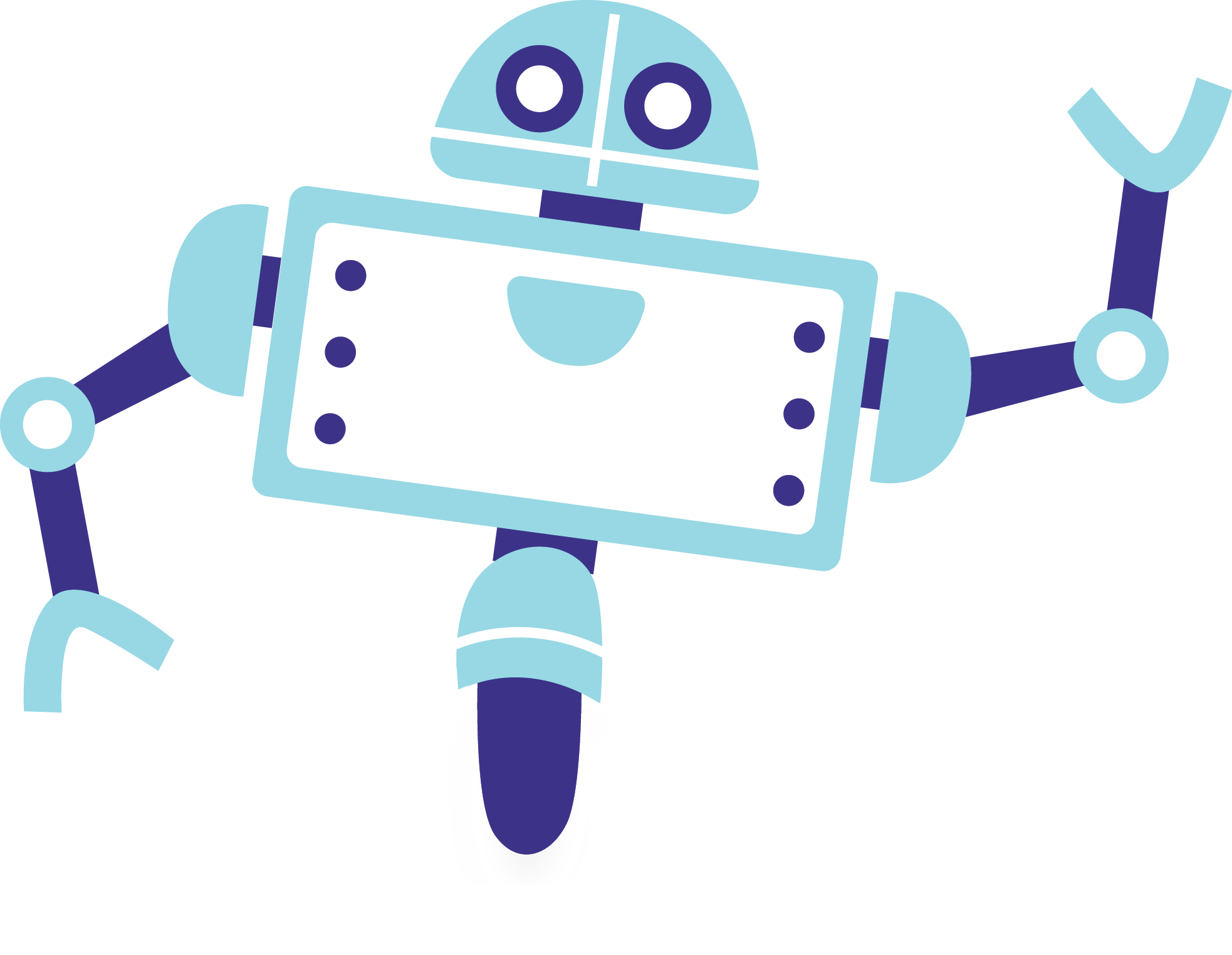
**VIRTUAL TOOLKIT: MISSION 0**

**STEP-BY-STEP**

To View Virtual Toolkit and Cyber Sleuth Lab at the same time MINIMIZE the toolkit window.

