SECURITY+ V4 LAB SERIES

Lab 25: Using Autopsy for Forensics and Lost Data Recovery

Document Version: 2022-04-29

Material in this Lab Aligns to the Following	
CompTIA Security+ (SY0-601) Exam Objectives	4.1: Given a scenario, use the appropriate tool to assess organizational security 4.5: Explain the key aspects of digital forensics
All-In-One CompTIA Security+ Sixth Edition ISBN-13: 978-1260464009 Chapters	26: Tools/Assess Organizational Security 30: Digital Forensics

Contents

Introduction

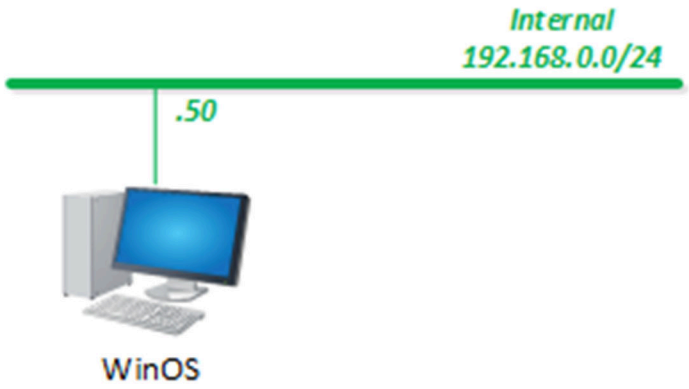
In this lab, you will experience how digital evidence is acquired and recorded.

Objective

In this lab, you will perform the following tasks:

- Create new cases in Autopsy
- Perform simple digital forensics

Lab Topology



Lab Settings

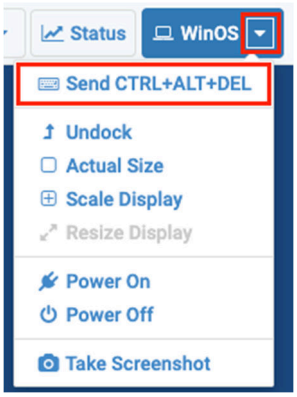
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
WinOS	`192.168.0.50`	`Administrator`	`NDGlabpass123!`

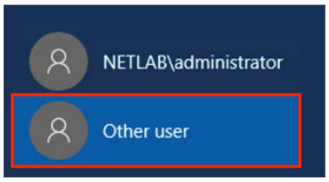
1 Create a New Case and Load the Evidence Image File

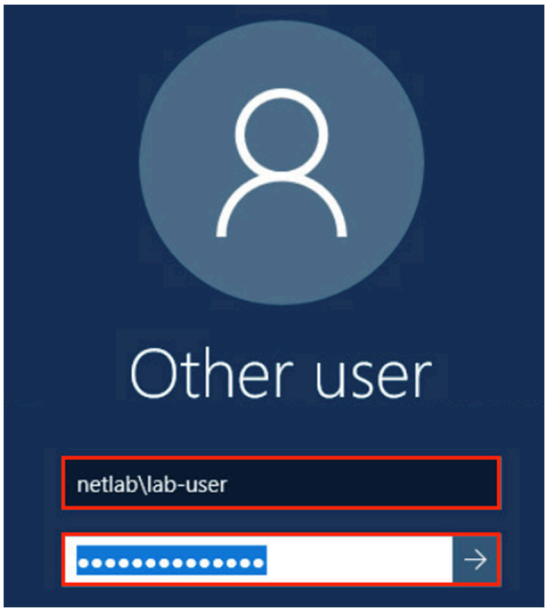
In this task, you will add the Active Directory Certificate Services role to the Windows server.

1. Launch the **WinOS** virtual machine to access the graphical login screen. While on the splash screen, focus on the *NETLAB+* tabs. Click the dropdown menu for the **WinOS** tab and click on **Send CTRL+ALT+DEL**.

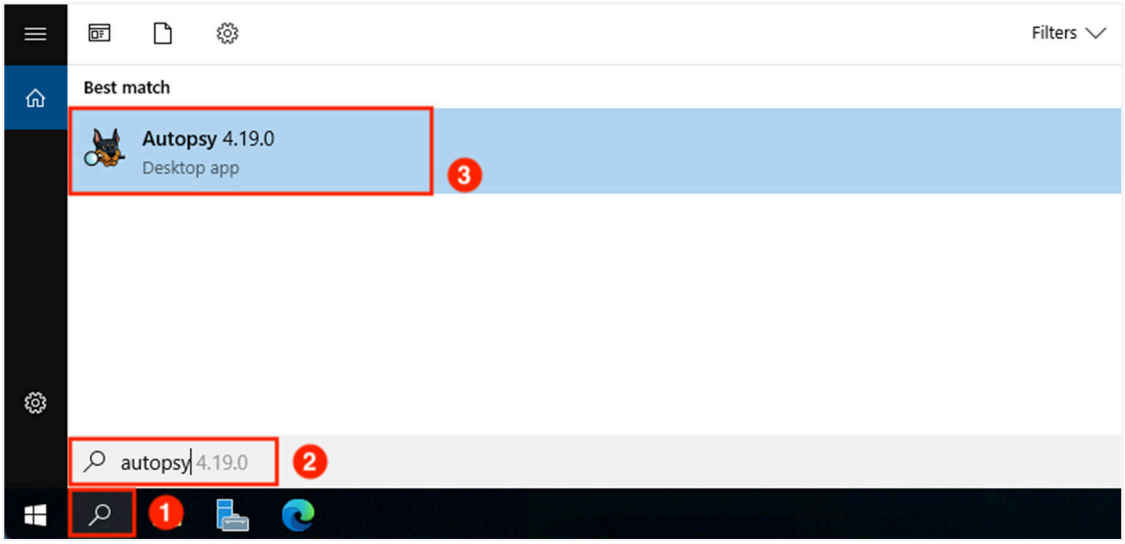


2. In the lower-left corner, click **Other user**, then type `netlab\lab-user` as the *username* and *password* `NDGlabpass123!`.

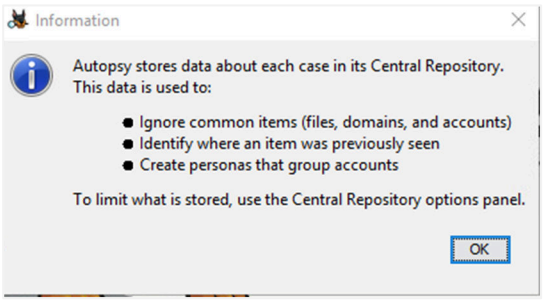




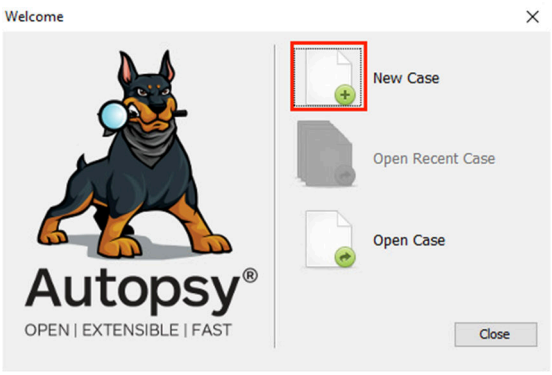
3. Ignore or minimize the *Server Manager* window, click the **Search** icon in the taskbar, type `Autopsy`, then click **Autopsy 4.19.0** to start the program.



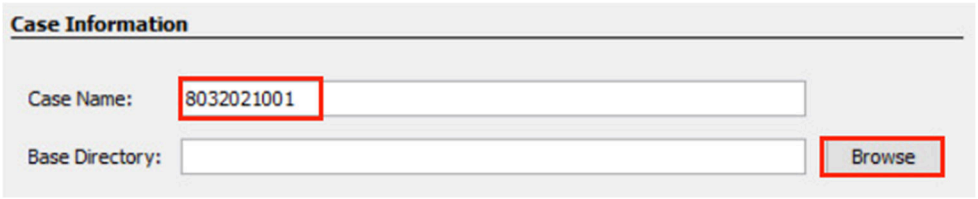
4. Click **OK** in the pop-up window.



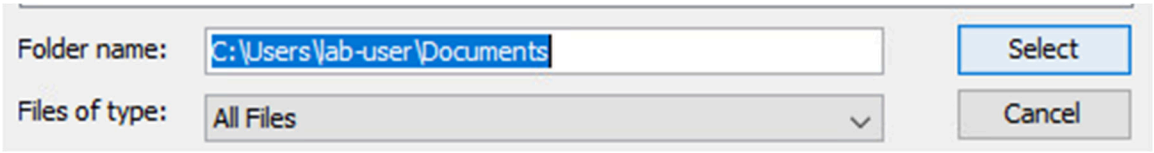
5. In the *Welcome* window, click the **New Case** button to start a new case.



