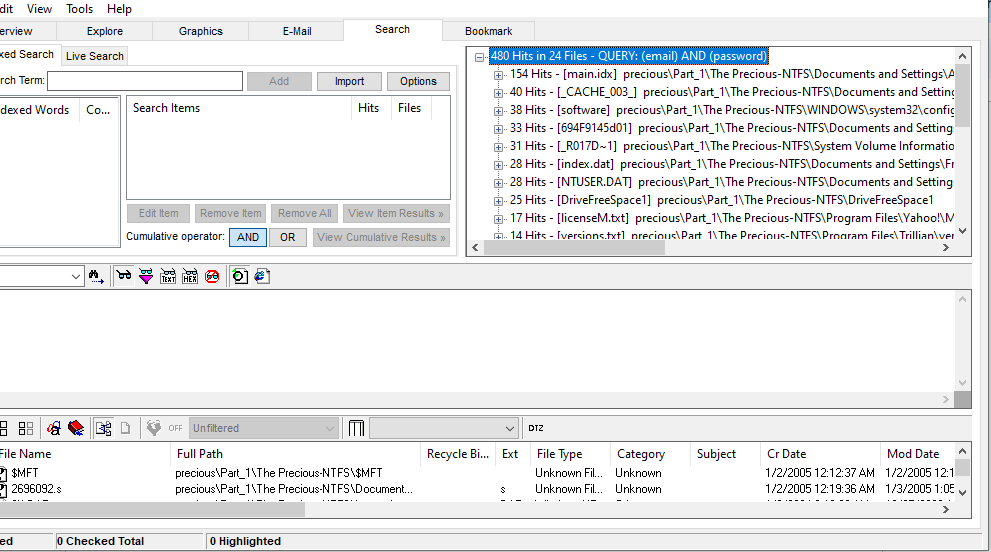


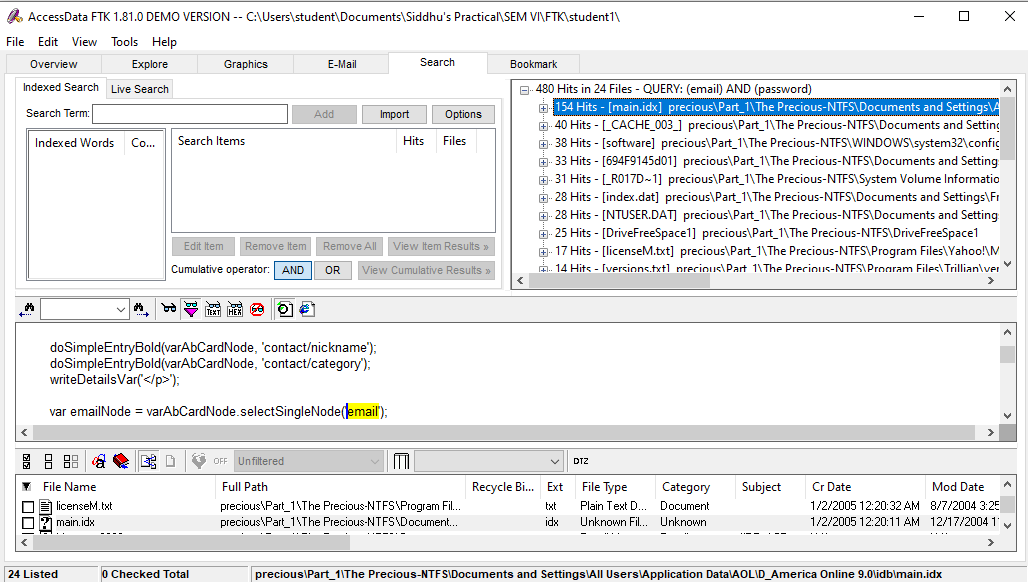
1. Go Search tab > indexed search tab and the following keywords



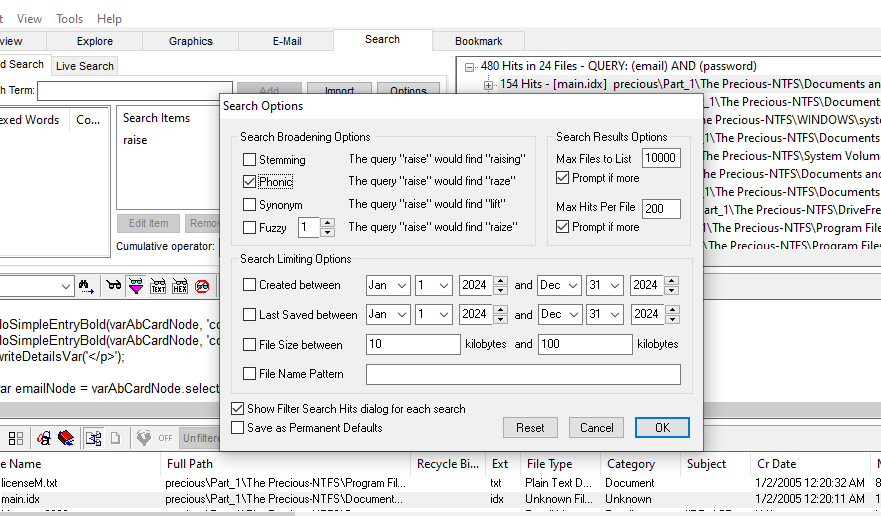
1. Click view cumulative results

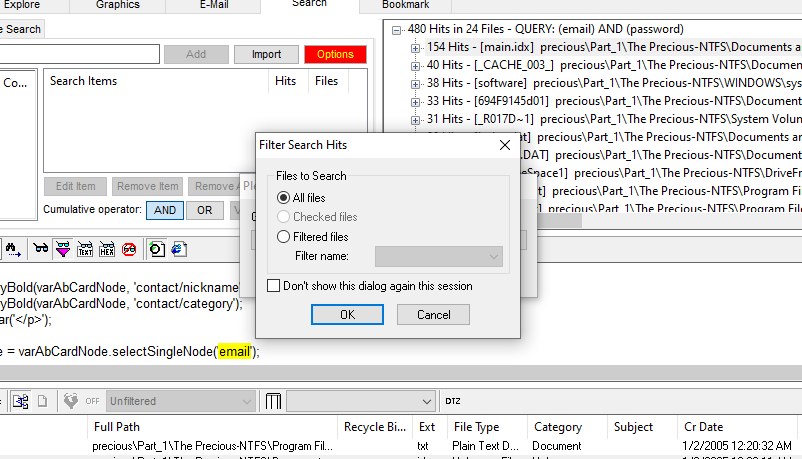




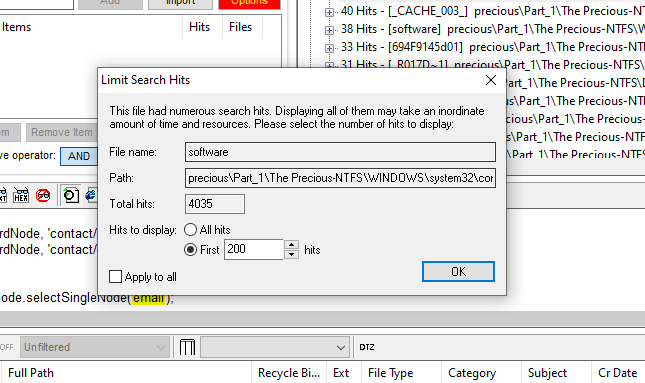


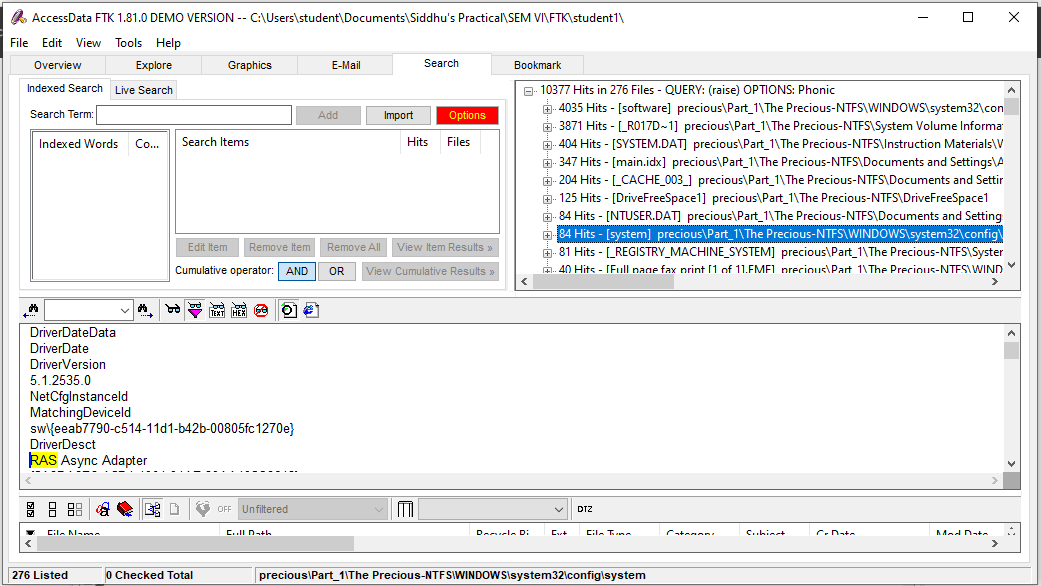
1. Add new keyword, click options and select the following options



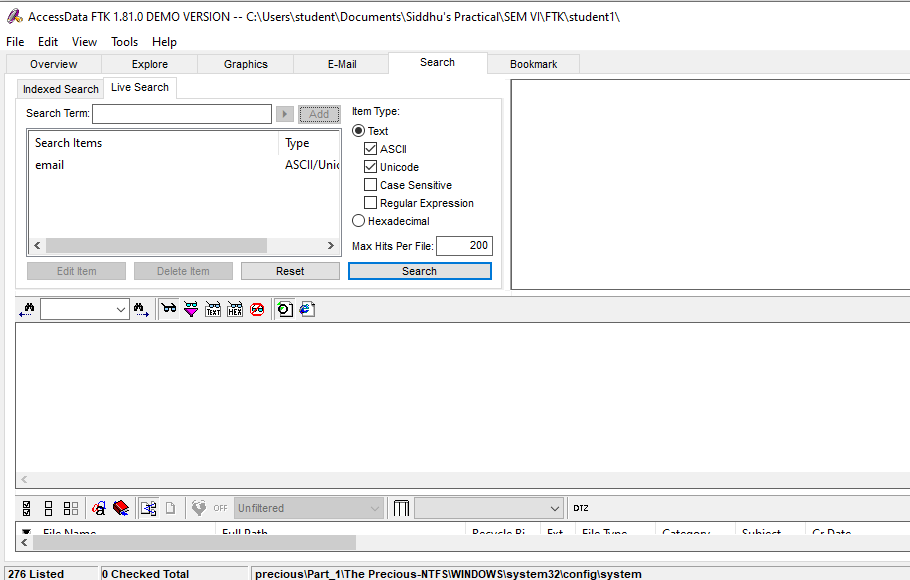


(click ok for all)

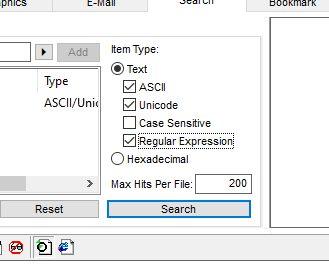




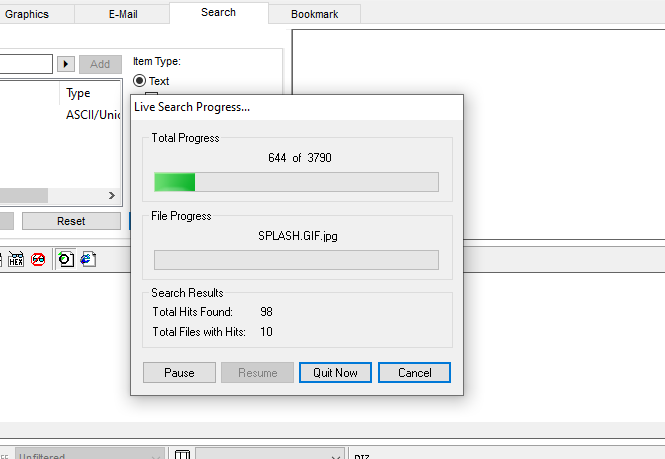
1. Go to live search tab and add the following keyword