**GOTO Window → Exit Full Screen**

****

**FIND THE ANSWERS**

Document your answers in your **Lab Notebook.**

Were you able to recover a deleted photo? Why?

* I was able to recover the photo because…

What information were you able to uncover about the photo recovered in **Autopsy**?

* How many photos did you recover?
* When were the photos most likely taken?
* What specific device was used to take the photos?

What additional information did you learn about the photos by looking at the EXIF metadata in **JPEGsnoop**? Is location information indicating where the photo was taken in the EXIF metadata?

**Be sure to list:** the date you conducted the investigation; the step-by-step process involved in recovering the data; and the digital forensic tools and versions used to recover the photo and examine the EXIF metadata.

**Copy into your Lab Notebook:** (1) the Image Log located in the Mission 0 folder on the Toolkit’s desktop and (2) the EXIF metadata in JPEGsnoop from the photo you recovered.

**TIP:** Copy and paste the SDCard log and also the EXIF metadata from a recovered photo into the notebook.

**BEFORE YOU BEGIN**

**EXAMINE & COPY THE IMAGE LOG INTO THE LAB NOTEBOOK**

The **Image Log** is documentation generated when the **Forensic Copy** of the data was created.

1. Open **SDCard\_ImageLog.txt** found in ***Desktop* → *Mission 0* → *SDCard***
2. Take a look at the types of information found in the **Image Log**
3. Copy the **Image Log** text to your **Lab Notebook**:

1. *Edit* → *Select All or [CNTRL]-[a] / [CMND]-[a]*

2. *Edit* → *Copy or [CNTRL]-[c] / [CMND]-[c]*

3. In the Lab Notebook, click on **[ADD NEW DATA]** button at the bottom of the window

4. Type **Image Log** in the *Title* Field

5. Right-Click in the *Data* area and select Paste *or [CNTRL]-[v] / [CMND]-[p]*

6. Click **[SAVE]**

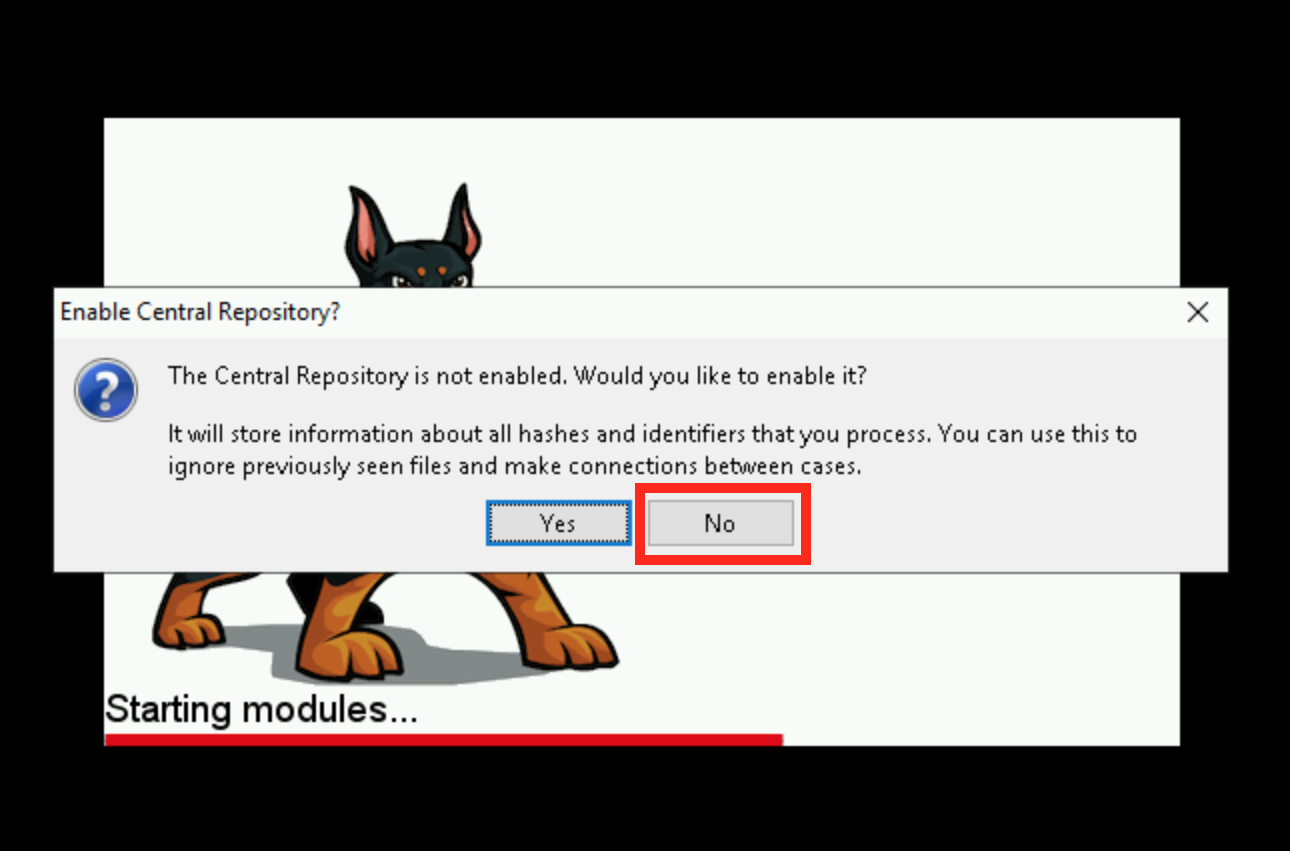