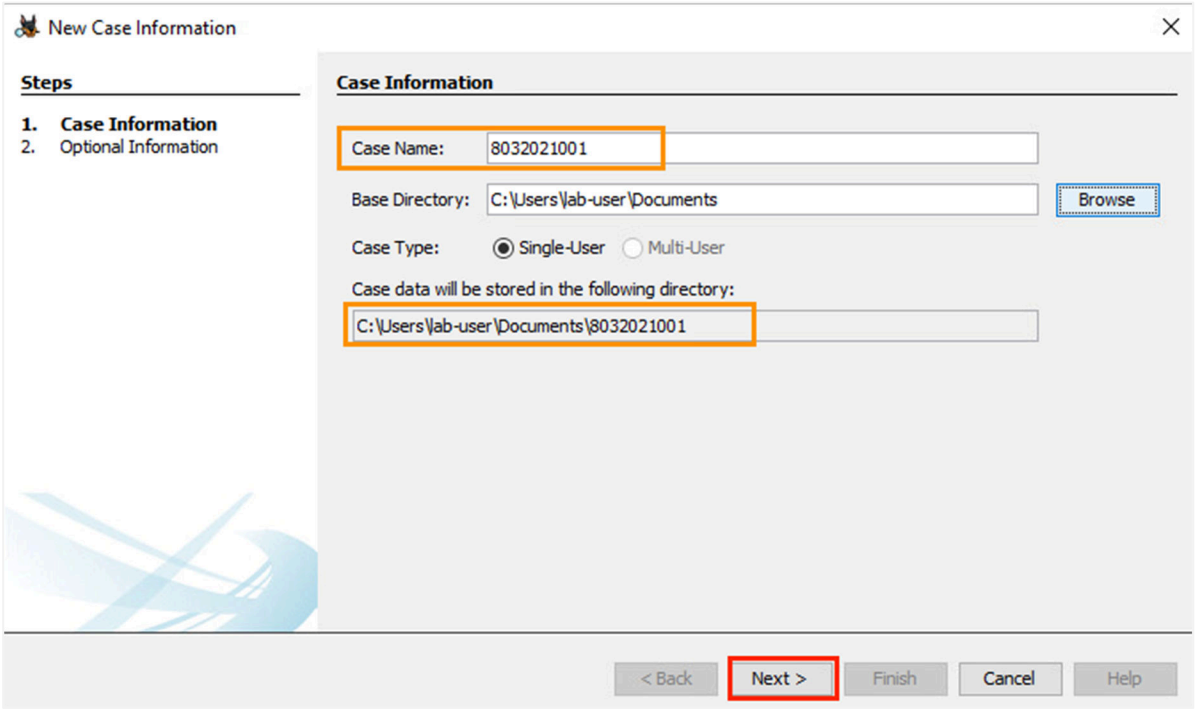
6. Type `8032021001` as the *Case Name*, and click **Browse.**



7. In the *Select file* window, in the *Folder name* box, double-check to make sure it looks like the picture shown below, then click **Select.**