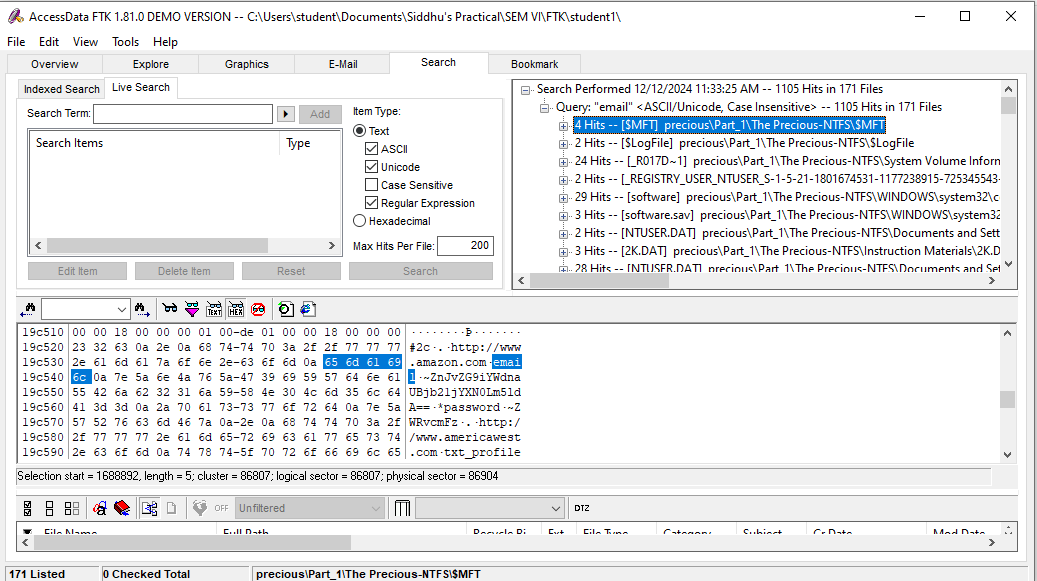


1. Check regular expression

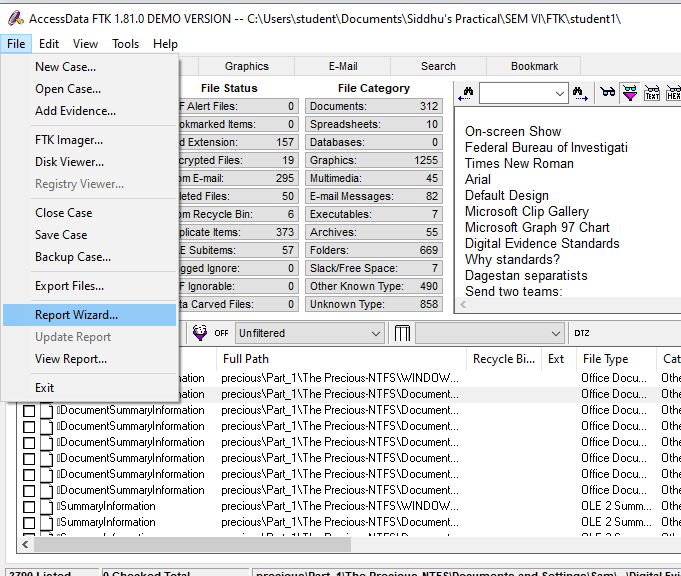


1. Start search

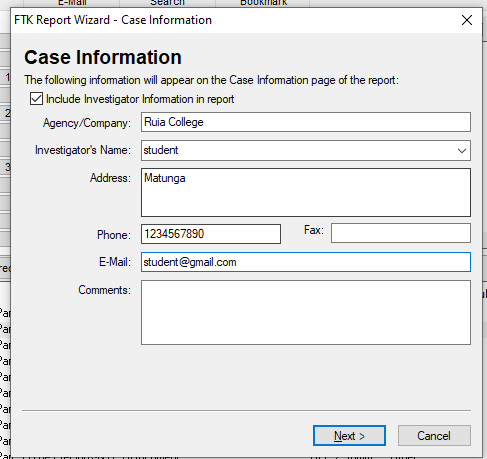




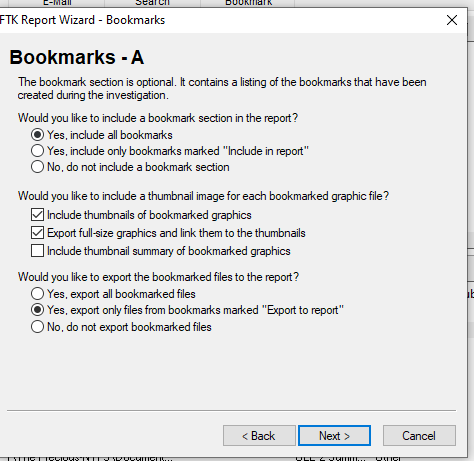
1. Click file > report wizard



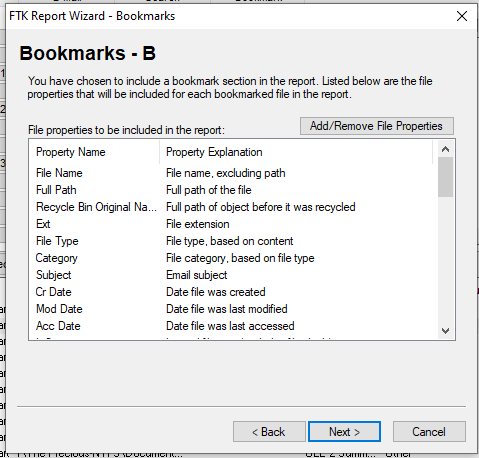
1. Enter the following details



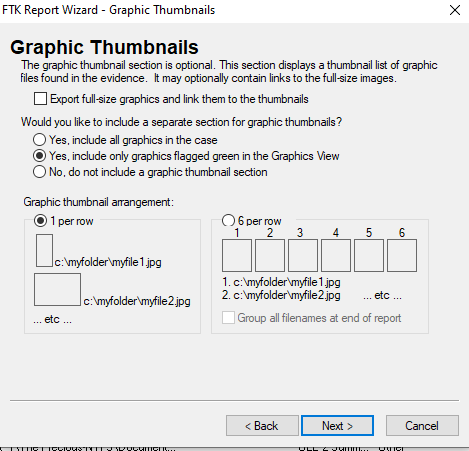
1. Click next



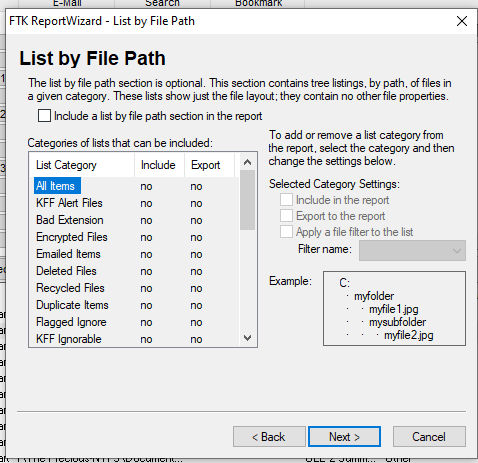
1. Click next



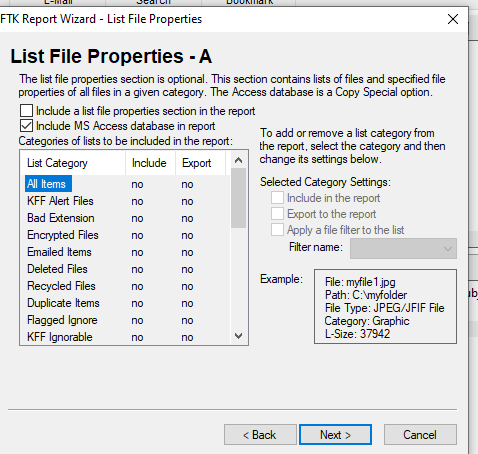
1. Click next



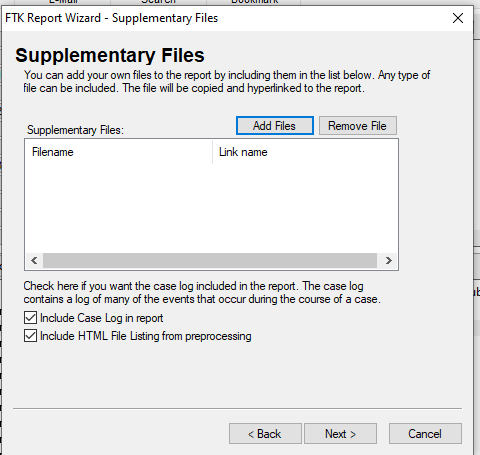
1. Click next



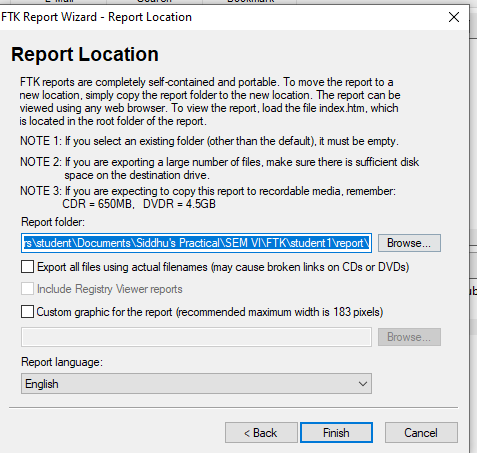
1. Click next



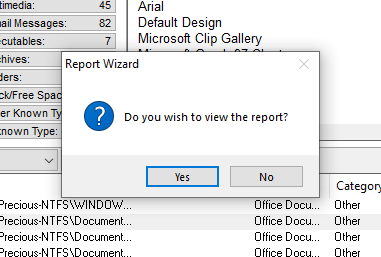
1. Click next



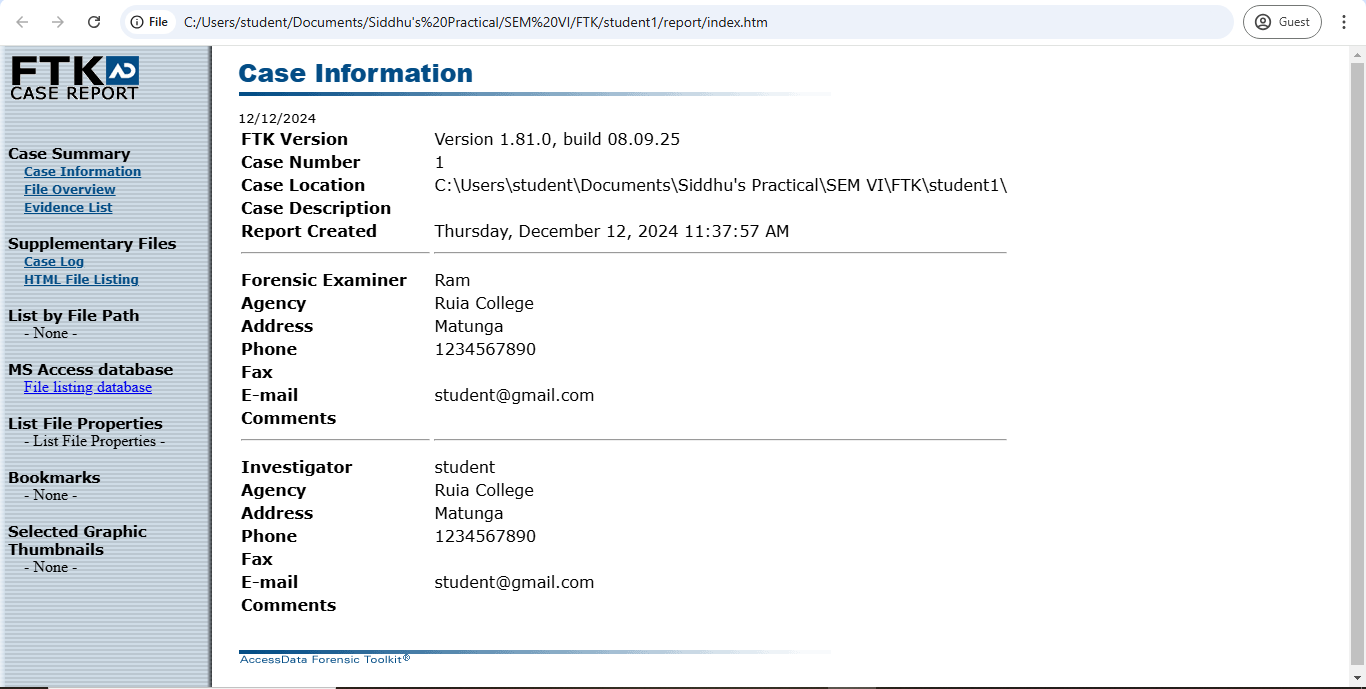
1. Click next



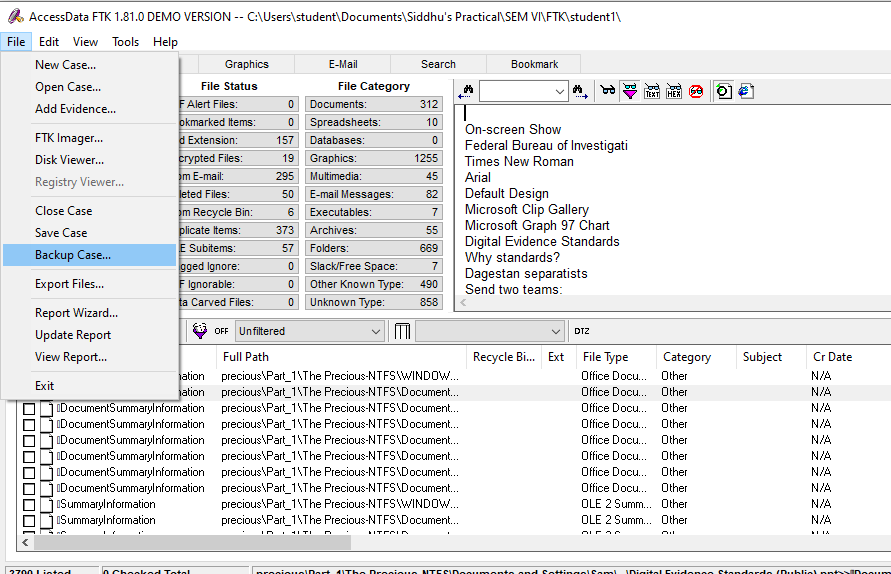
1. Click yes

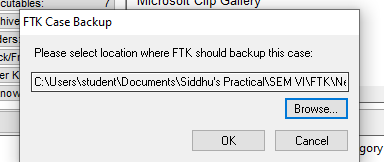


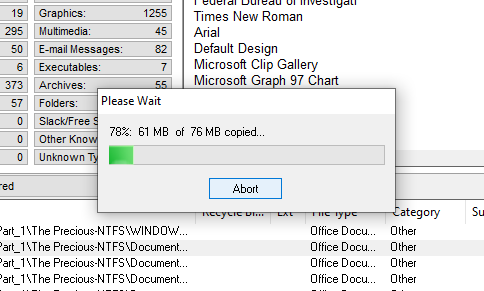
1. View the report

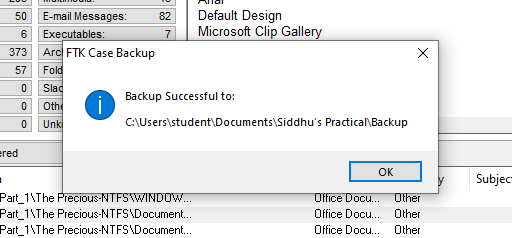


1. Click backup case

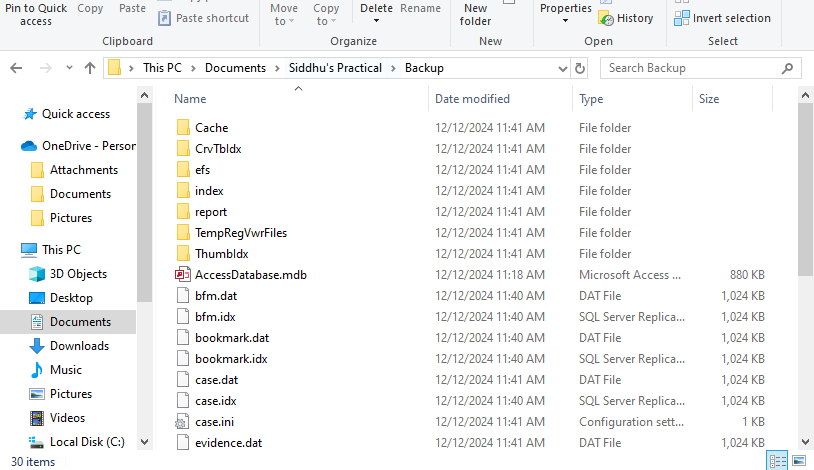




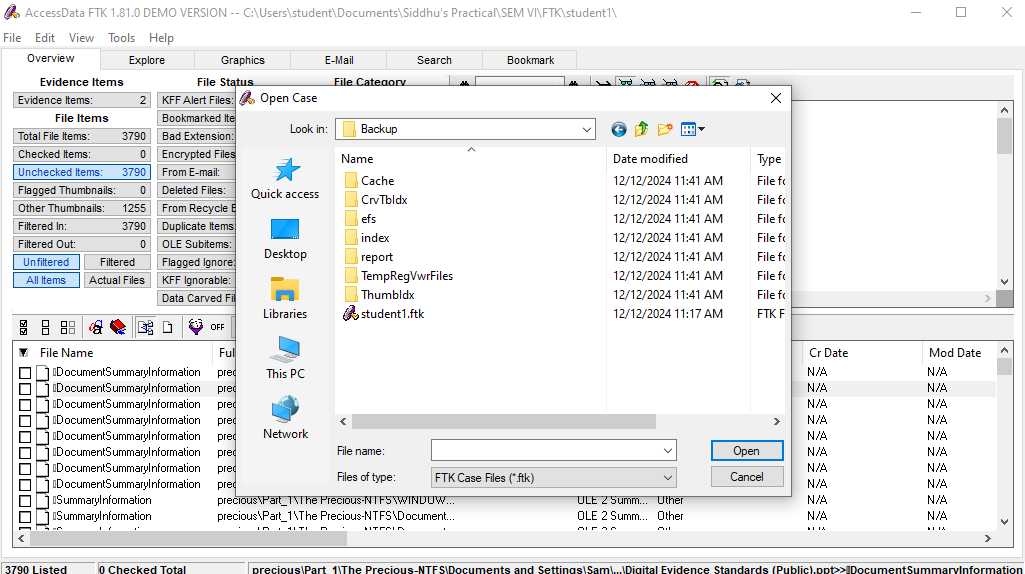




1. Backup Folder



1. Open the backup case again



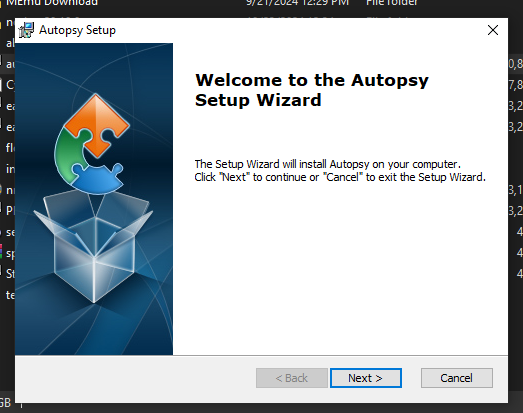
**Q.2] using Autopsy**

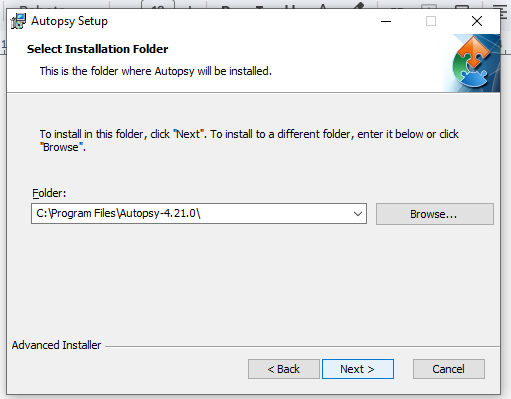
**Aim :** Using **Autopsy** for Case Investigation

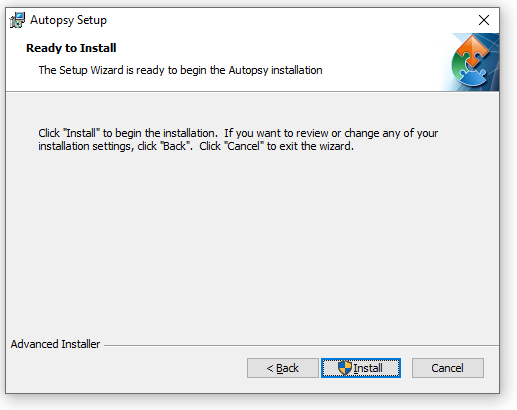
1. **Autopsy tool :**

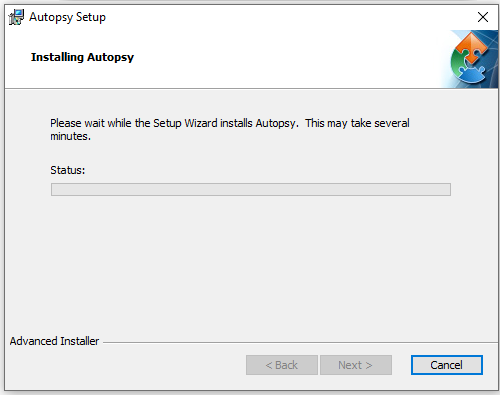
**Step 1:** Download and install Autopsy tool [autopsy-download](https://www.autopsy.com/download/)