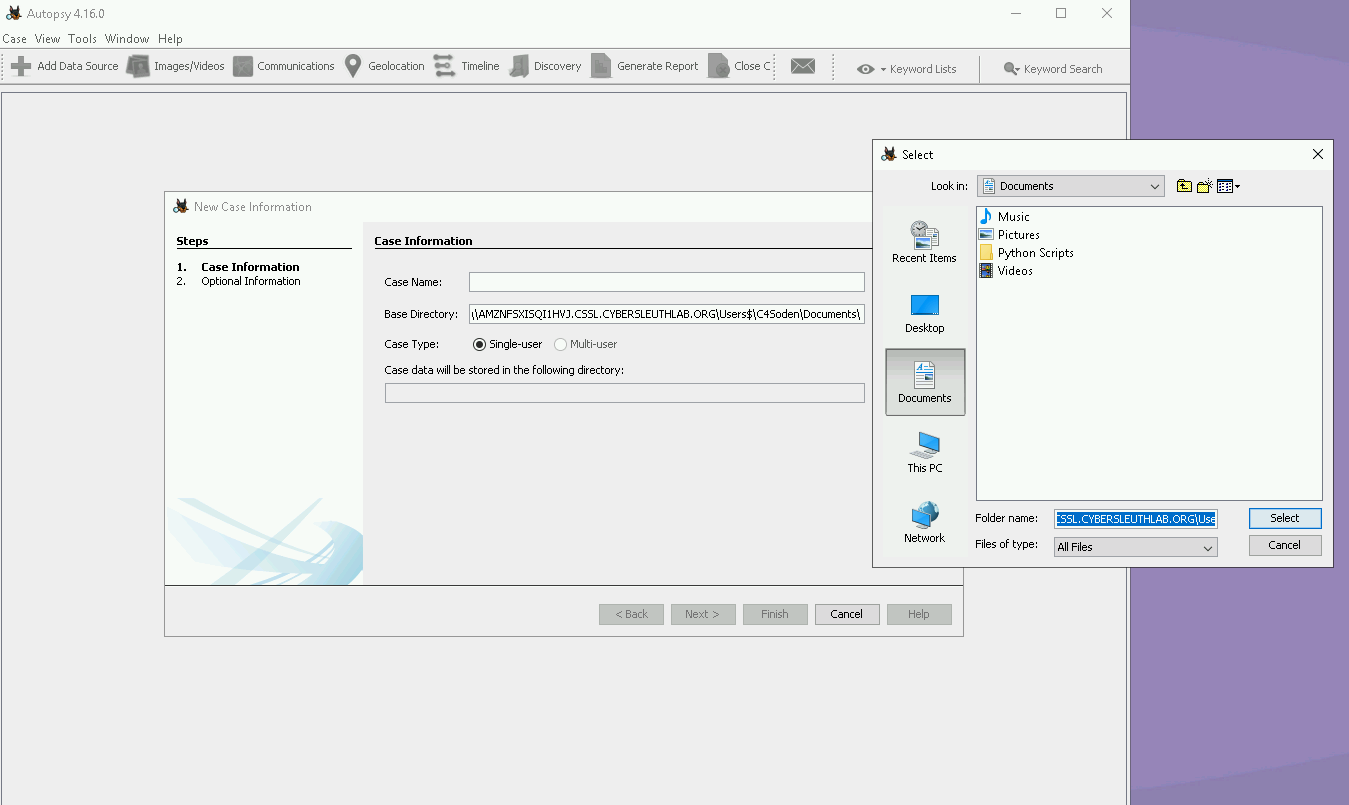
**INVESTIGATE – PART 1**

**Using Autopsy to Recover Deleted Data**

**OPEN AUTOPSY**

* Open Autopsy (wait for it to open)
* Select “No” when window pops up “Enable Central Repository”





**STEP 1 Create a New Case**

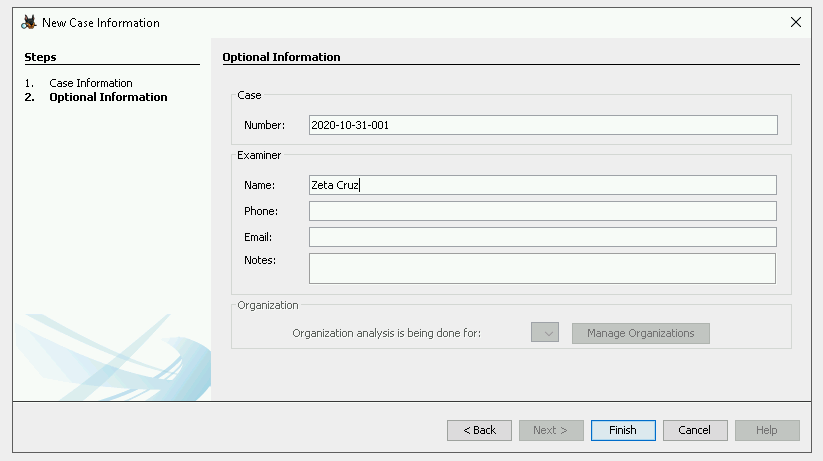
1. Select **Create New** **Case**
2. Enter a **Case Name**
3. Enter **Base Directory**