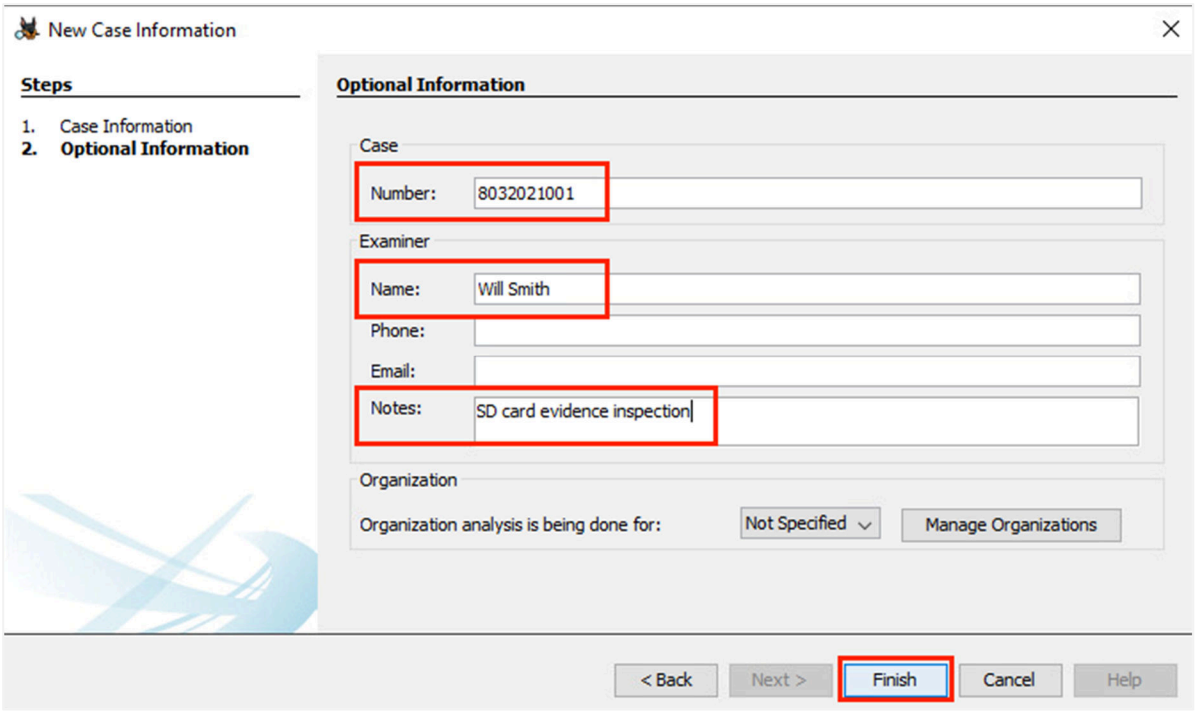


8. You will be brought back to the *Case Information Step*, review the information, then click **Next.**

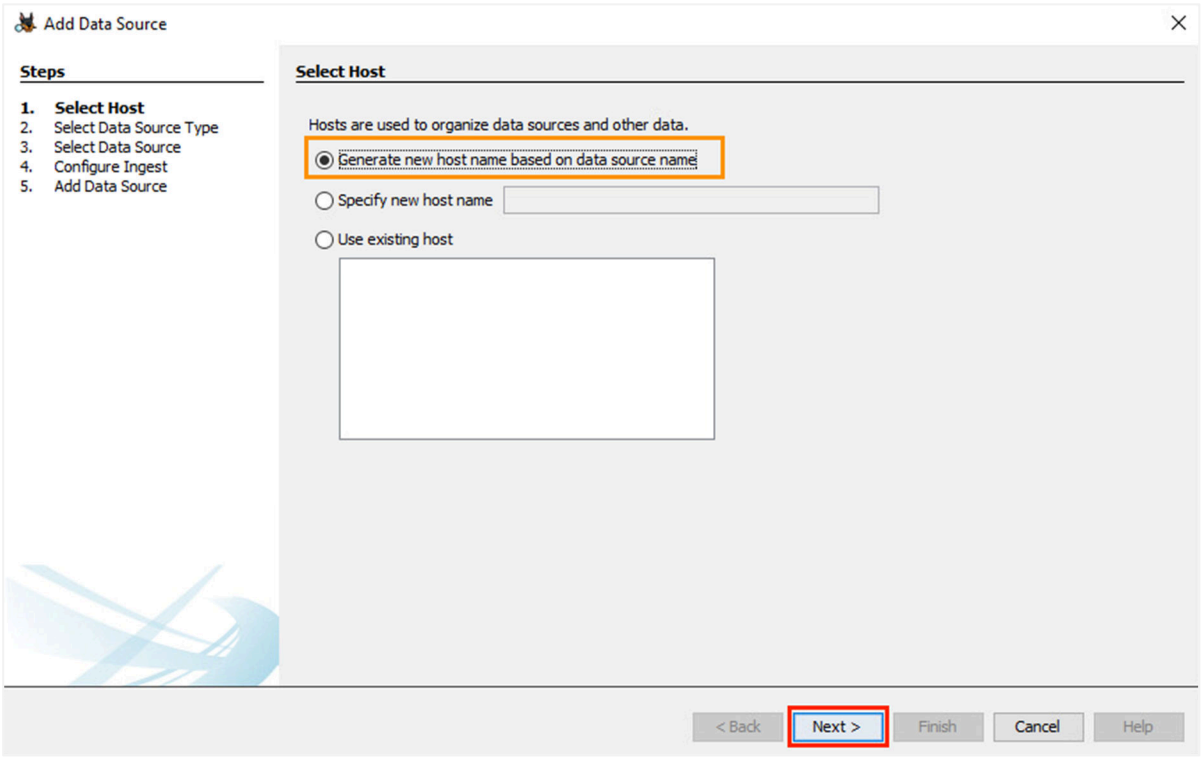


9. On the optional information page, we choose to fill out the following information, then click **Next.**

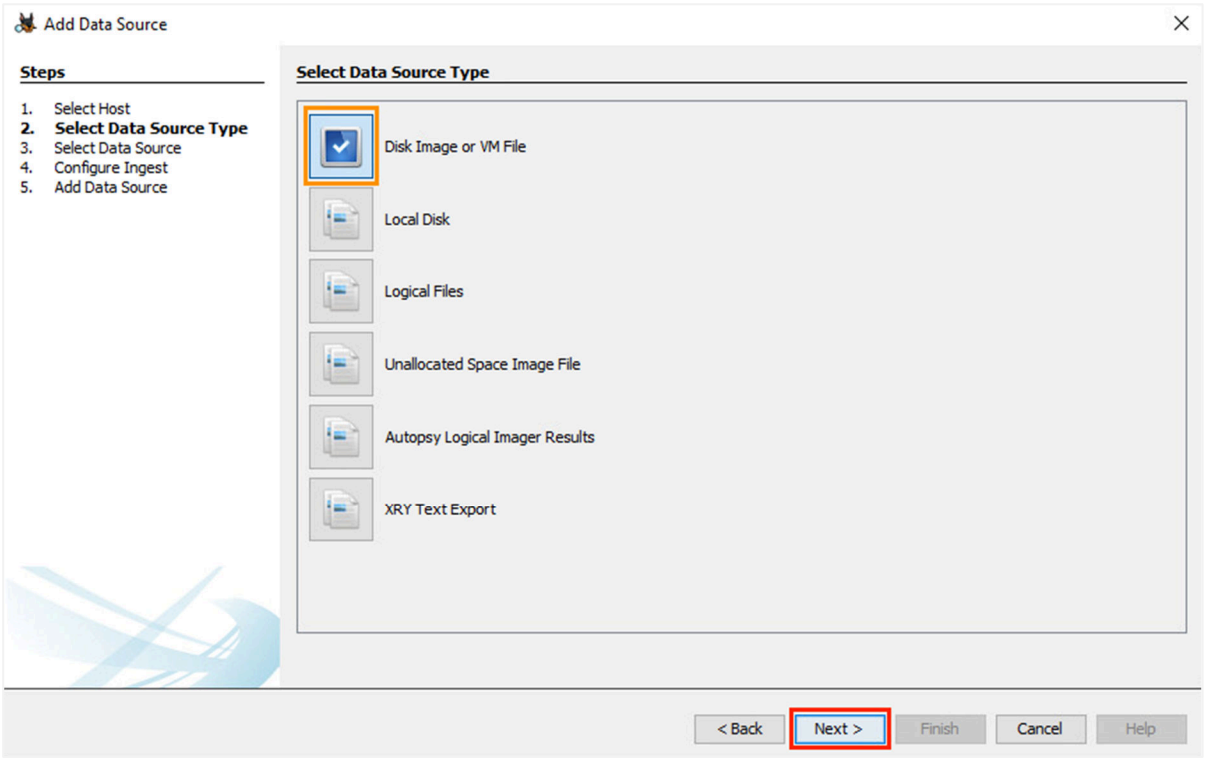
Number: `8032021001`
Name: `Will Smith`
Notes: `SD card evidence inspection`



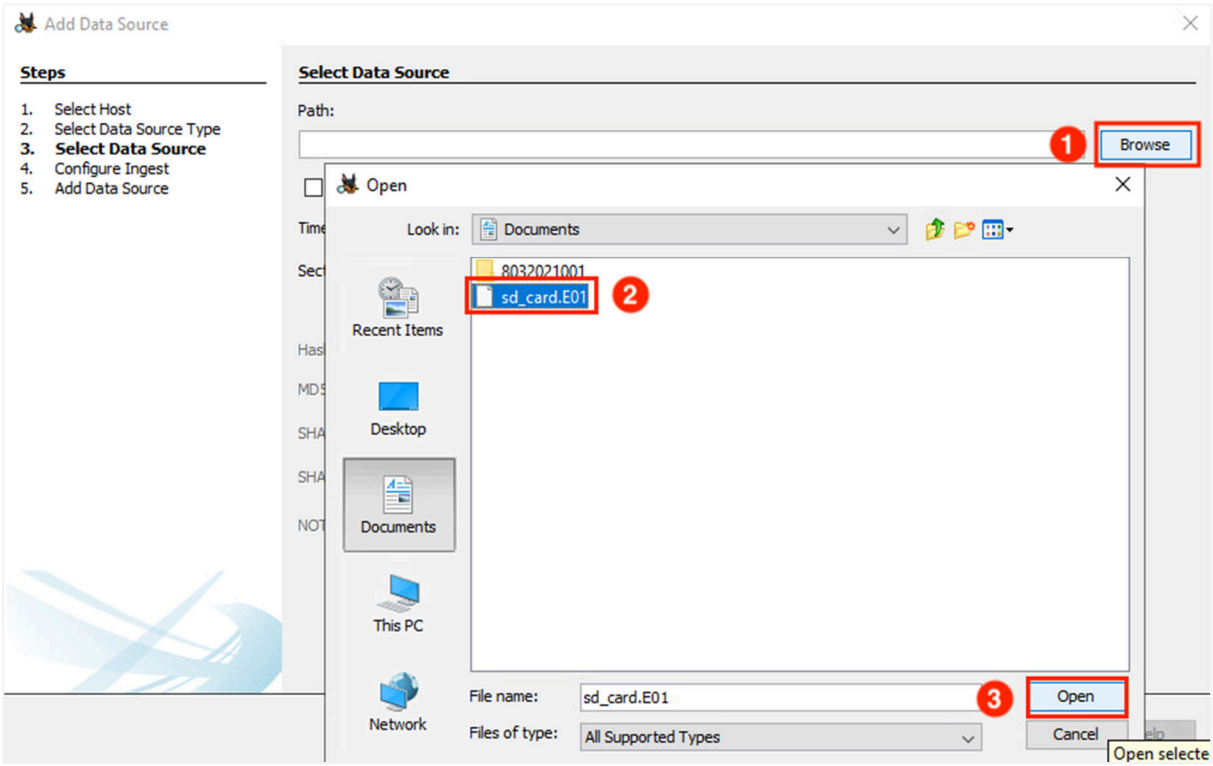
10. Wait until *Add Data Source* is opened. In the *Select Host* step, make sure *Generate new host name based on data source name* is selected and click **Next.**



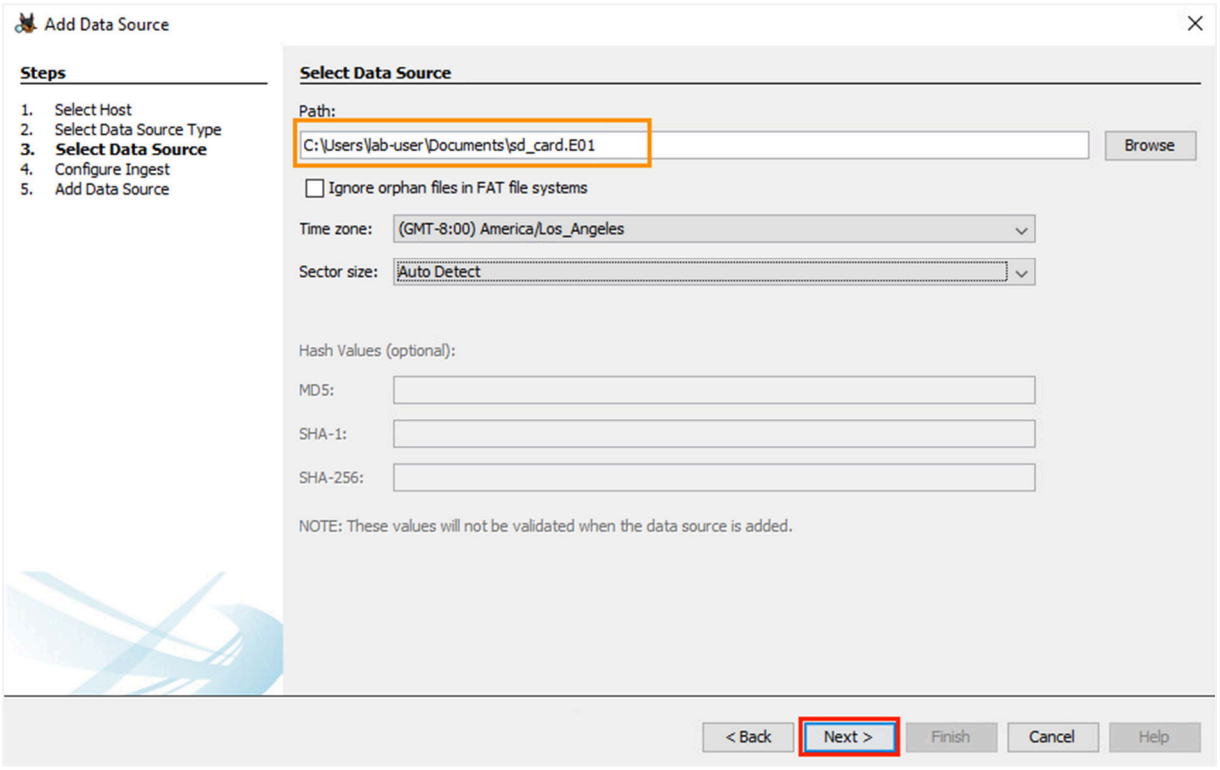
11. On the next screen, make sure the *Disk Image or VM File* option is selected and click **Next.**