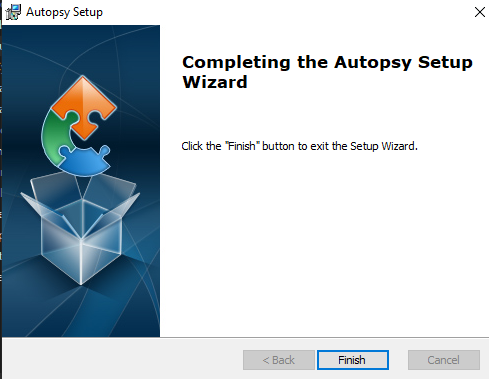




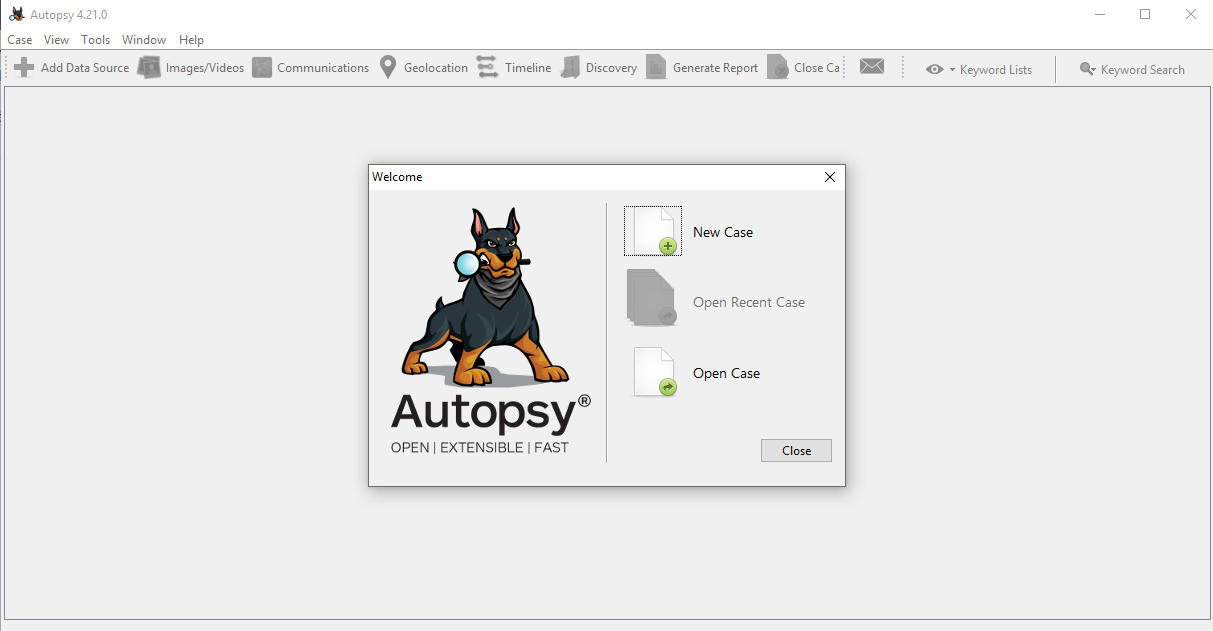






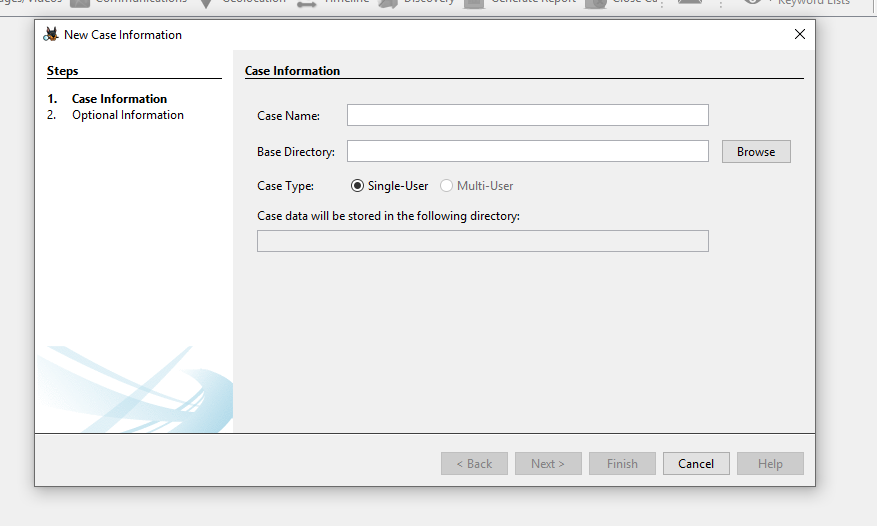


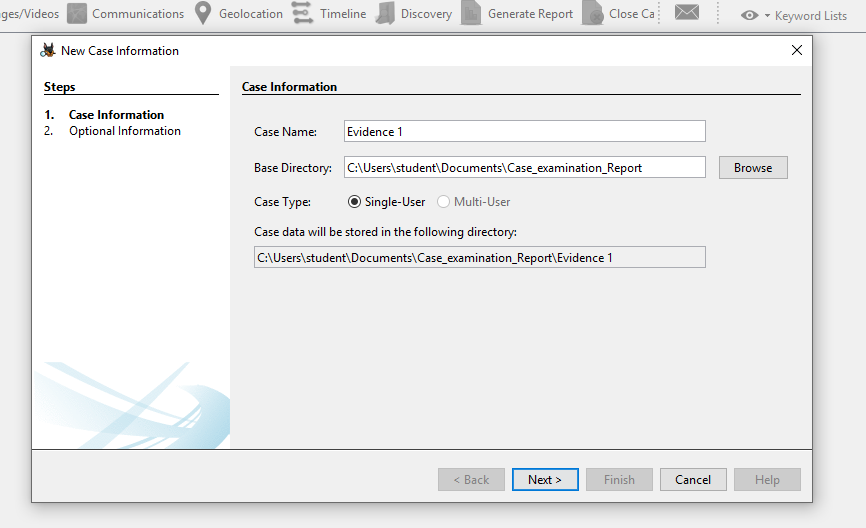
**Autopsy Interface**



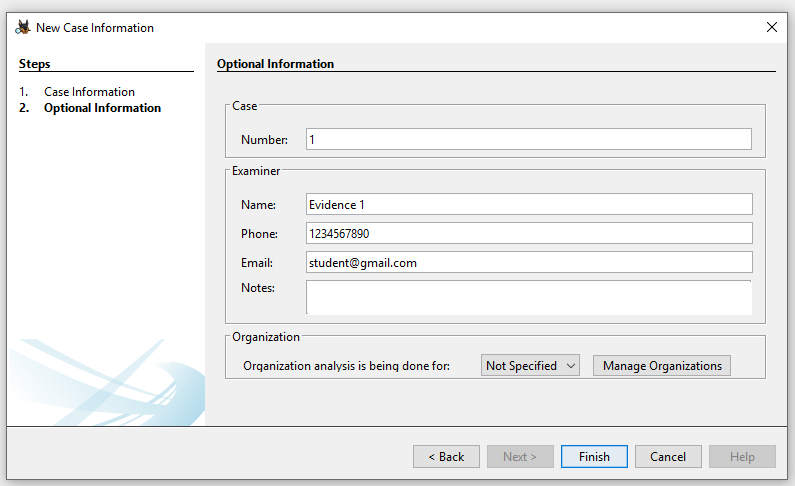
**Step 2 :**  Add new case

Add **Case Name** and **Base directory**

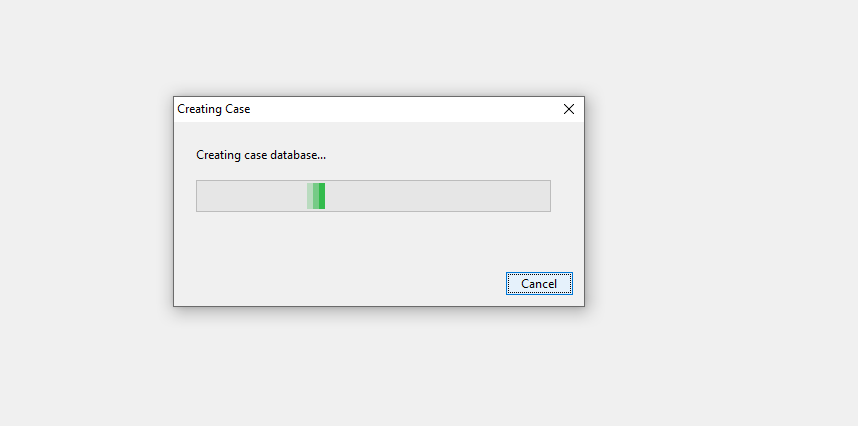




**Step 3:**  Enter Case Information and click on **Finish**

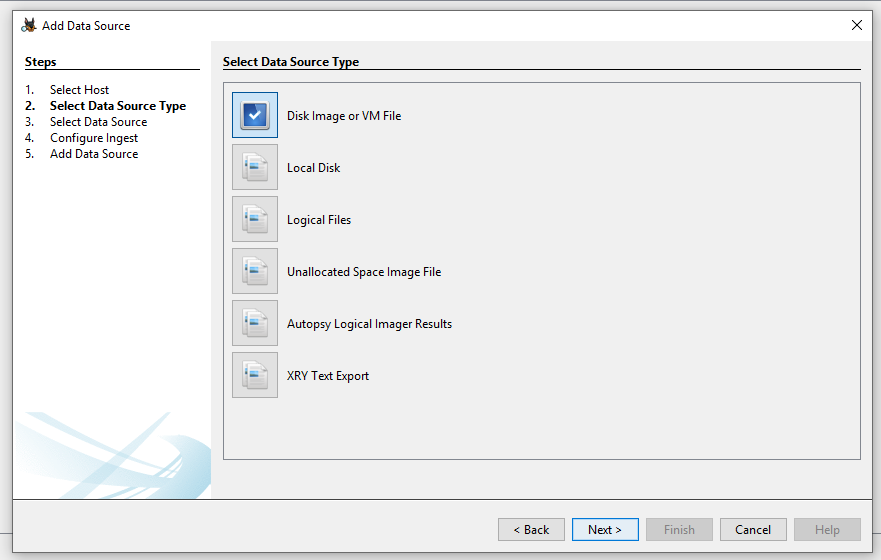


Case Database will be created

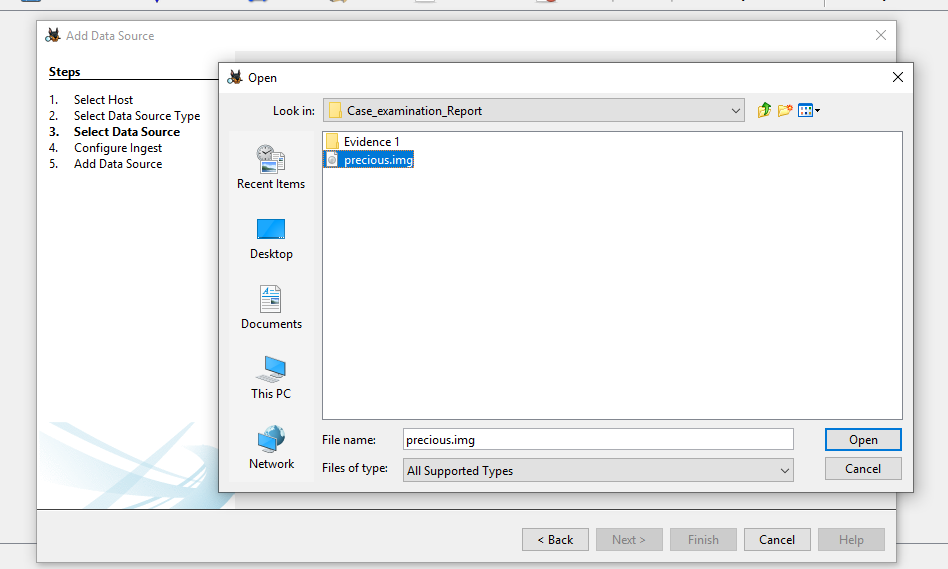


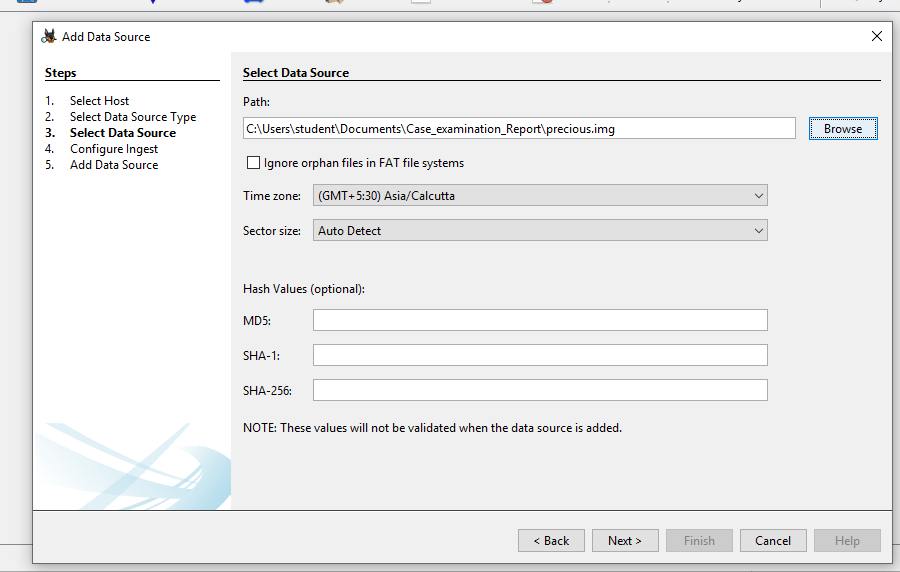
**For Image 1 - precious.img file**

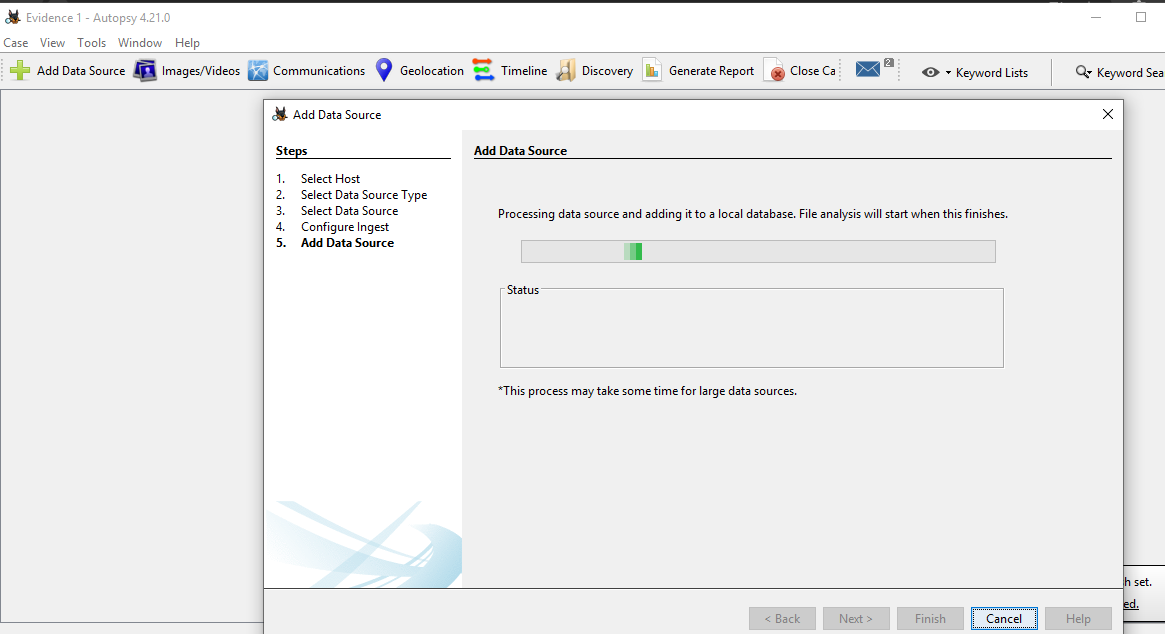
**Step 4** : Select type of data source - **Disk Image** and click on **Next**



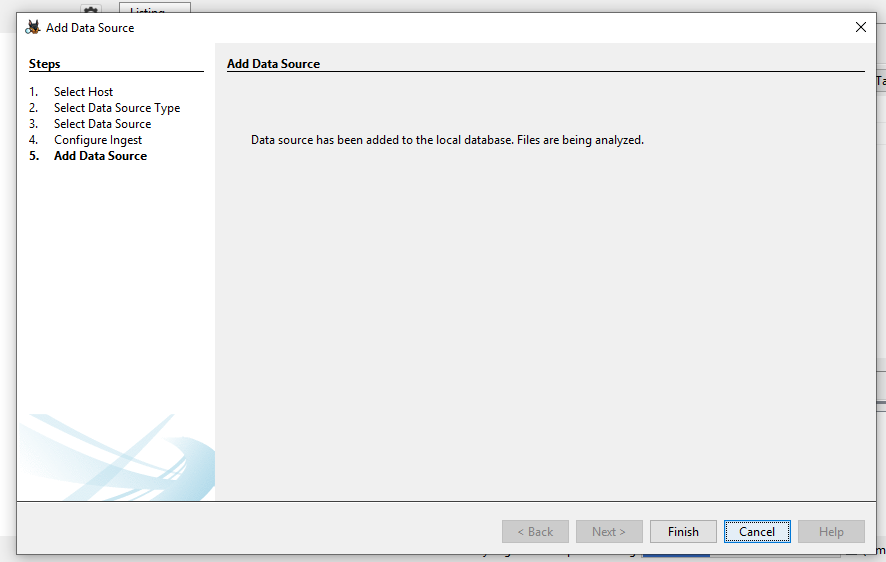
**Step 5 :** Select Data source path ( Give Image’s path) and click on **Next**

