



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

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.
KALI LINUX™ is a trademark of Offensive Security.
Microsoft®, Windows®, and Windows Server® are trademarks of the Microsoft group of companies.
VMware is a registered trademark of VMware, Inc.
SECURITY ONION is a trademark of Security Onion Solutions LLC.
Android is a trademark of Google LLC.
pfSense® is a registered mark owned by Electric Sheep Fencing LLC ("ESF").
All trademarks are property of their respective owners.

Contents

Introduction	3
Objective	3
Lab Topology.....	4
Lab Settings.....	5
1 Create a New Case and Load the Evidence Image File	6
2 Explore the Autopsy Software and Examine the Evidence Image.....	13
3 Generating a Report.....	20

Introduction

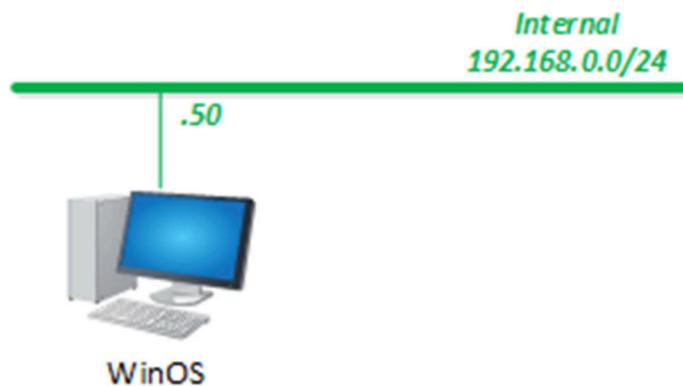
In this lab, you will experience how digital evidence is acquired and recorded.

Objective

In this lab, you will perform the following tasks:

- Create new cases in Autopsy
- Perform simple digital forensics

Lab Topology



Lab Settings

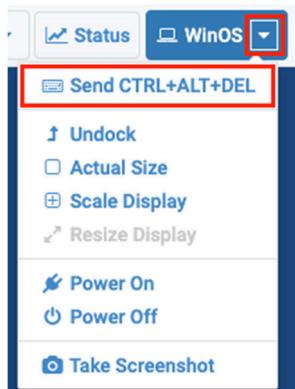
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
WinOS	192.168.0.50	Administrator	NDGLabpass123!

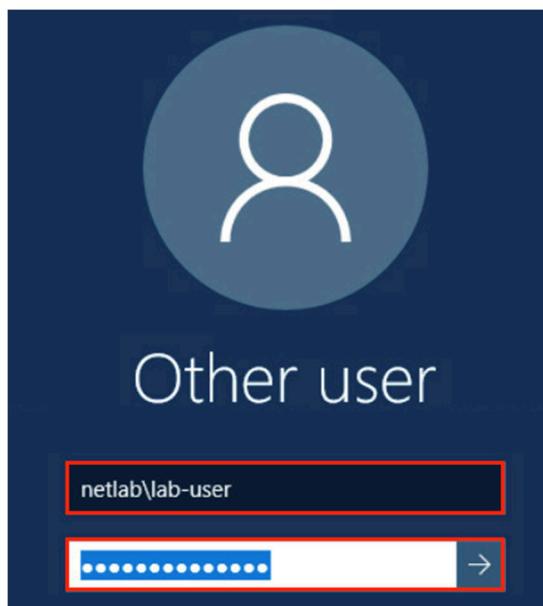
1 Create a New Case and Load the Evidence Image File