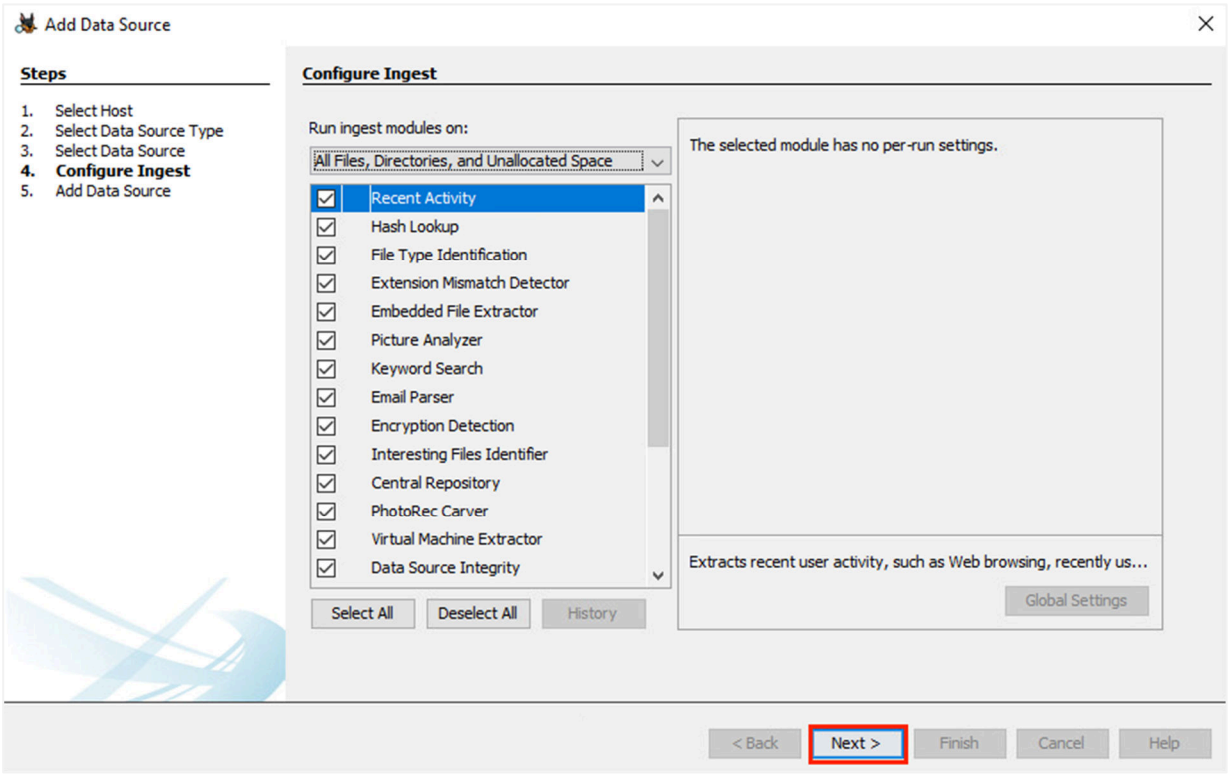
12. On the new screen, click **Browse,** then select the **sd_card.E01** file, and click **Open.**



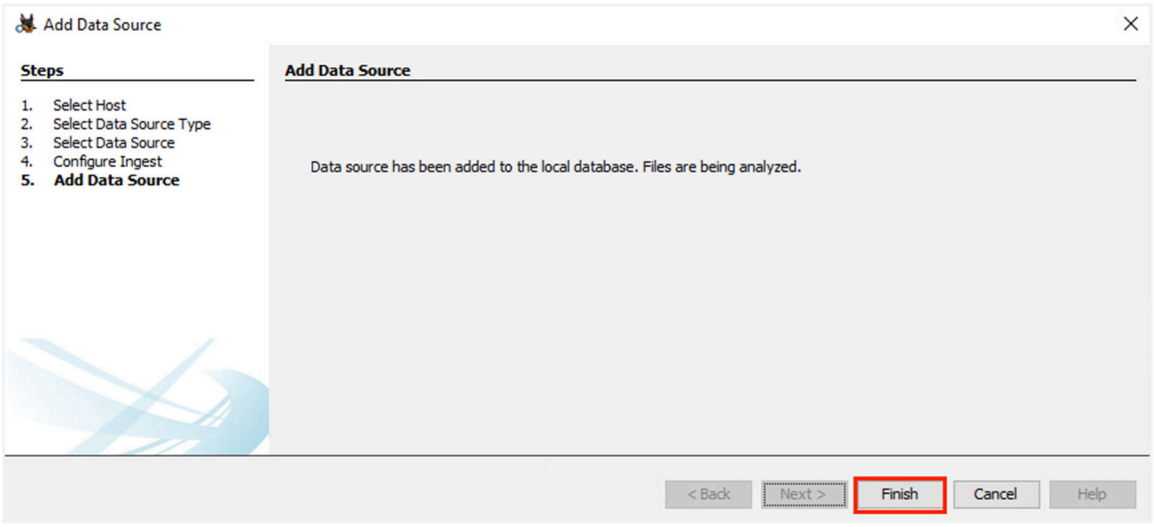
13. Review the information, then click **Next.**



14. On the *Configure Ingest* step, leave the default setting and click **Next.**



15. The program will analyze the image file. Once complete, click **Finish.**



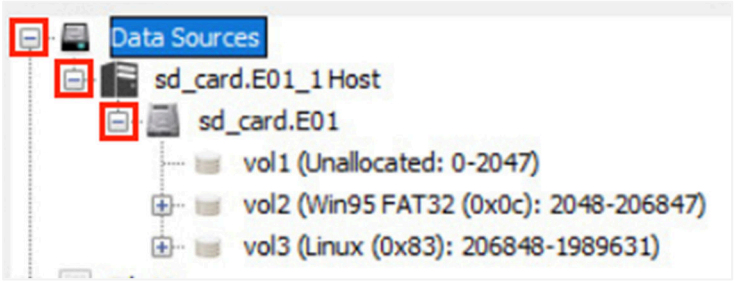
16. *Autopsy* will start adding the source. Proceed to the next section.

2 Explore the Autopsy Software and Examine the Evidence Image

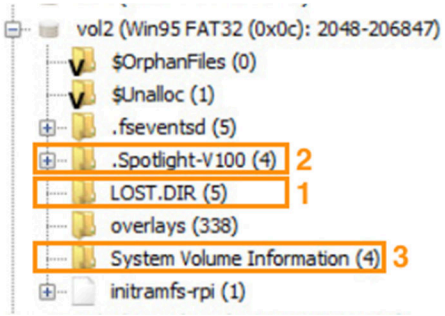
1. Now, we are in the *Autopsy* software, with the image loaded as our case evidence file. Notice, in the lower-right corner, it indicates that the software is still analyzing the files found from the evidence image.

2. At the top-right corner of the *Autopsy* window, click the square to maximize the window, so we get a bigger view of the program. This will help to view the files if there is a long list to display.

3. First, let's click on the **+** in front of the *Data Source*, then click the **+** again, and click it for the third time; you will see the partition information. The image was partitioned into three parts, *Vol1, Vol2*, and *Vol3*. *Vol2* is in a Win FAT32 format, *Vol3* is in a Linux format.

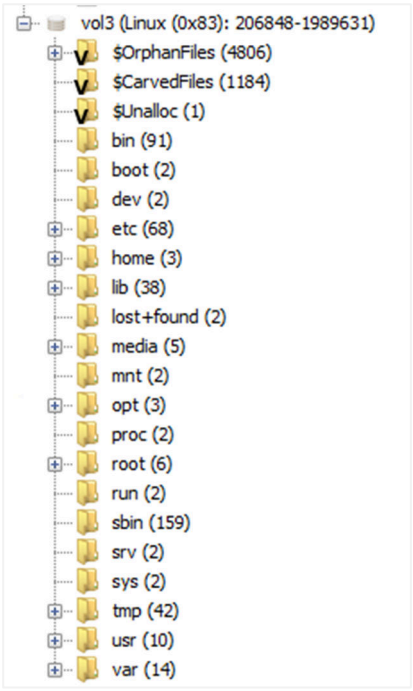


4. Click the **+** in front of Vol2; we can see that the evidence was once plugged into 1)an Android device; 2) a Mac computer; 3) a Windows computer. Feel Free to expand different folders in *Vol2* to explore the files found.