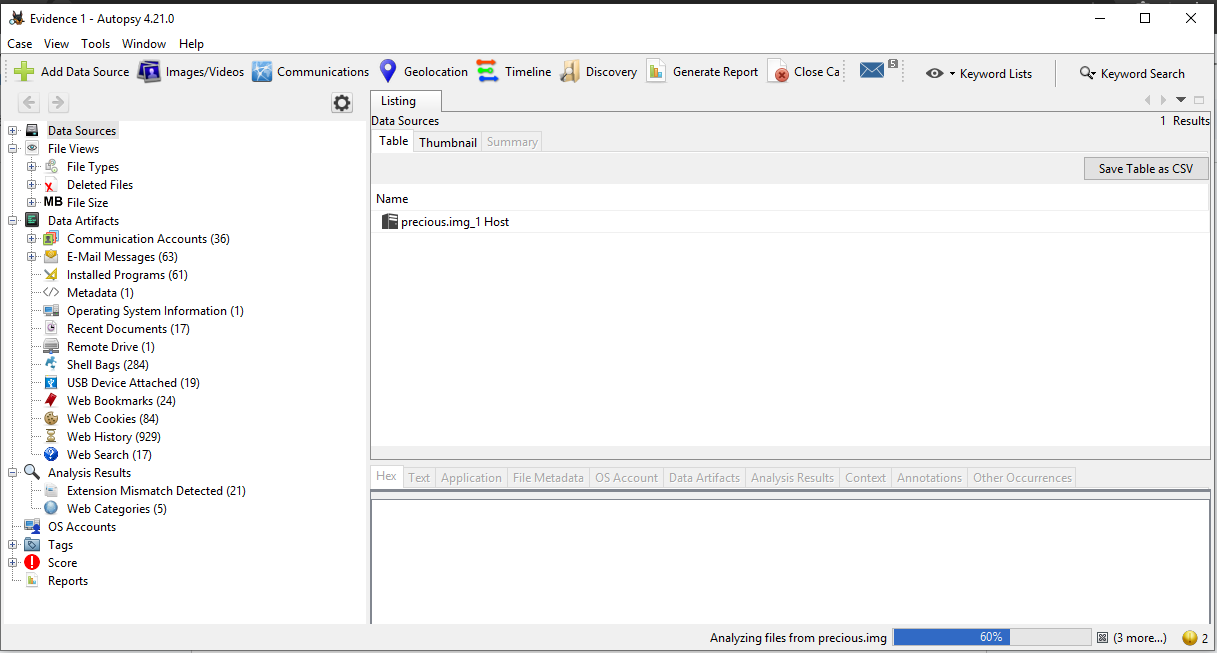






**After Successfully adding the data source below message will be displayed**

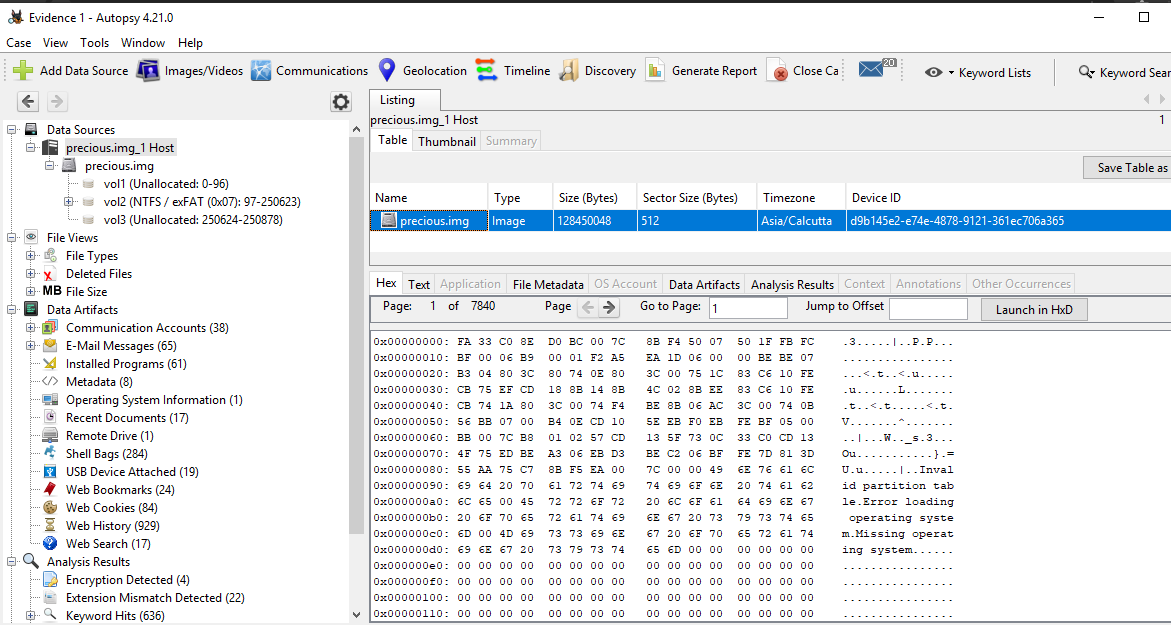




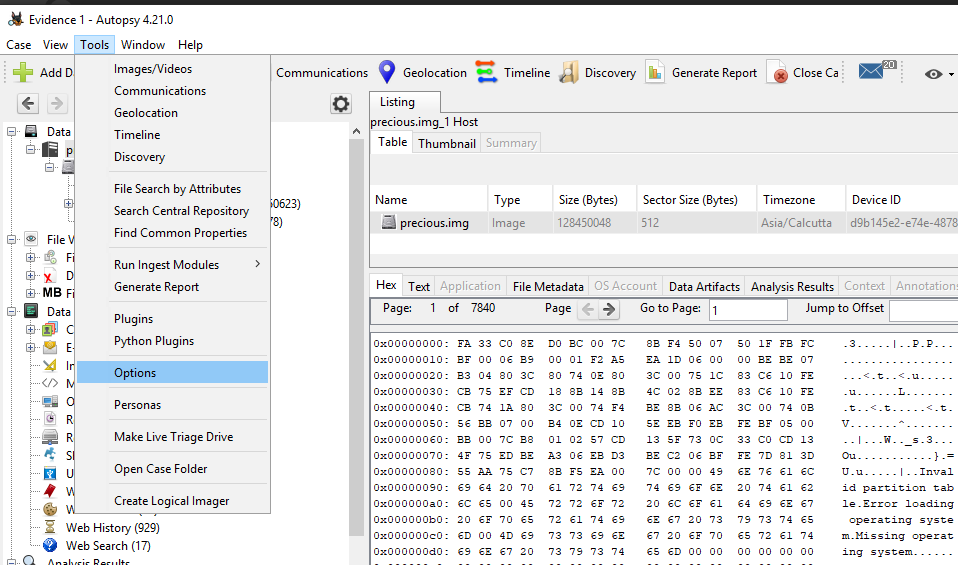
**Tool is analyzing the file**

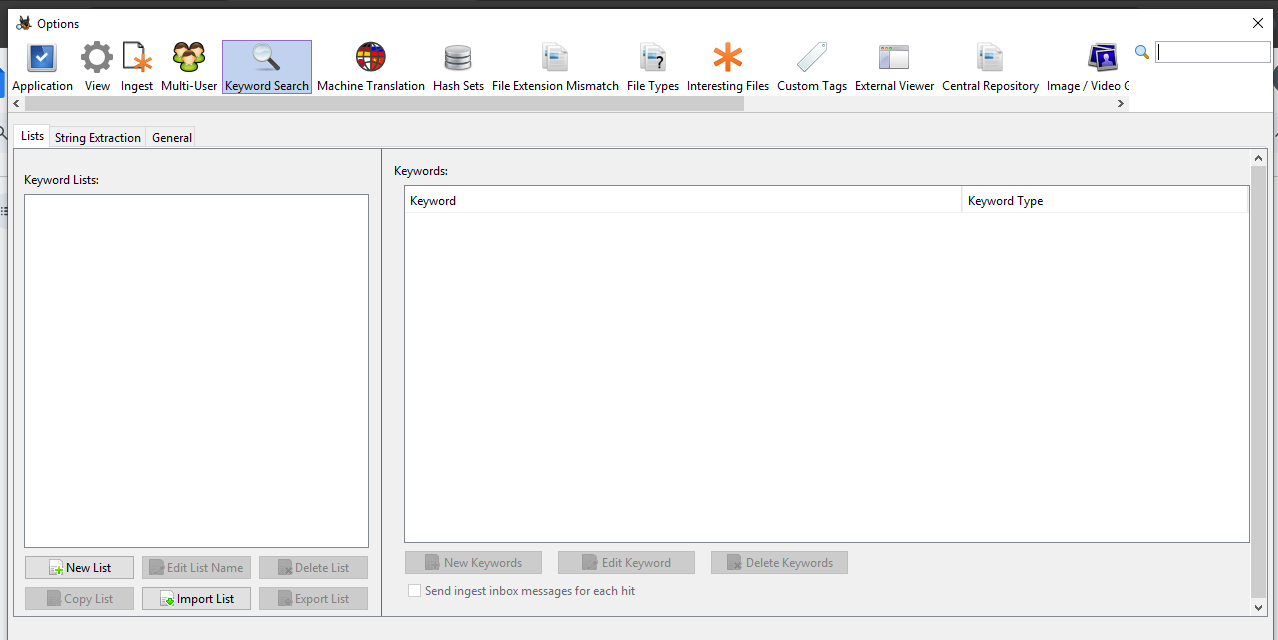


**Step 6:** click on the image to view the hexadecimal content of the file

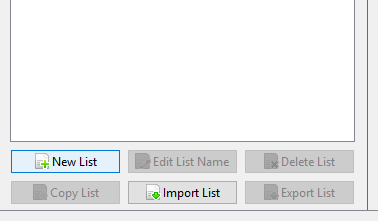


**Step 7 :** To perform keyword search select **Tools** - **options** -**Keyword search**

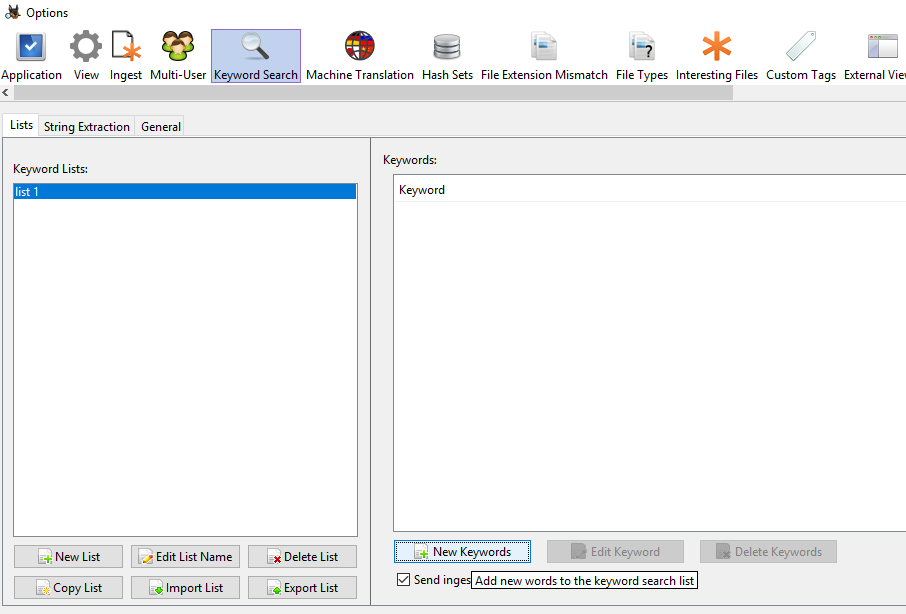




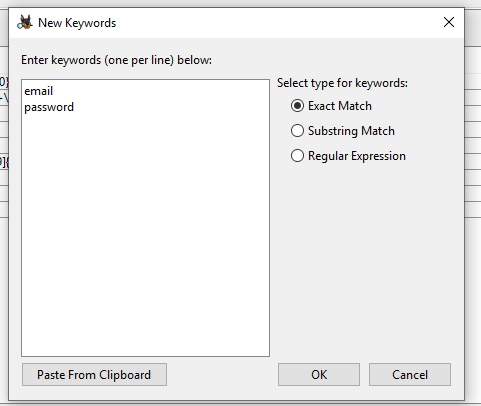
**Step 8 :** Create new Keyword list



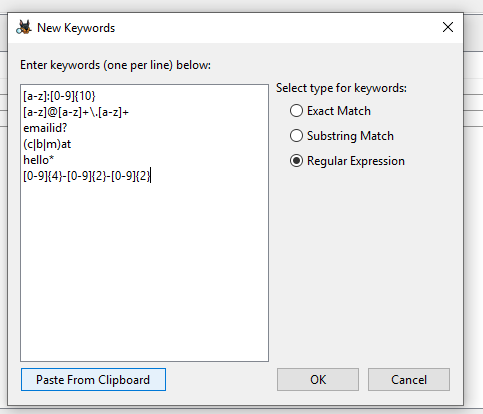
**Step 9 :** Add new keywords



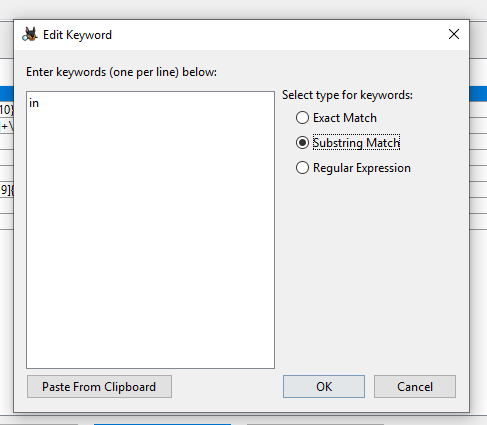