**IF Base Directory doesn’t automatically load**

Click **[Browse]** and choose **Documents**

Click **[Select]**

Click **[Next]**

*Case data will be stored in this directory.*

1. Additional Information:

Enter **Case Number**

today’s date / case of the day

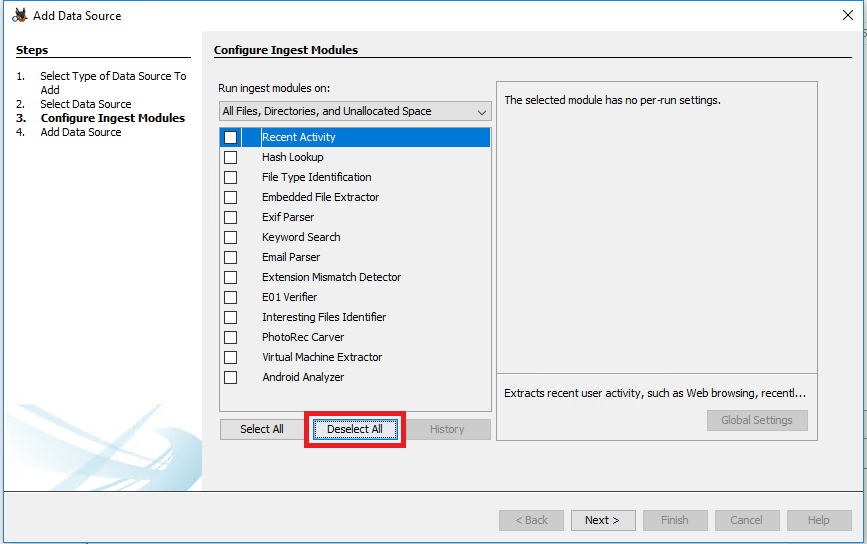
*Example: 2020-1031-001*

Enter **Examiner Name**

**(**your code name)

Click **[Finish]**

**STEP 2 Add Case Data**

1. Select Type of Data

**Disk Image or VM File** on

**Add Data Source** screen

Click **[Next]**

1. Select Data Source

Browse to select the appropriate case data file (located in **Mission 0 folder** on desktop)

Click **[Open]**

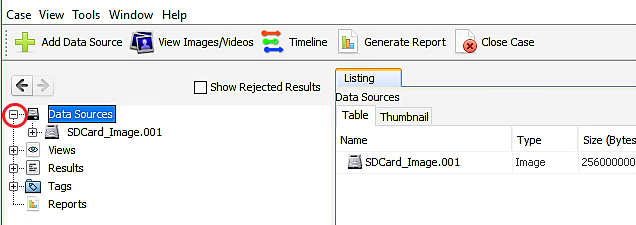
Click **[Next]**

1. In the **Configure Ingest Module** window

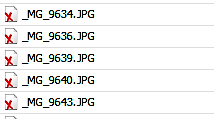
**Deselect All** check boxes

Click **[Next]**

Click **[Finish]**

**STEP 3 Review the Case Data**

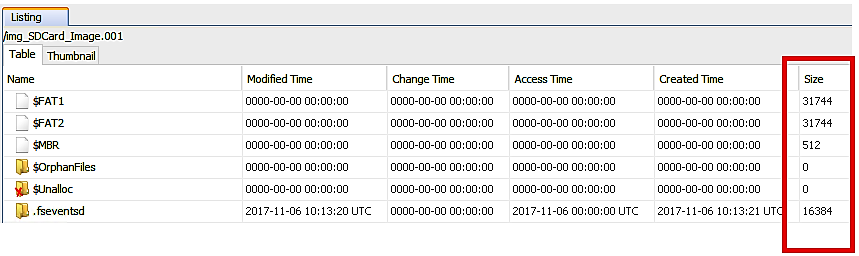
1. Open the **DATA SOURCES** folder on the top left
2. Click on the words **SDCard\_Image.001** to display the items in the Listing window to the right



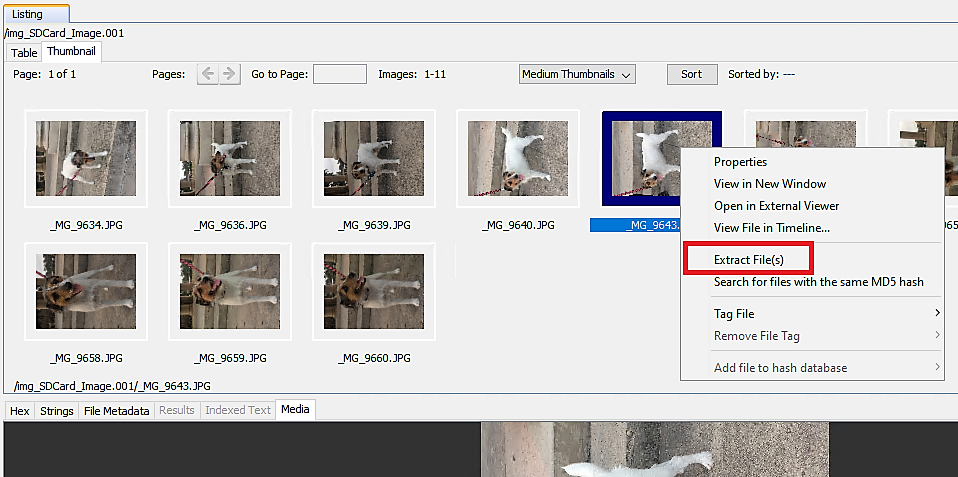
1. Determine If you successfully recovered any deleted files