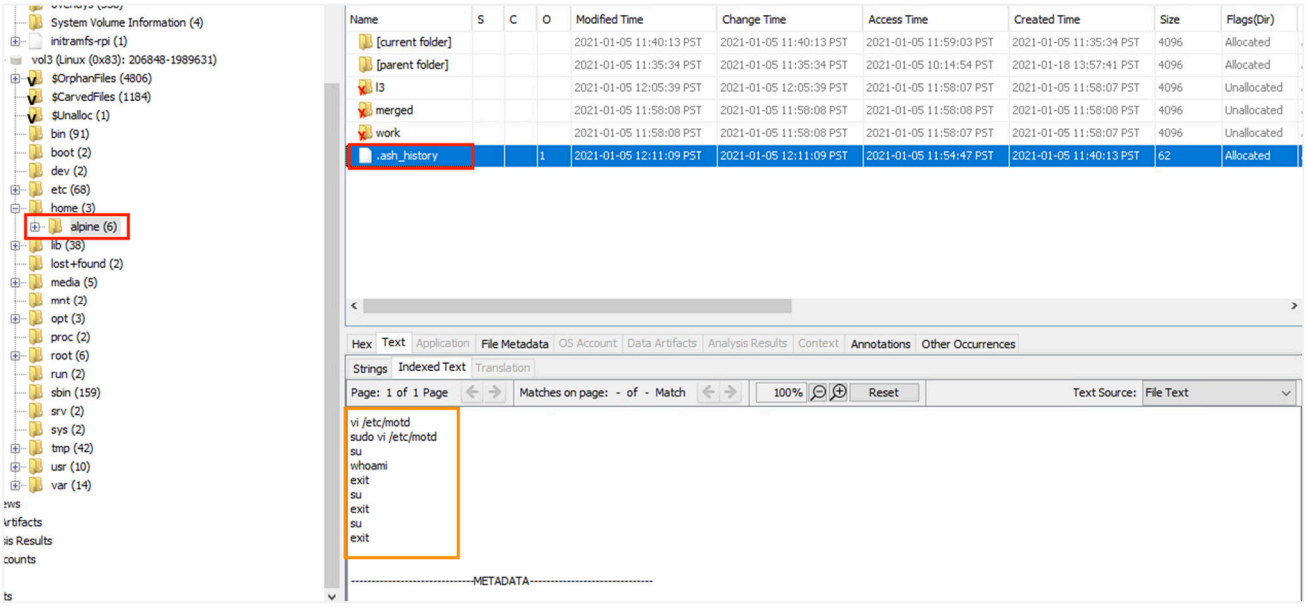


Certain systems will auto generate certain files/folders. For instance: the .Spotlight-V100 is from macOS; LOST.DIR is from Android; and System Volume Information is from Windows OS.

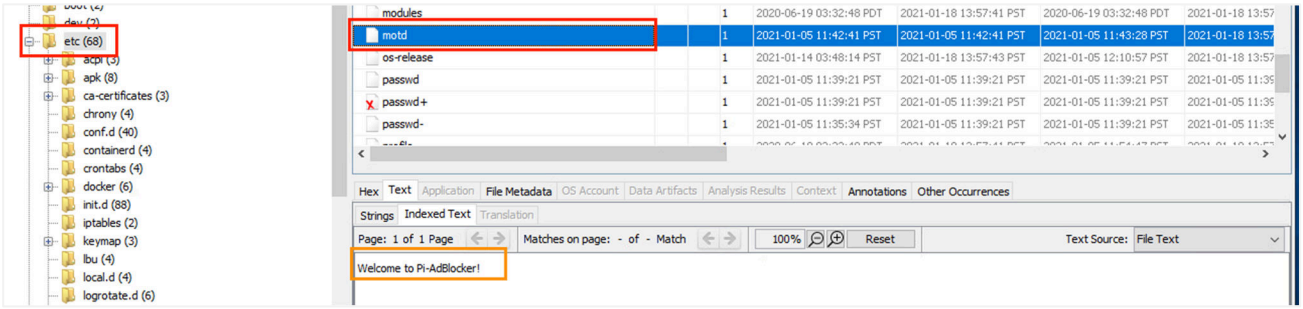
5. Click the **+** in front of *Vol3*. We will see a structure that looks like a Linux system.



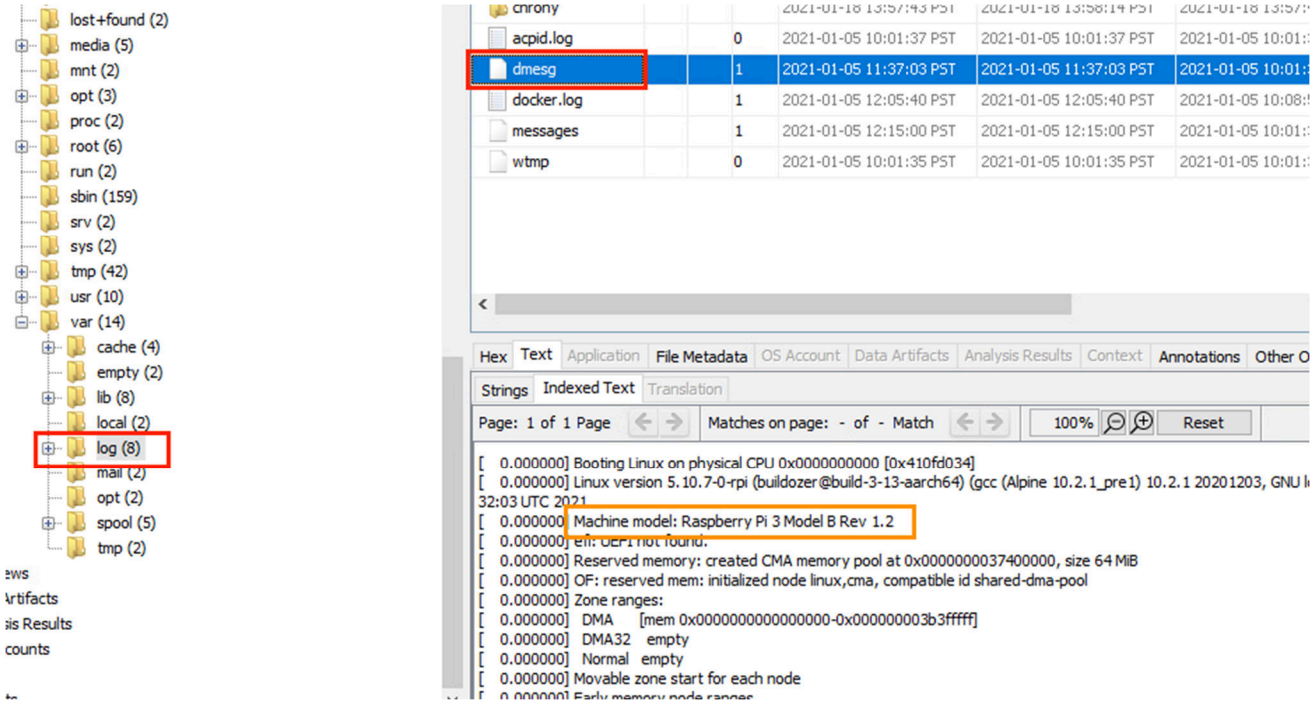
6. Click to expand the **home** folder; we see a folder named *alpine*, which is also the username. Click on **alpine**; on the right side, it will open the *alpine* folder. Click on the **.ash_history**. We can see what commands had executed before. It looks like someone changed the content in the *motd* file.



7. We'll now click on the **etc** folder, and to the right side, find the **motd** file and click to examine the file content. You will need to scroll down to see the file. The *motd* file says *Welcome to Pi-AdBlocker!* We can confirm that this SD card was once used to host the Pi-AdBlocker server.

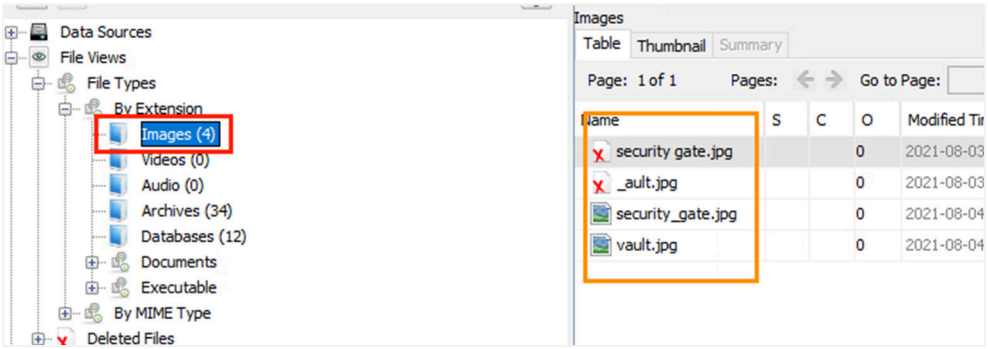


8. There is other information one can find in the *etc* folder. Please feel free to explore the files. Next, we will check the *var* folder.
9. Click the **+** in front of *var*, then click the **log** folder. Then on the right side, click the **dmesg** file. *dmesg* contains the hardware information the alpine system was running on. It looks like the system was on a *Raspberry Pi 3 Model B* device.