**Step 10 :** select type for keywords - **Exact Match**



select type for keywords - **Regular Expression**

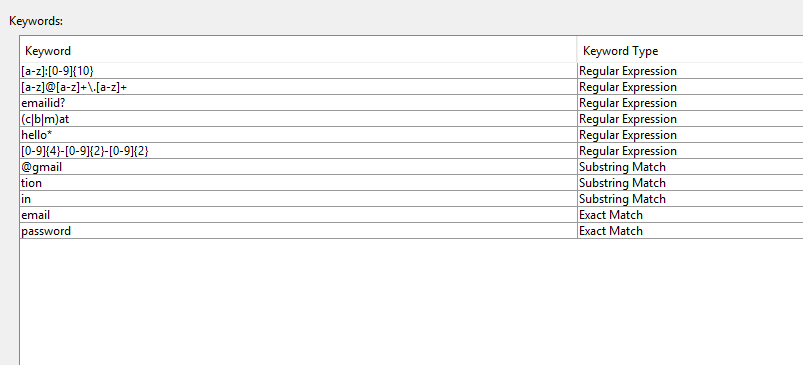


select type for keywords - **Substring match**

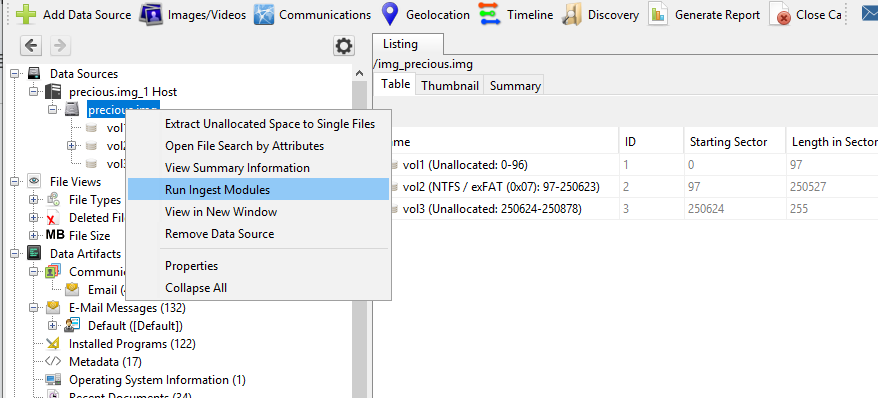


And click on **OK**

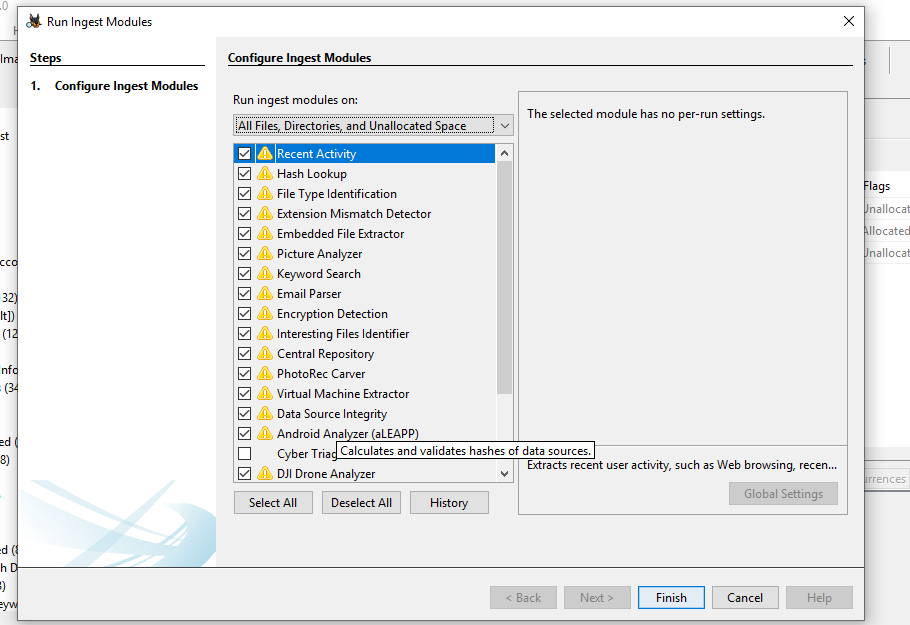
**Keyword list**



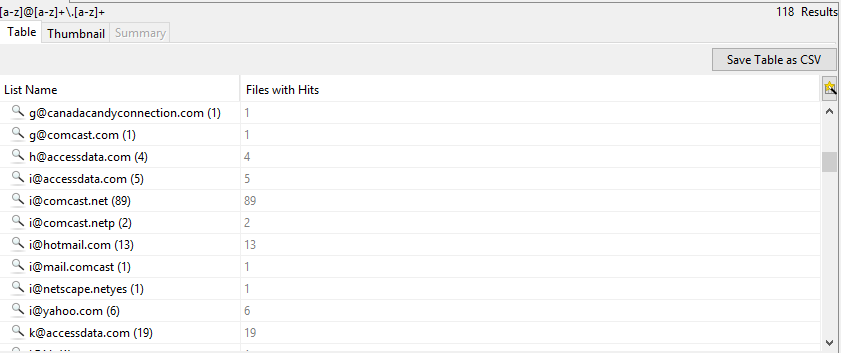
**Step 11 :** Right click on precious.img and select **Run Ingest Modules**

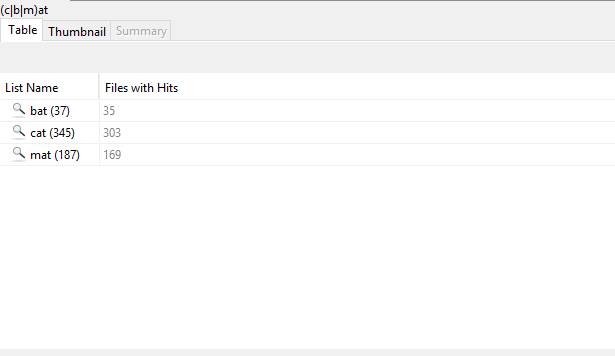


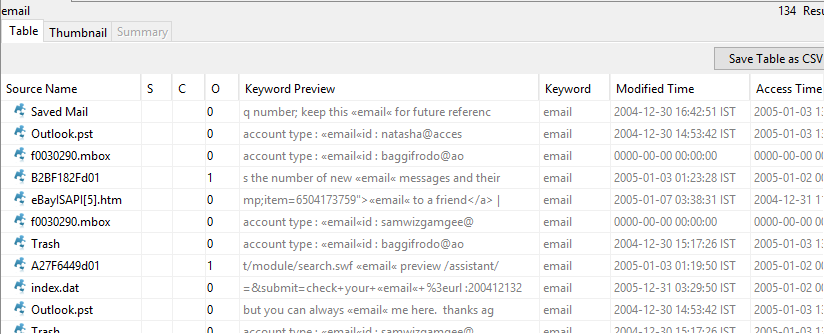
Check if **keyword search** is selected and **click on Finish**

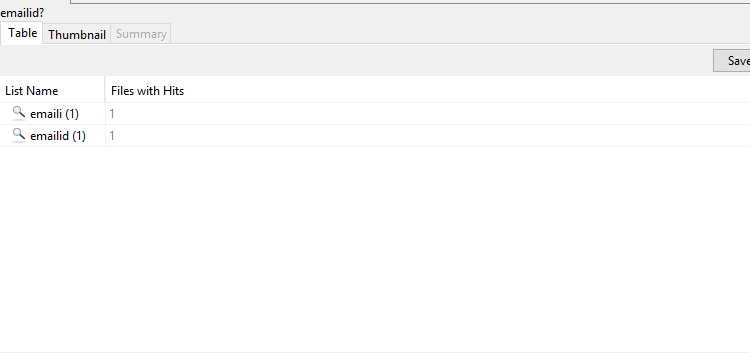


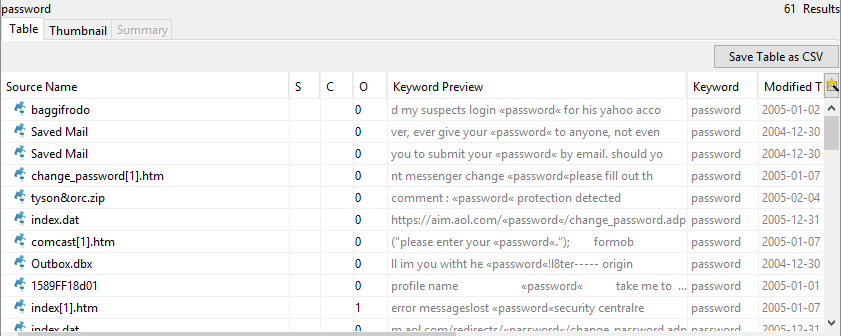
**Step 12 :** To test Keywords select **Analysis Result** - **keyword Hits** - **list 1** (Keyword list name )