Files Marked with a **Red X** = Deleted Files

**Successfully Recovered Files = File Size is greater than 0**



1. Click on the **Thumbnail tab** to see if any of the recovered files are photos
2. Select a Recovered Photo

**STEP 4 Extracting The Results**

1. Right Click on the recovered Photo you want to use
2. Choose **Extract File** from the drop-down box
3. Rename the file by entering your code name
4. Save the File on the Desktop in

**Mission 0 → RecoveredPhoto** folder

**STEP 5 More Detailed Analysis**

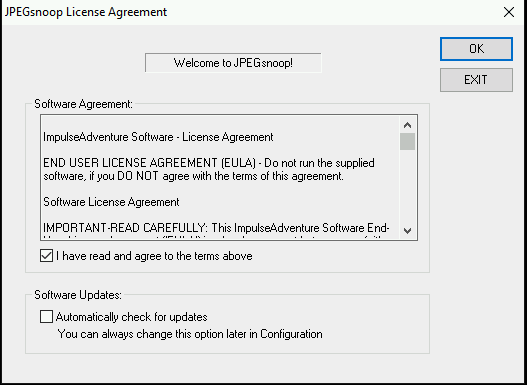
1. Highlight the photo you want to investigate in Autopsy so that image appears in the viewer
2. Select the **STRINGS tab** to view the information embedded in the image

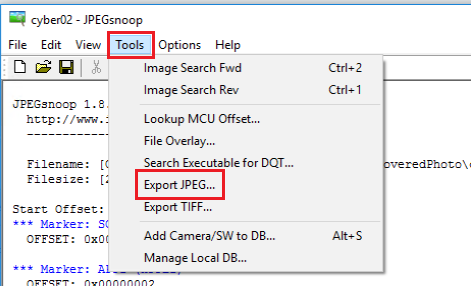


**INVESTIGATE – PART 2**

**Using JPEGsnoop to Review EXIF Metadata**

**Open JPEGsnoop**



1. Select File, Open Image and Select the photo you saved in the **RecoveredPhoto** folder
2. Examine the EXIF metadata stored in the image
3. Copy and paste the EXIF metadata to your Lab Notebook **(SEE TIP 1 BELOW)**
4. Copy and paste the photo to your computer’s desktop

* In JPEGSnoop, click on ***Tools* → *Export JPEG***
* Leave all Settings unchecked and click **[OK]**
* Save the File in the **Desktop → Mission 0 → RecoveredPhoto** folder
* Right-Click on the icon/name for the file and select *copy*.
* Back on your local Desktop, right-click and select *paste*.

**TIP 1 – Copy and Paste to Lab Notebook**

1. *Edit* → *Select All or [CNTRL]-[a] / [CMND]-[a]*

2. *Edit* → *Copy or [CNTRL]-[c] / [CMND]-[c]*

3. Over in the Lab Notebook, click on **[ADD NEW DATA]** button at the bottom of the window

4. Type **JPEGSnoop EXIF DATA** in the *Title* Field

5. Right-Click in the *Data* area and select Paste *or [CNTRL]-[v] / [CMND]-[p]*

6. Click **[SAVE]**