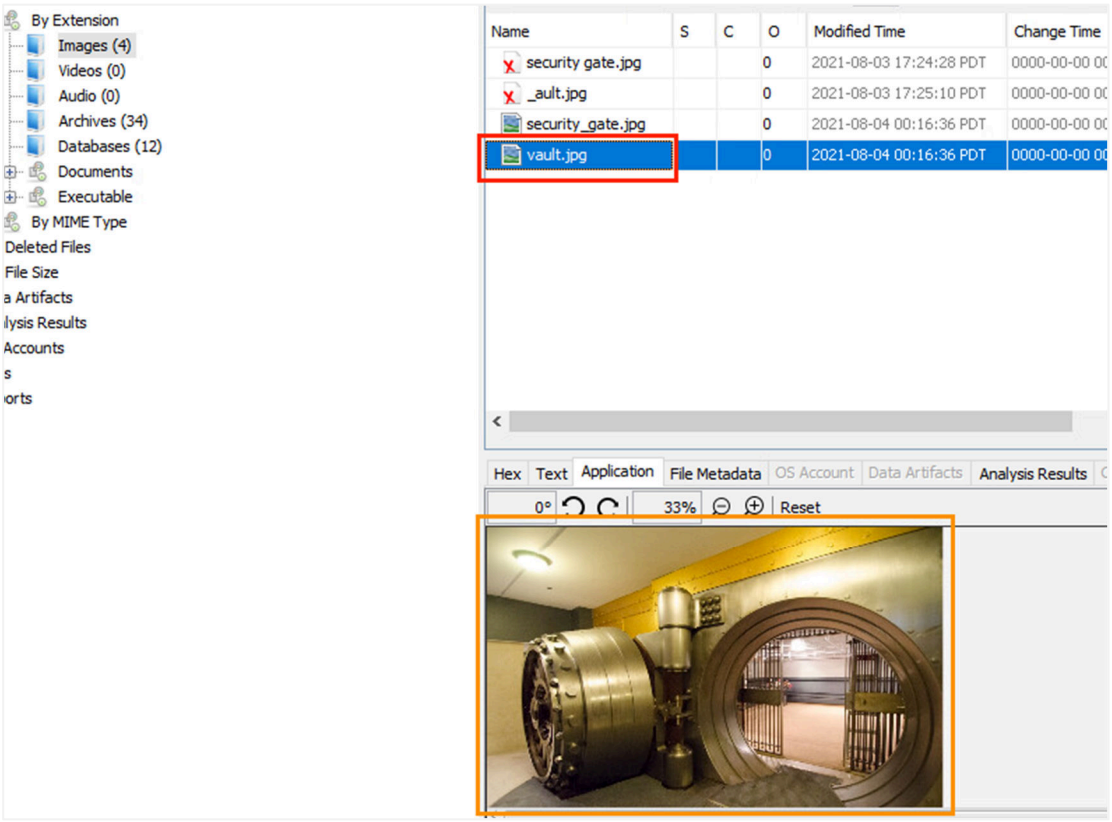


10. To the left side, scroll to the top, then click the **-** in front of the *Data Source* to compress the folder, so it is easier to navigate. Next, we will pay attention to the *File Views* section.

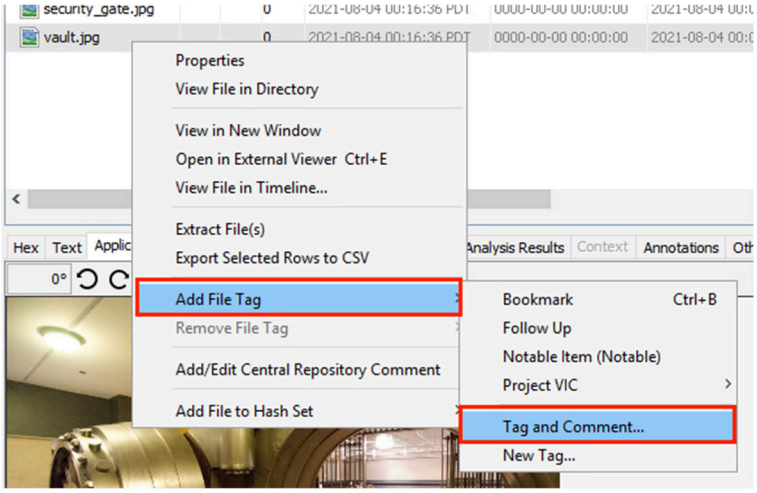
11. Click the **+** in front of **File Views**, then **File Types**, and then **By Extension,** and then click on **Images.**



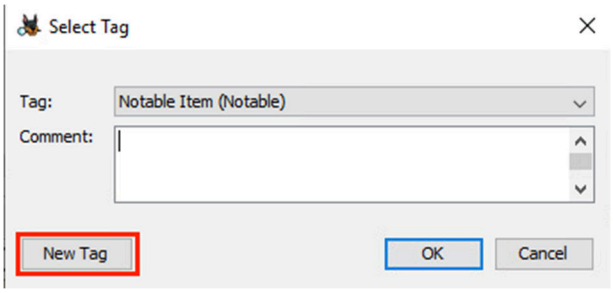
12. On the right side, we see 4 *.jpg* files, the **X** mark on the file icon indicates the file was previously deleted. If you click on one of the other two files, you will see an image preview in the *Autopsy* software.



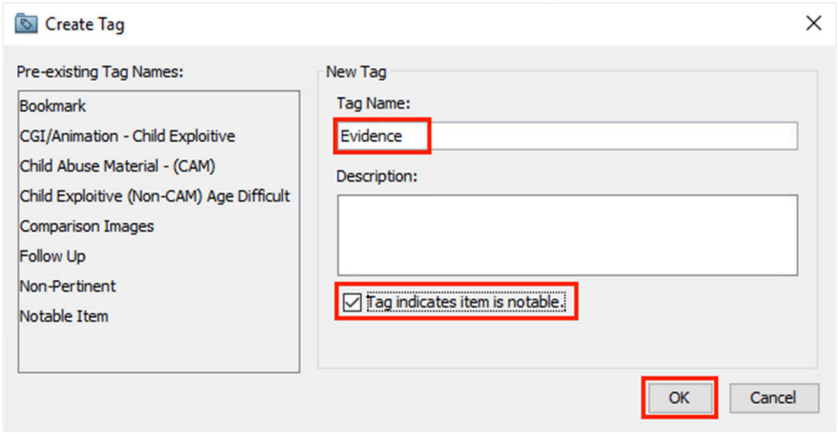
13. Right-click on **vault.jpg**, select **Add File Tag > Tag and Comment**.



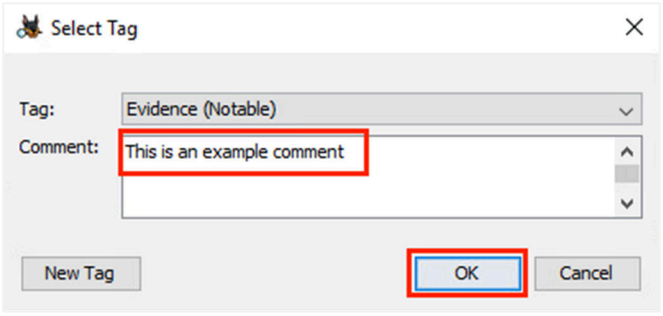
14. In the pop-up window, we are going to add a new tag. Click the **New Tag** button.



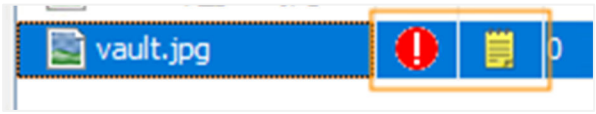
15. We will name the new tag as `Evidence` and then check the **checkbox**. Click **OK.**



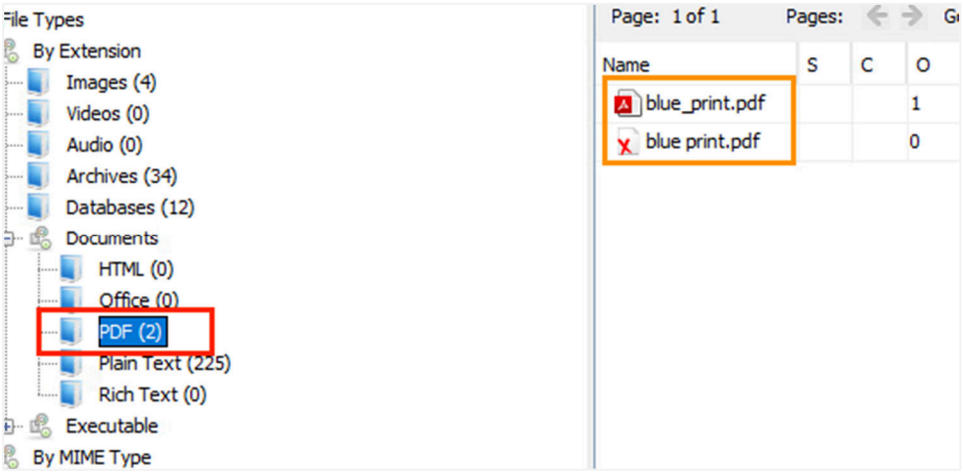
16. Once we are brought back, the new tag will be applied automatically. We will add `This is an example comment` in the *Comment* box. Then, click **OK.**