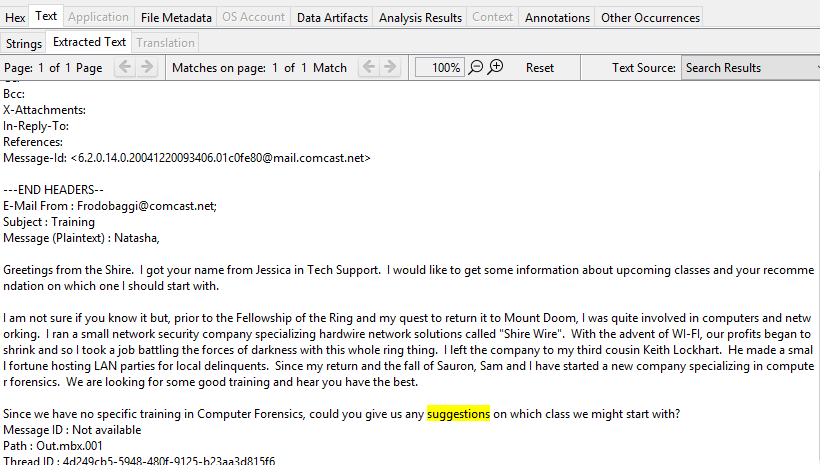


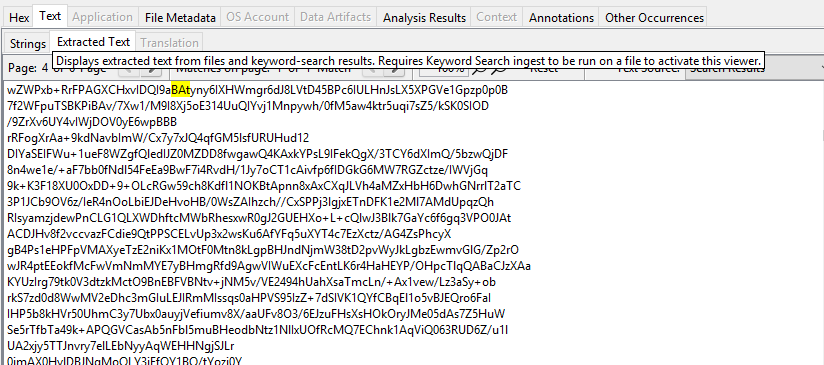


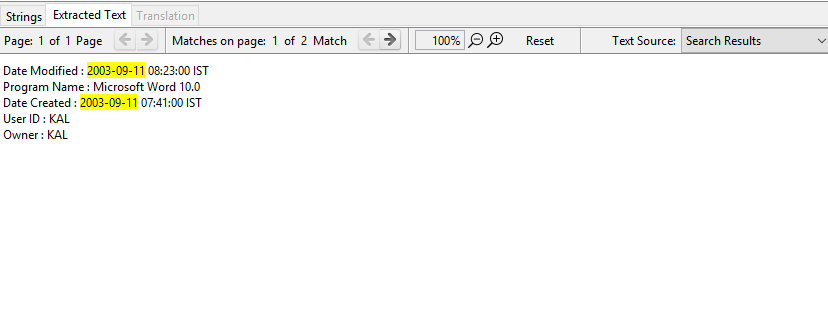




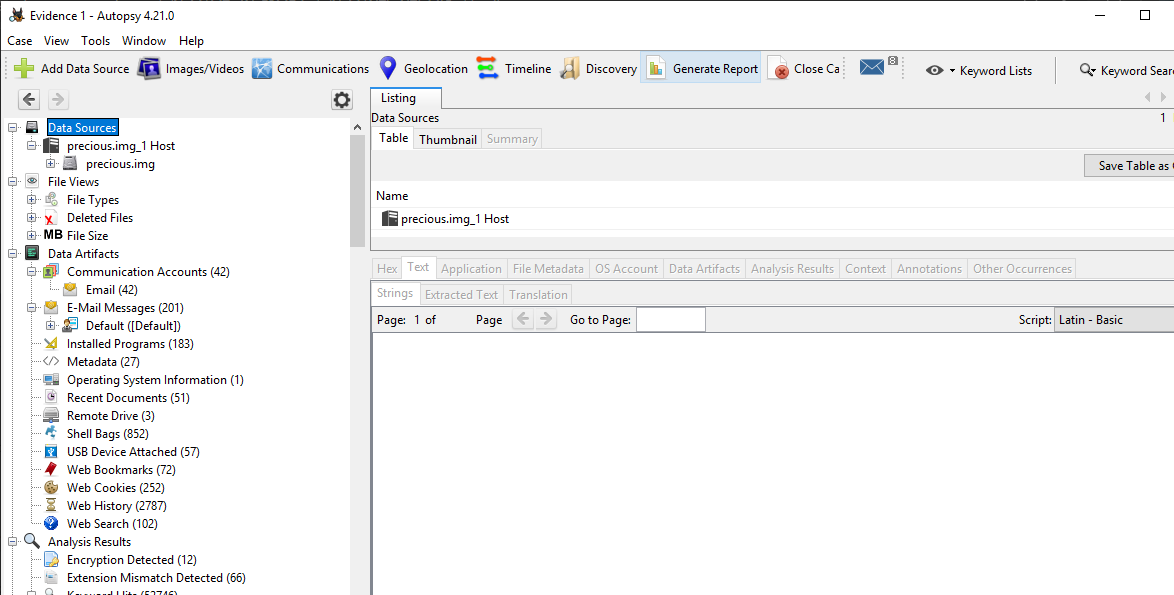


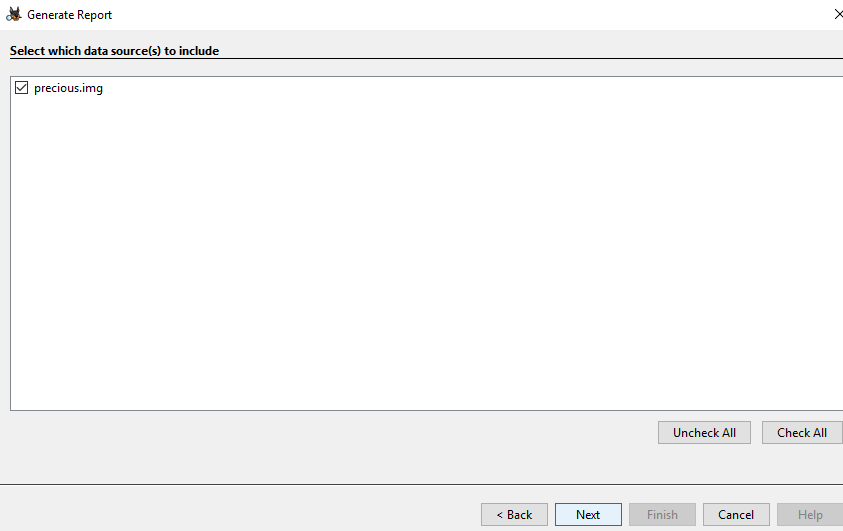


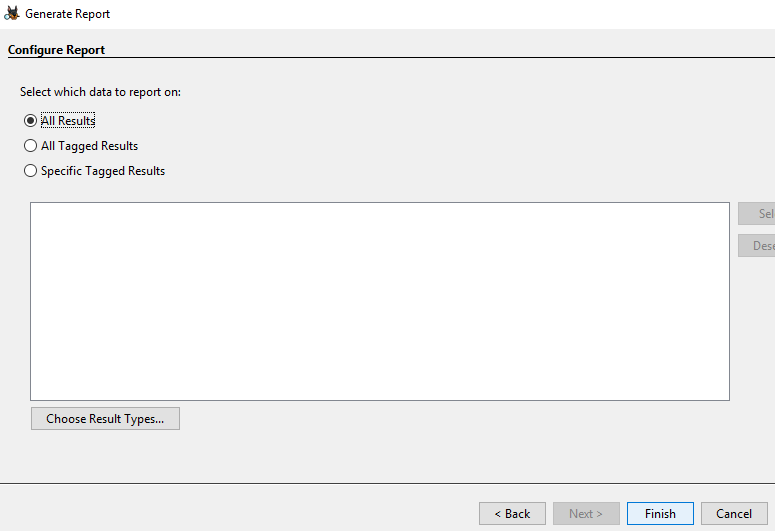


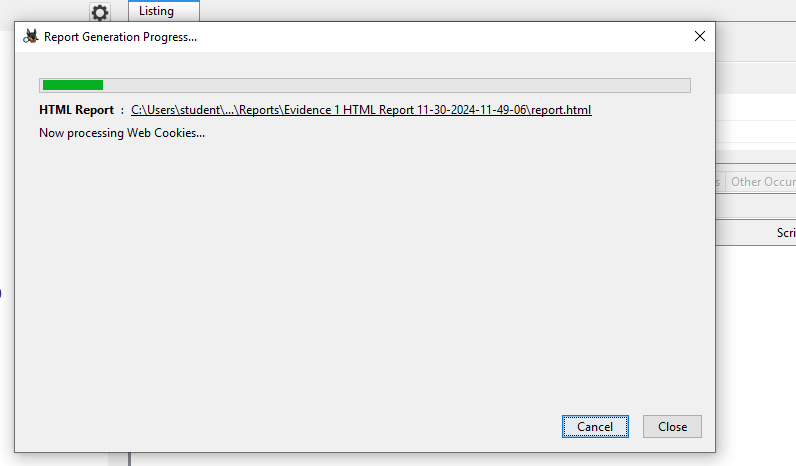


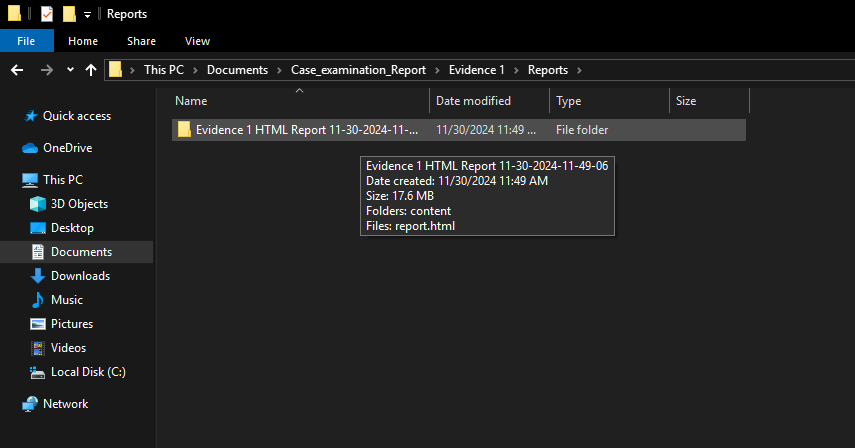
**Step 12 :** Generate a report of the Examination

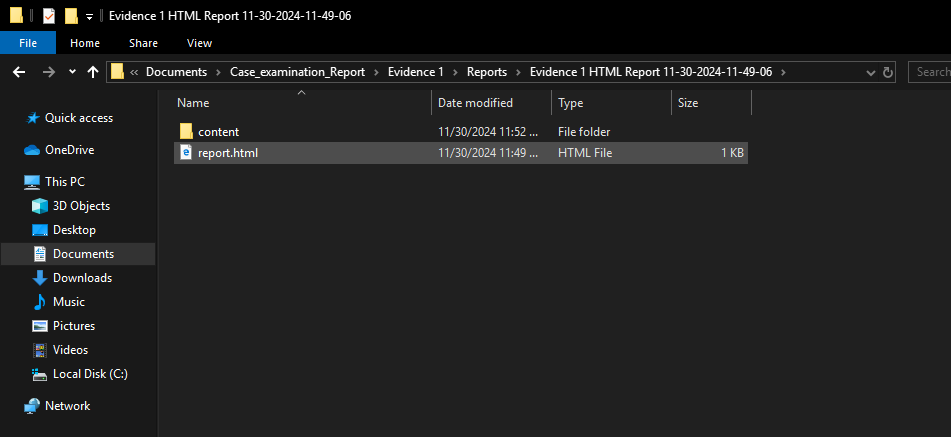




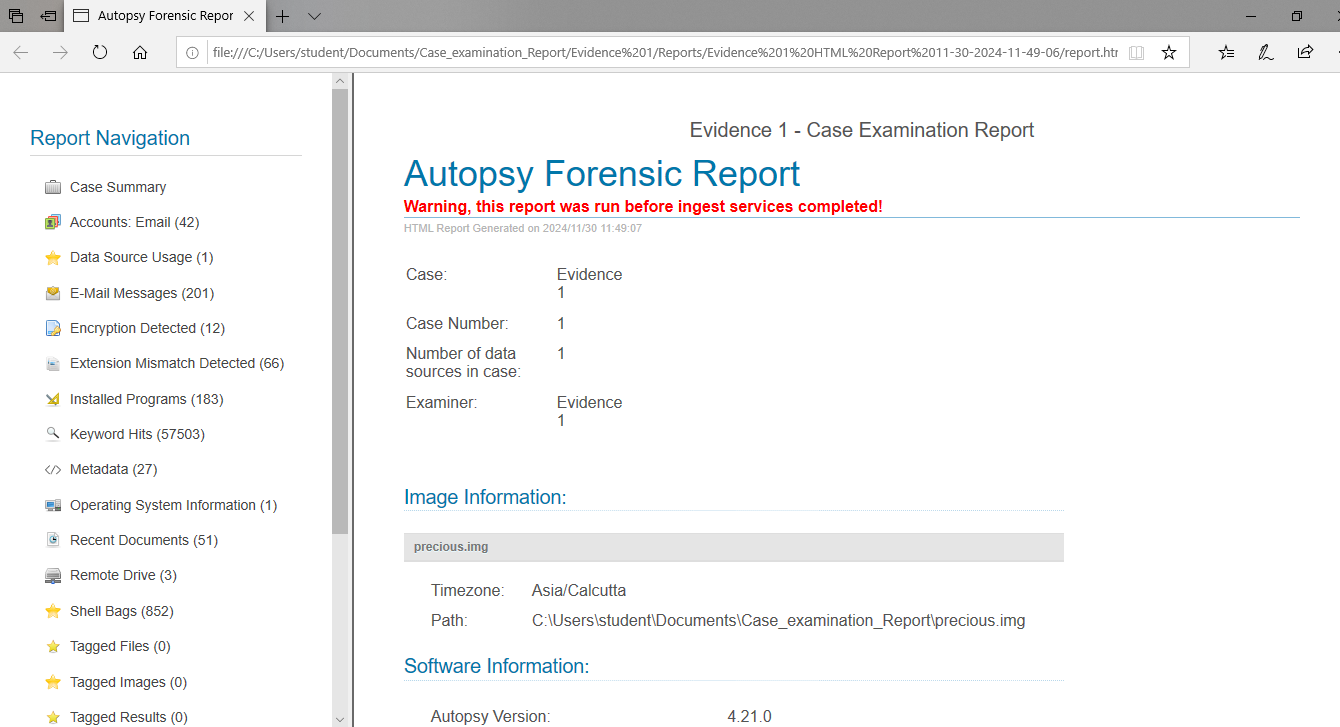


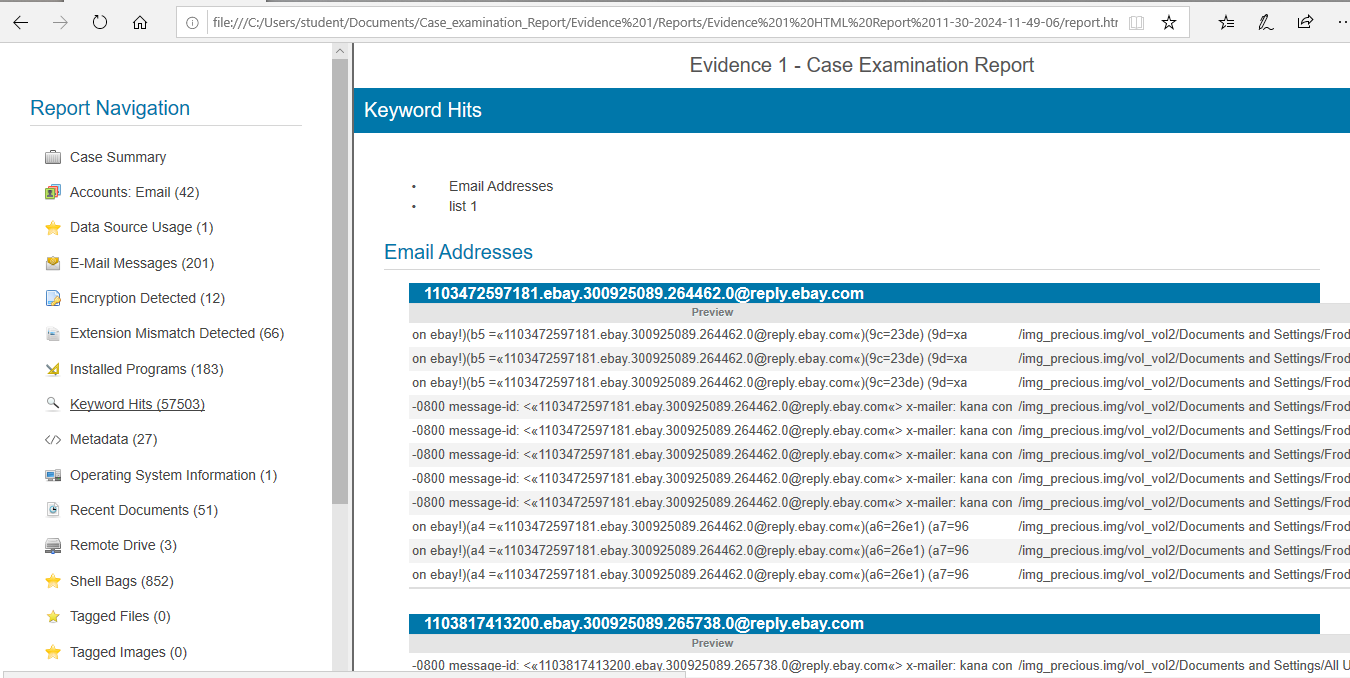






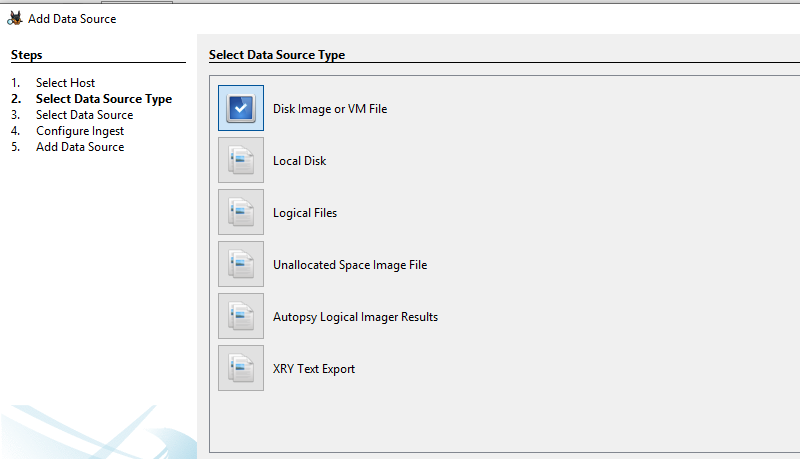
Step 13: Open Report File



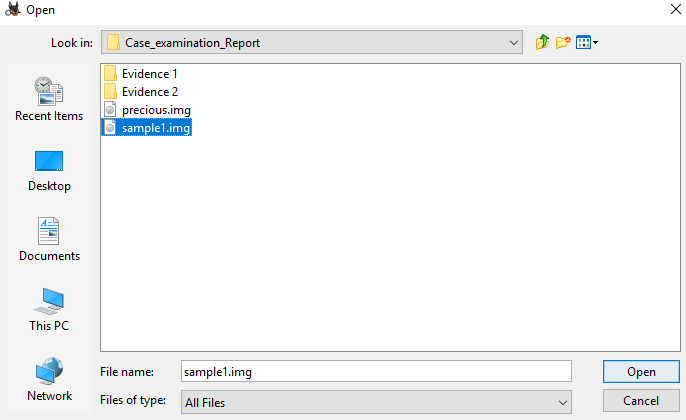


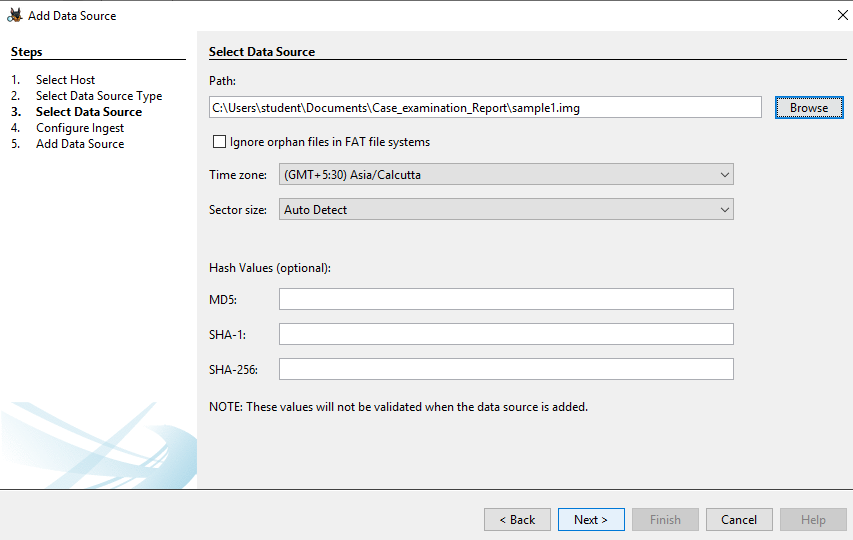
**For Image 2 - sample1.img file**

**Step 1 : Select type of data source - Disk Image and click on Next**

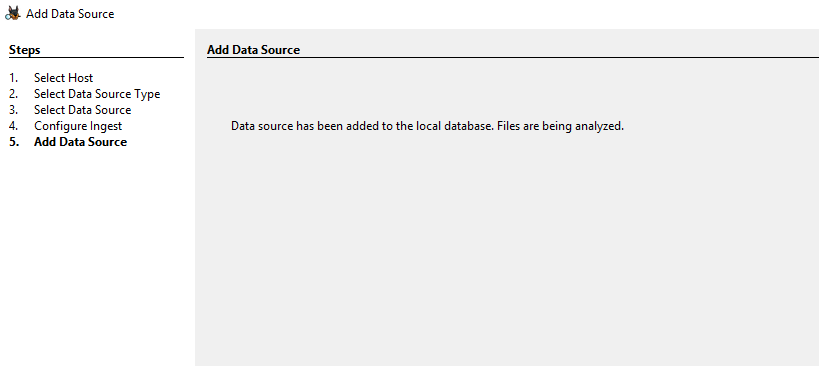


**Step 2 : Select Data source path ( Give Image’s path) and click on Next**



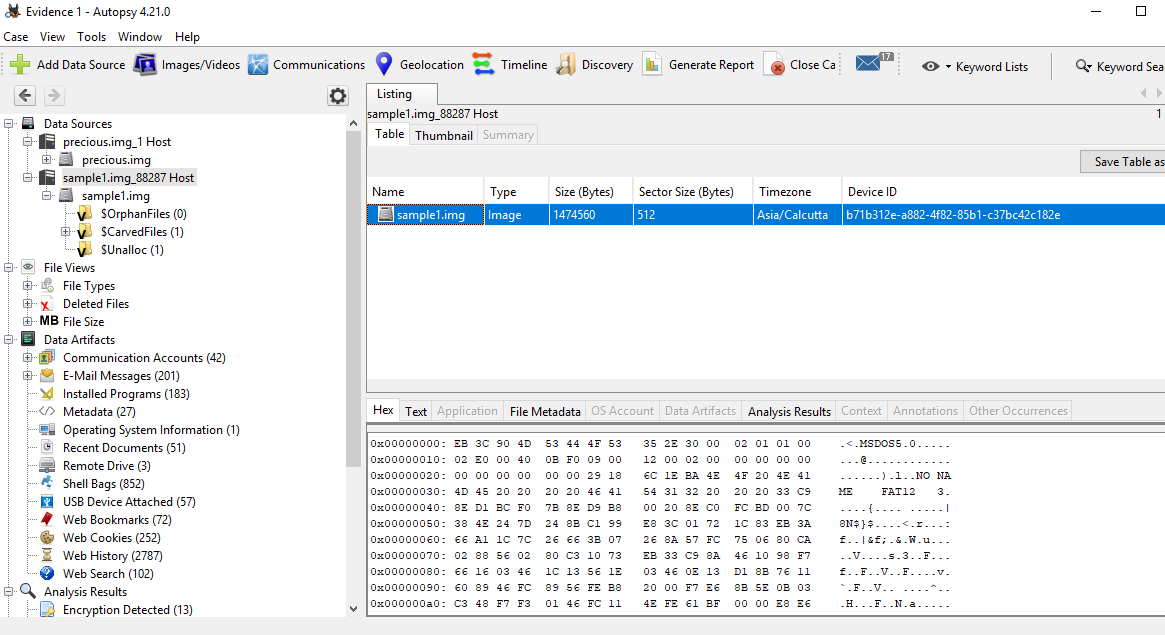


**After Successfully adding the data source below message will be displayed**

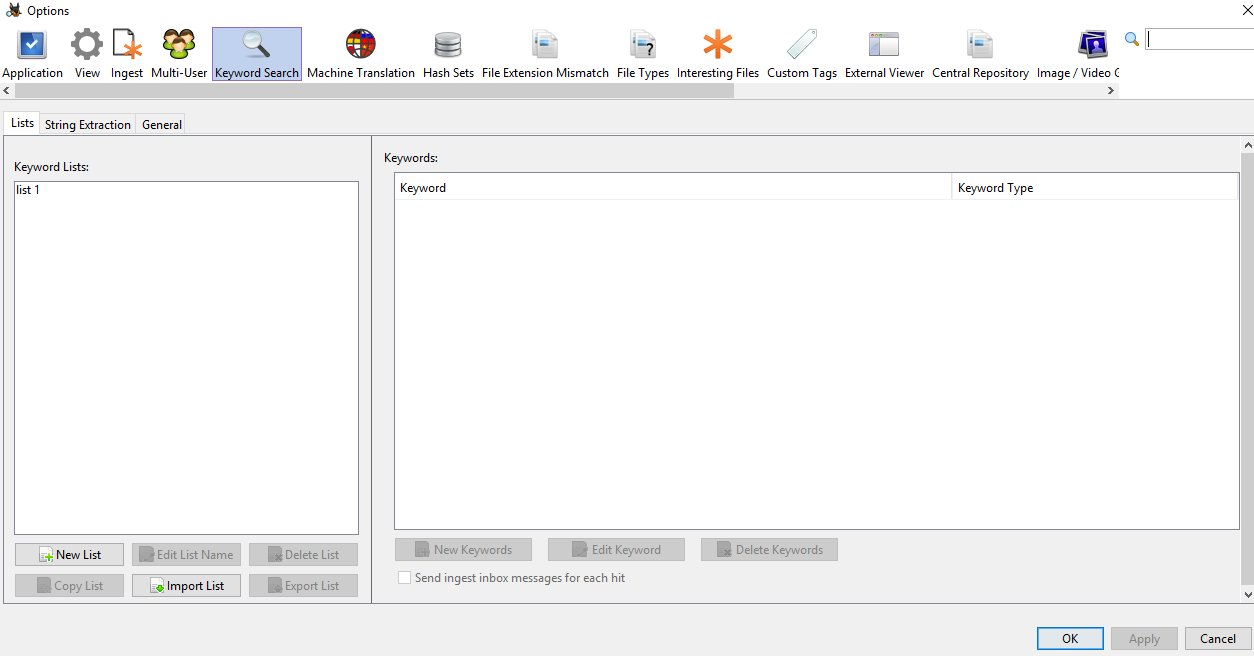


**Tool is analyzing the file**

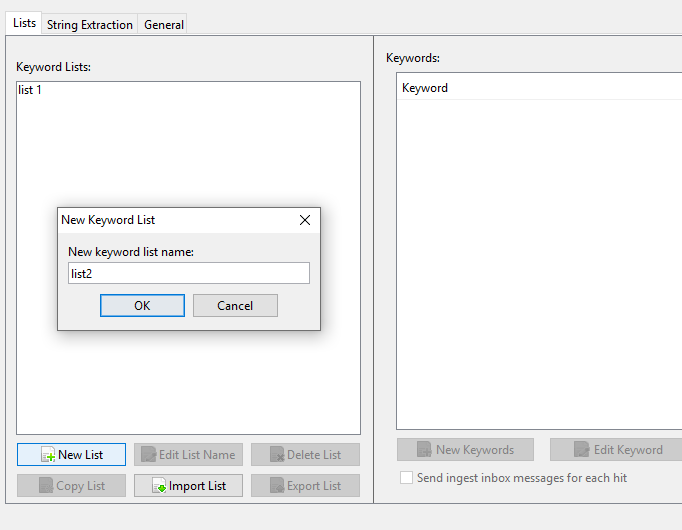
**Step 3: click on the image to view the hexadecimal content of the file**