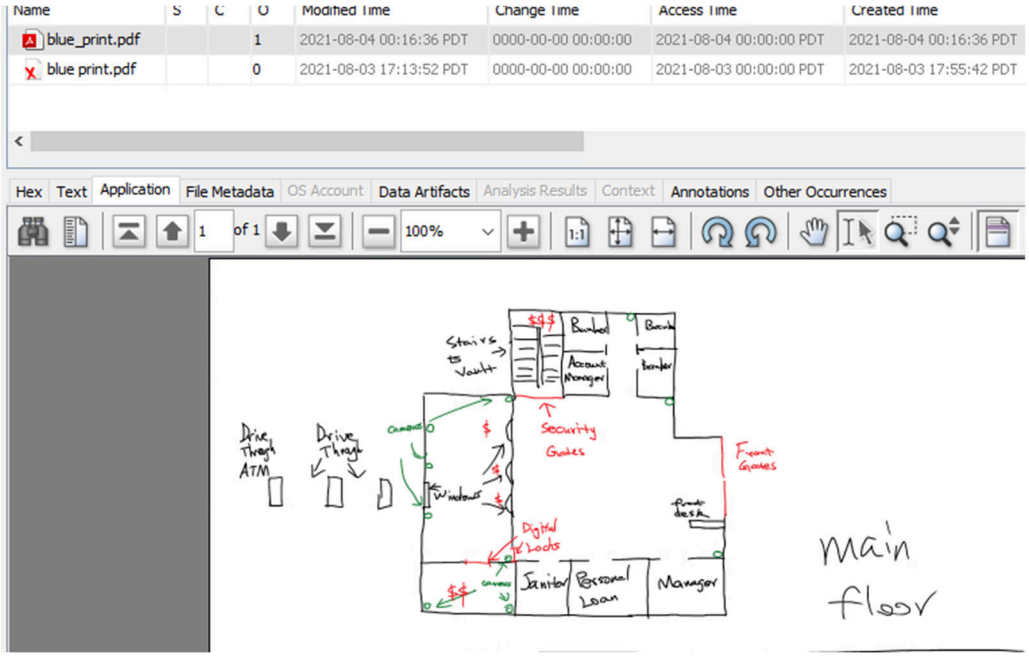
17. You will now see two icons added to the file. Repeat the step to add the evidence tag and comments to **security_gate.jpg**.



18. Now let's move on to the *Documents*; click **+** to expand it, then click **PDF**. There should be two files listed on the right side.



19. Click on the first PDF file; the preview will show a hand-drawn blueprint of a bank. This is important evidence that is related to a bank robbery.

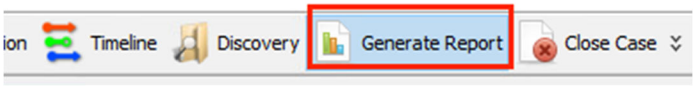


20. Repeat the tag-adding step to add tag and comments to the PDF file.

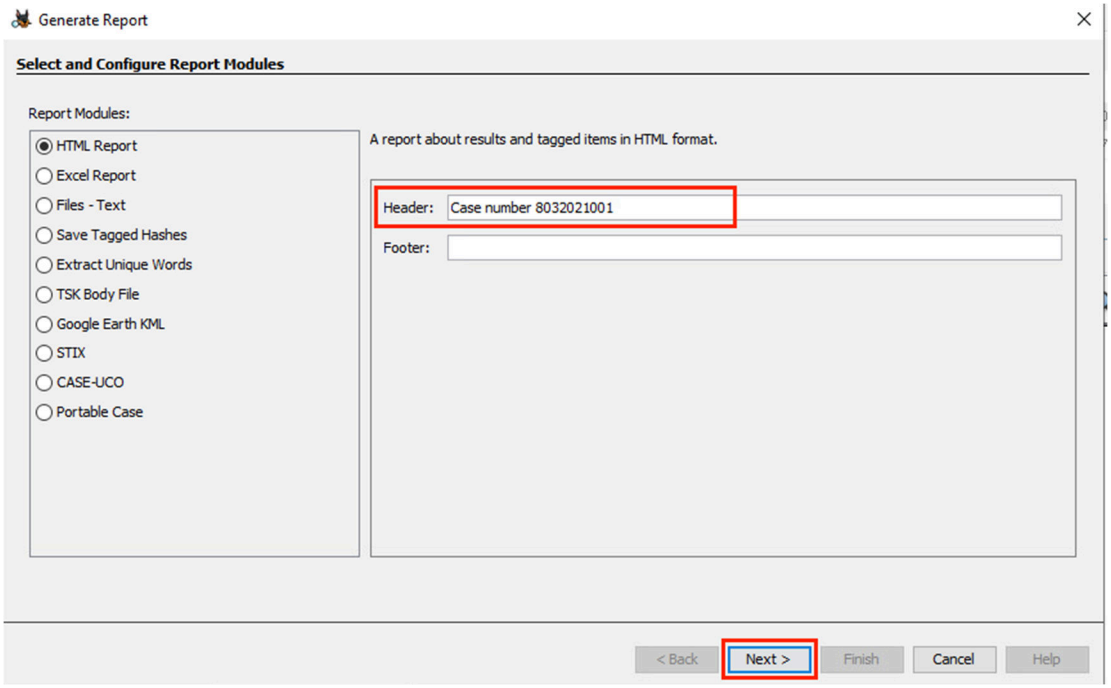
21. The investigation section is finished. Continue to the next section to generate a report.

3 Generating a Report

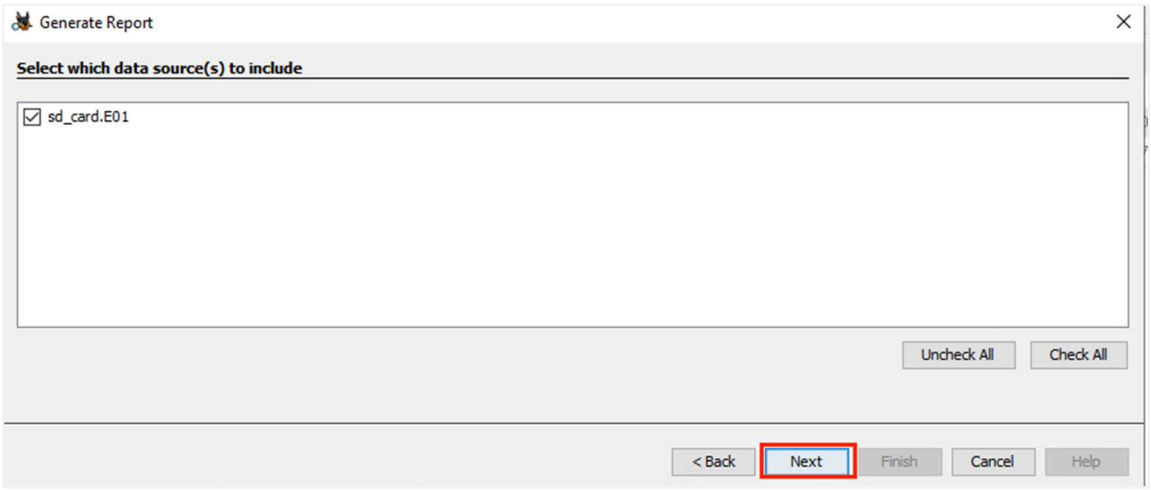
1. Let's say that we did more investigation and did not find any other evidence. It is now a good time to generate the report. Click on the **Generate Report** button in the toolbar.



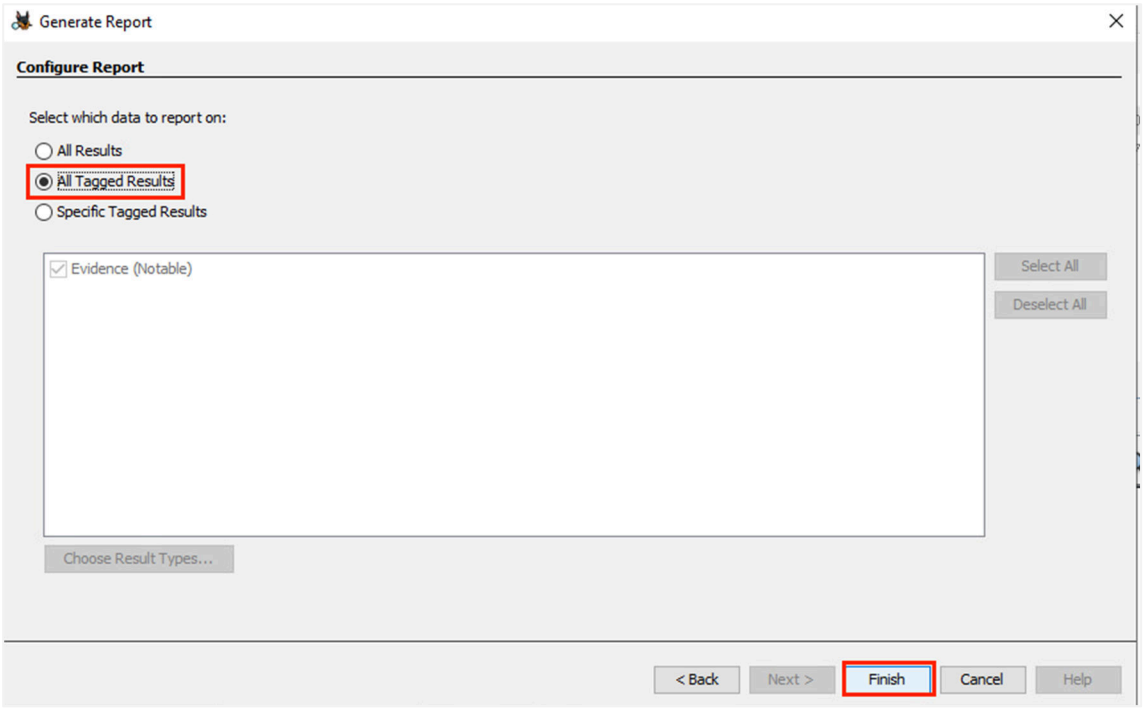
2. A window will pop up, and we will be creating an HTML Report. We will put `Case number 8032021001` as our *Header* and leave the *Footer* blank. Click **Next.**



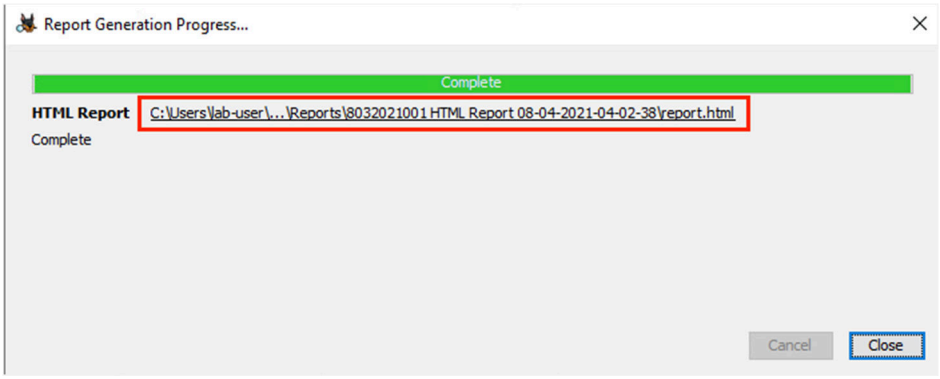
3. On the *Select which data source(s) to include* step, leave the default setting, click **Next.**



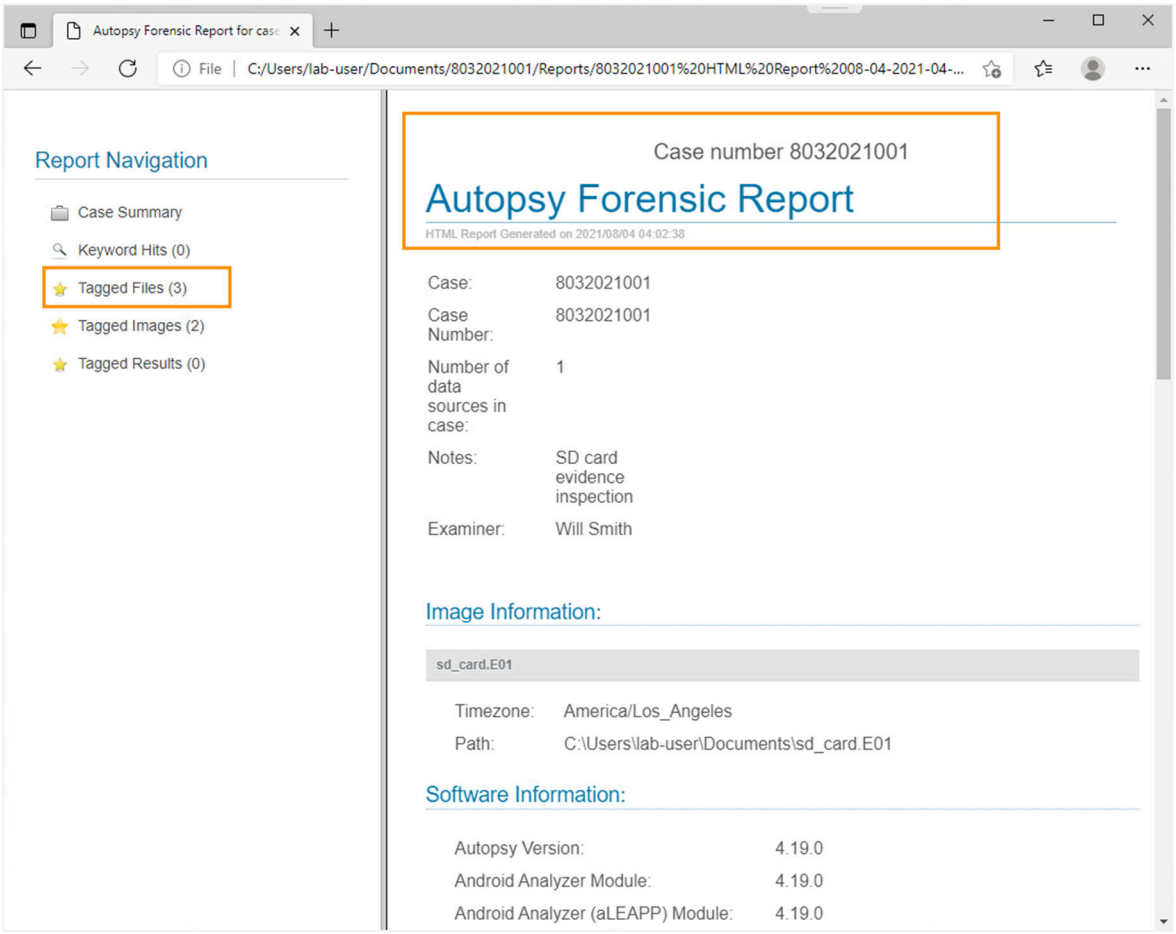
4. On the *Configure report* step, check the **All Tagged Results** radio button, then click **Finish.**



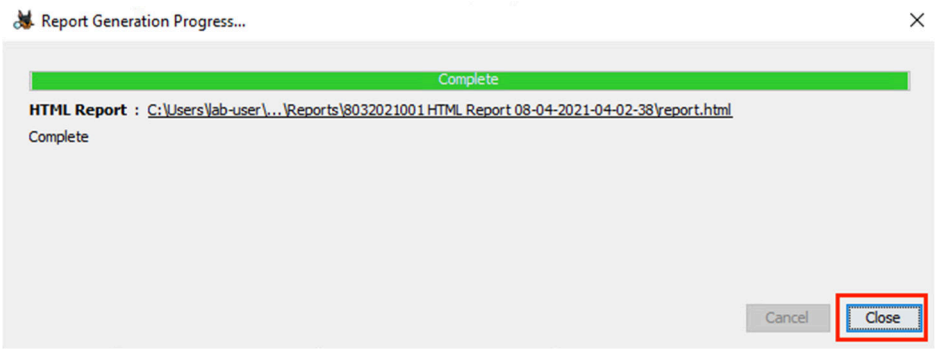
5. The program will generate the report. When it completes, click on the *HTML Report* URL link to see the report.



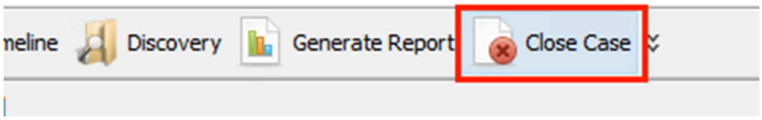
6. Feel free to scroll down and explore the HTML report. The previously tagged files will be pulled out as the evidence image. You can check them by clicking on the **Tagged Files** link on the left side of the page.



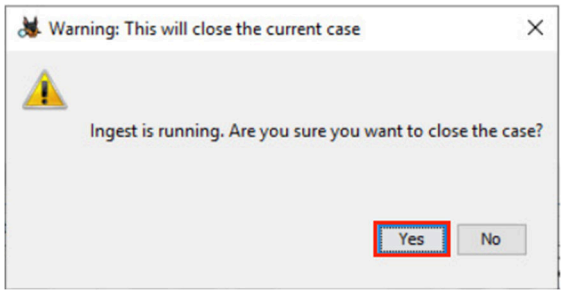
7. Close the browser window. Then close the report generation window.



8. Back to the *Autopsy* window, if we think everything is done. We can now click the **Close Case** button.



9. If prompted saying that *Ingest is running*, go ahead and click **Yes** to close the case.



10. You will be brought back to the *Welcome* page.
11. The lab is now complete; you may end the reservation.