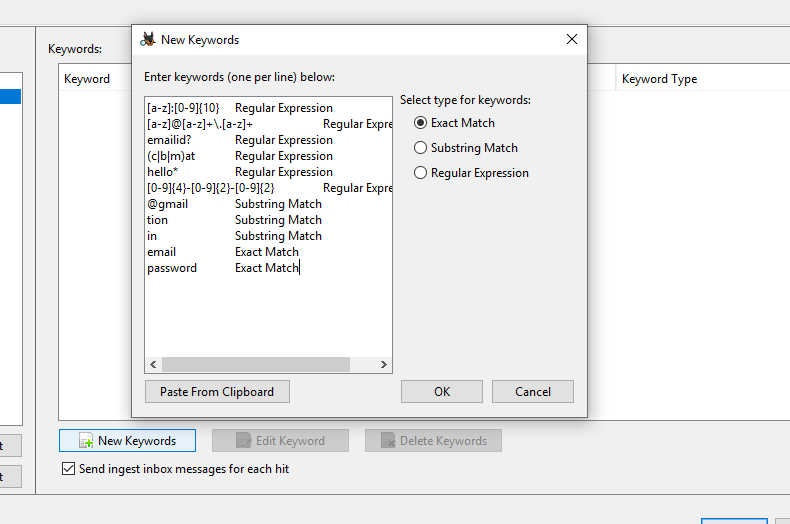
**Step 4 : To perform keyword search select Tools - options -Keyword search**



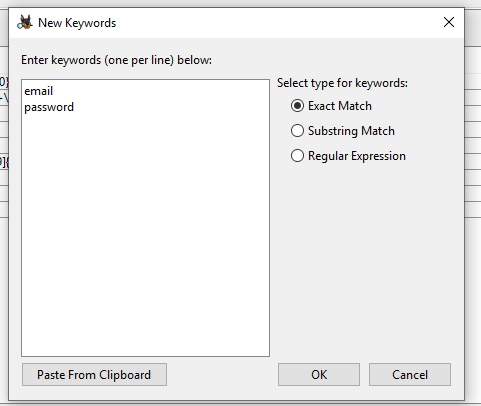
**Step 5 : Create new Keyword list**



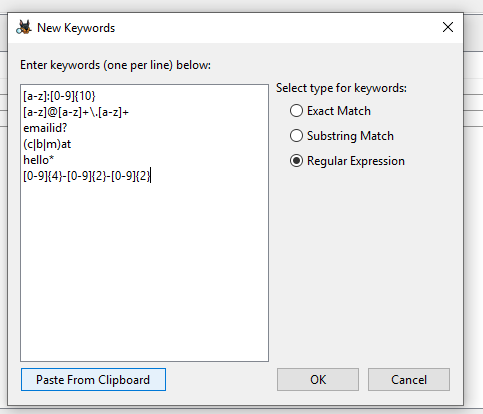
**Step 6 : Add new keywords**



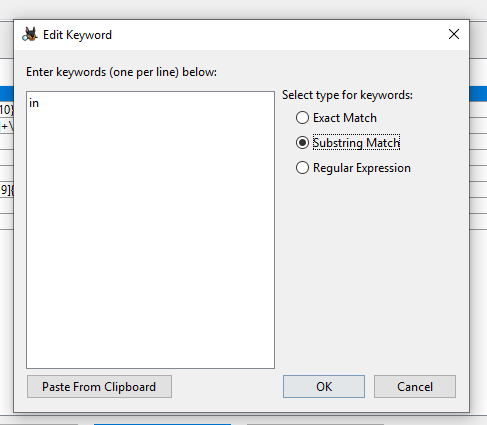
**Step 7 : select type for keywords - Exact Match**



**select type for keywords - Regular Expression**

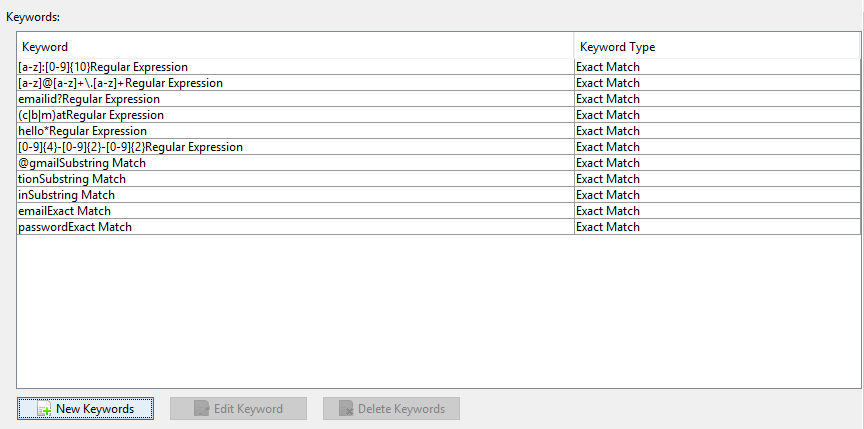


**select type for keywords - Substring match**

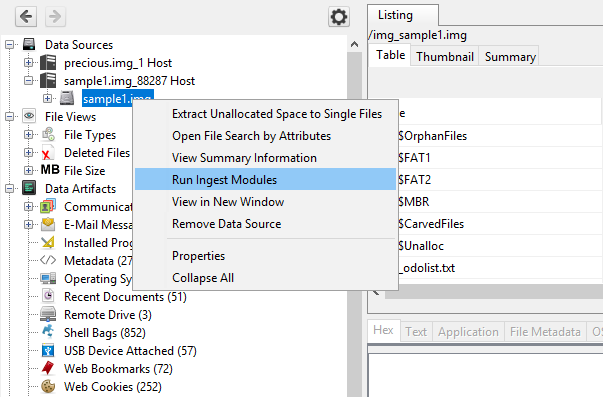


**And click on OK**

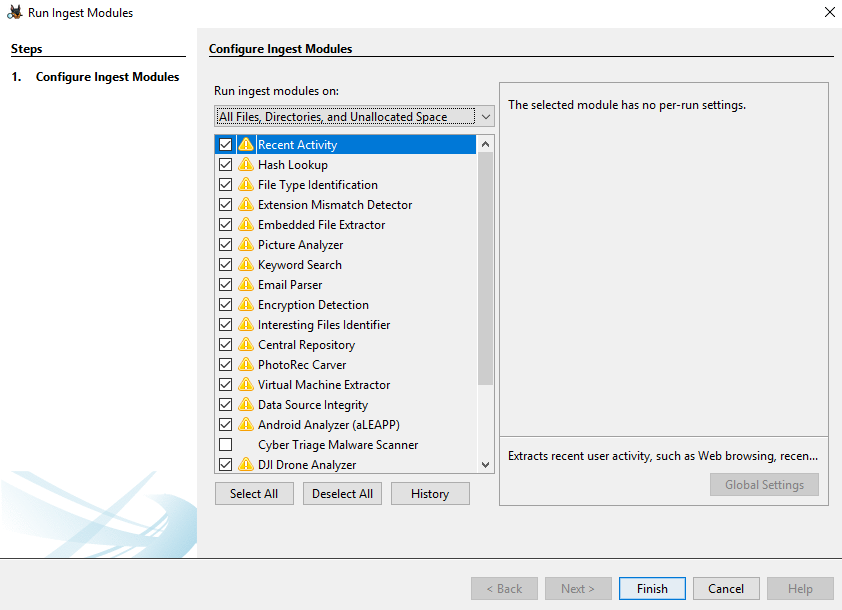
**Keyword list**



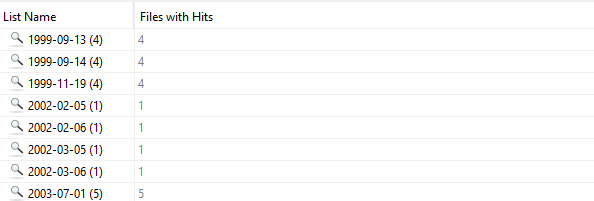
**Step 8 : Right click on sample1.img and select Run Ingest Modules**

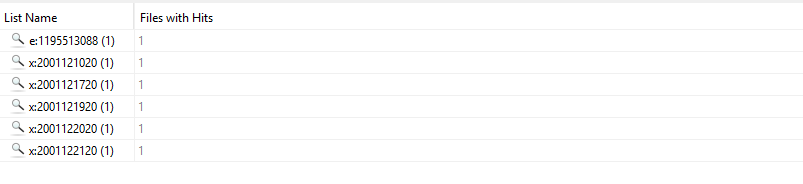


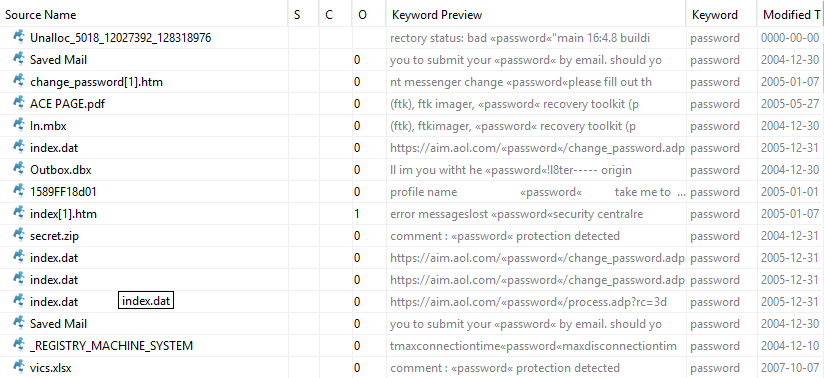
**Check if keyword search is selected and click on Finish**

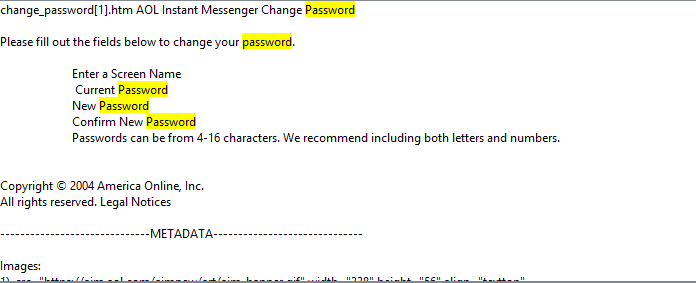


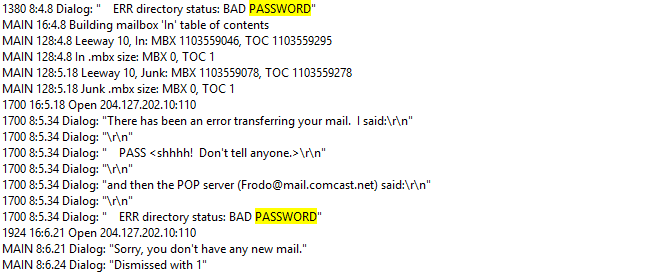
**Step 9 : To test Keywords select Analysis Result - keyword Hits - list 2 (Keyword list name )**

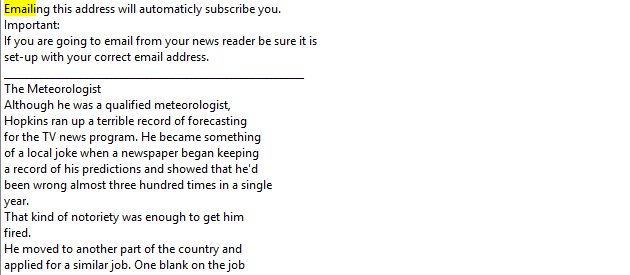




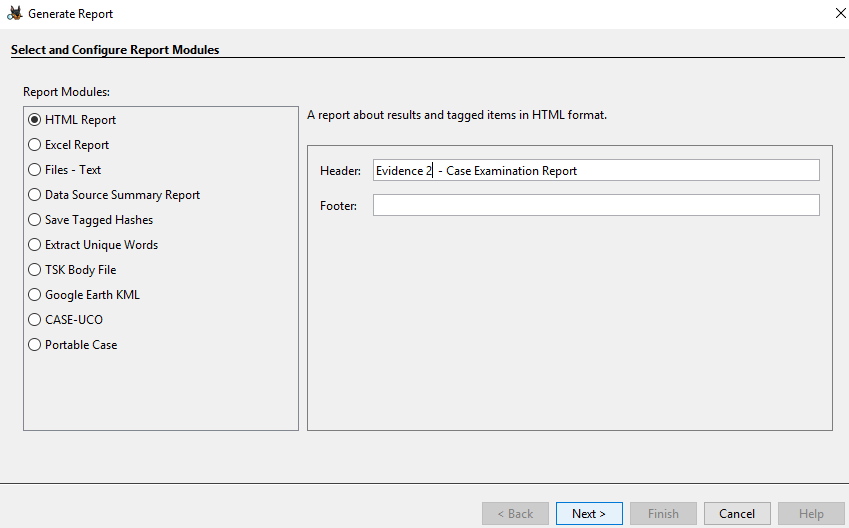


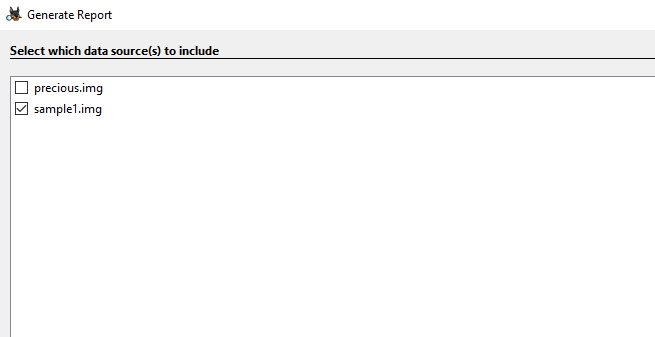


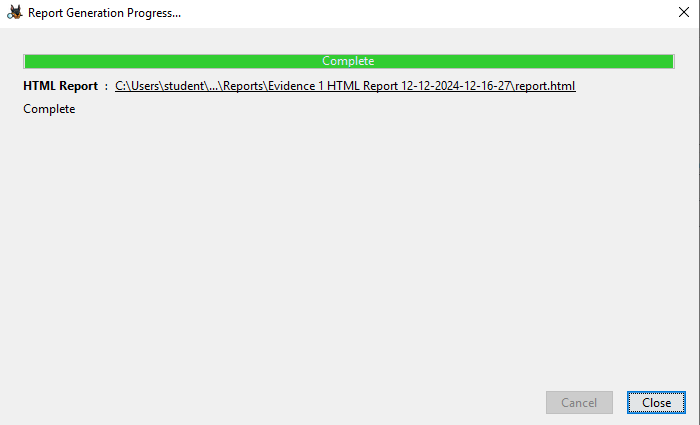




**Step 10 : Generate a report of the Examination**







**Step 11: Open Report File**