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

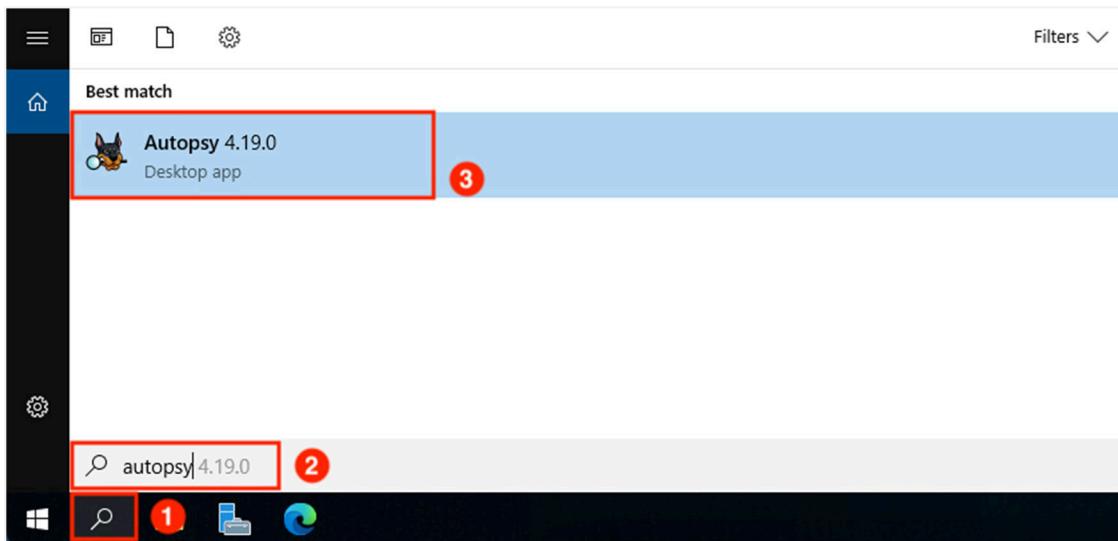
1. Launch the **WinOS** virtual machine to access the graphical login screen. While on the splash screen, focus on the *NETLAB+* tabs. Click the dropdown menu for the **WinOS** tab and click on **Send CTRL+ALT+DEL**.



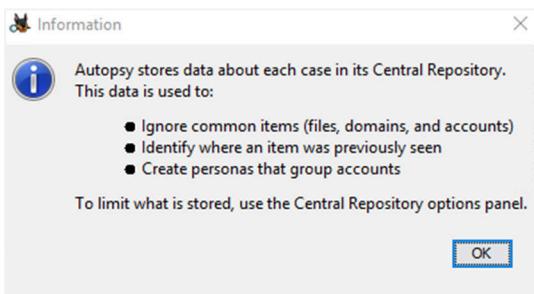
2. In the lower-left corner, click **Other user**, then type `netlab\lab-user` as the *username* and *password* `NDGLabpass123!`.



- 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.



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



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



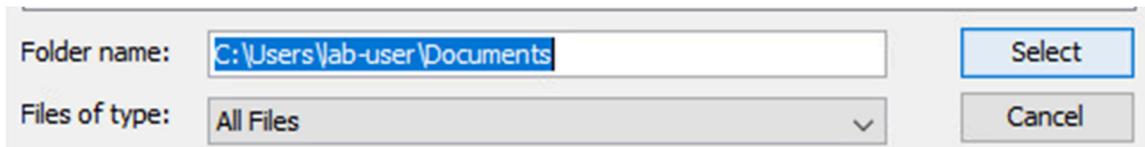
6. Type 8032021001 as the *Case Name*, and click **Browse**.

Case Information

Case Name:

Base Directory:

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**.

New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

Case Name:

Base Directory:

Case Type: Single-User Multi-User

Case data will be stored in the following directory:

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

New Case Information

Steps

- Case Information
- Optional Information

Optional Information

Case

Number: 8032021001

Examiner

Name: Will Smith

Phone:

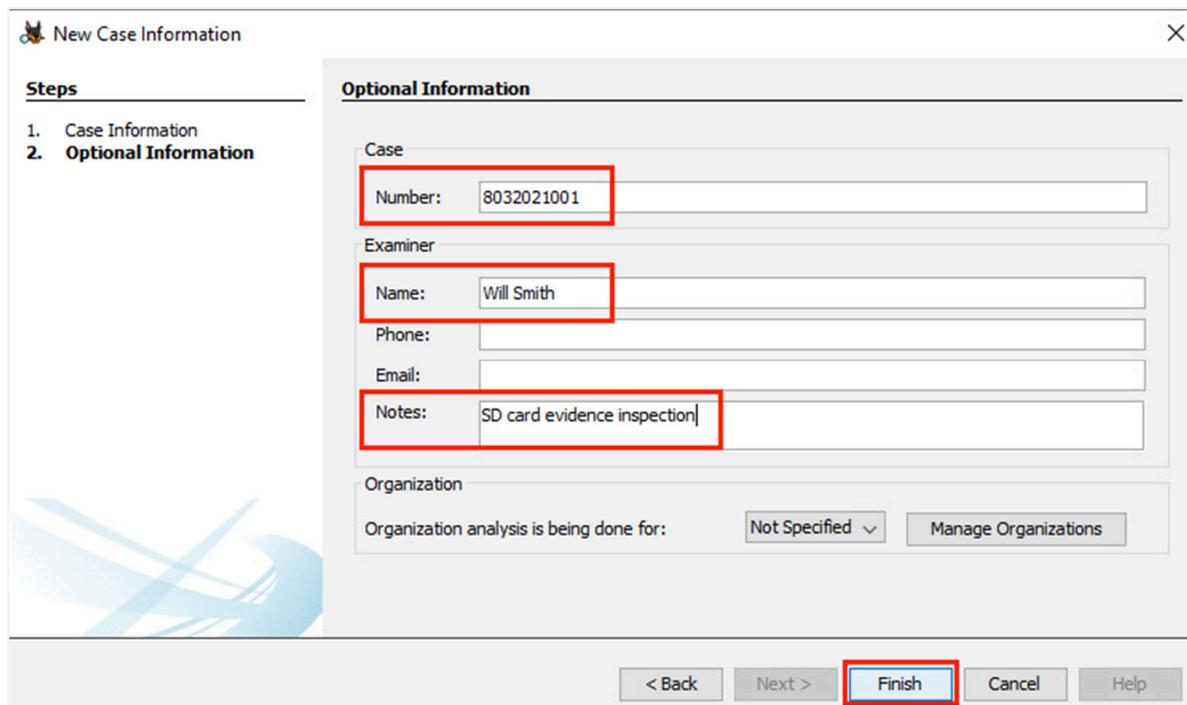
Email:

Notes: SD card evidence inspection

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > **Finish** Cancel Help



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**.

Add Data Source

Steps

- Select Host
- Select Data Source Type
- Select Data Source
- Configure Ingest
- Add Data Source

Select Host

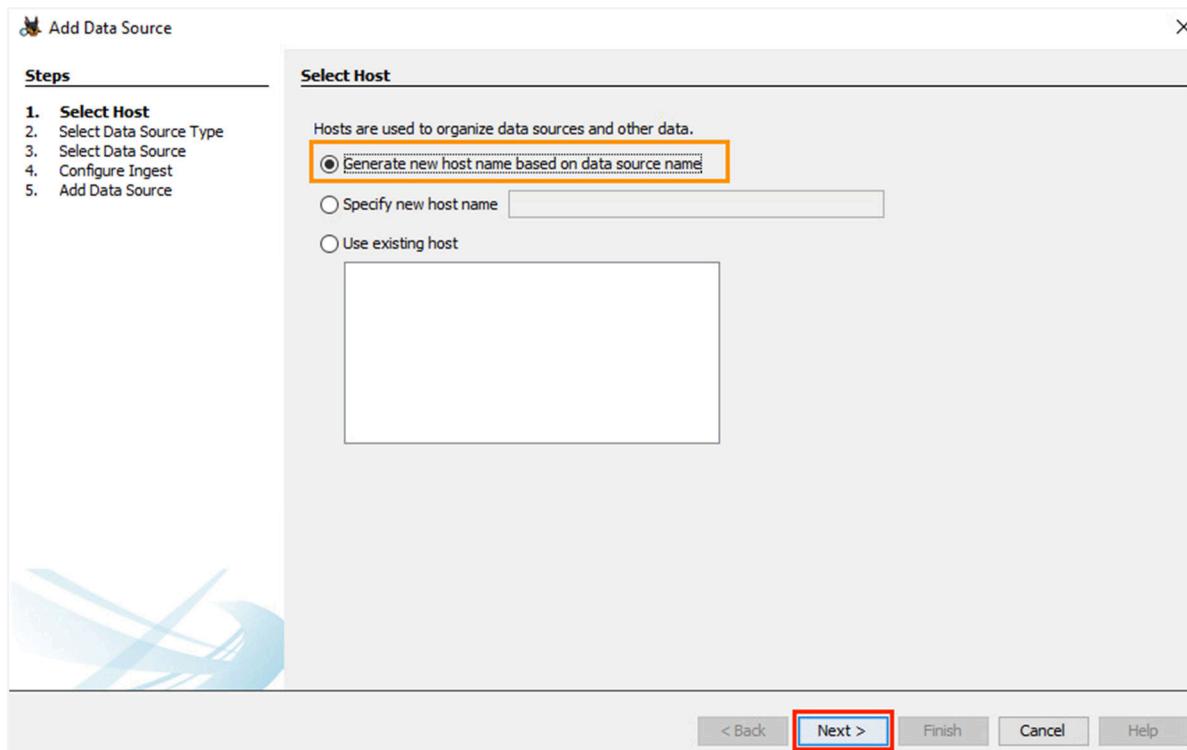
Hosts are used to organize data sources and other data.

Generate new host name based on data source name

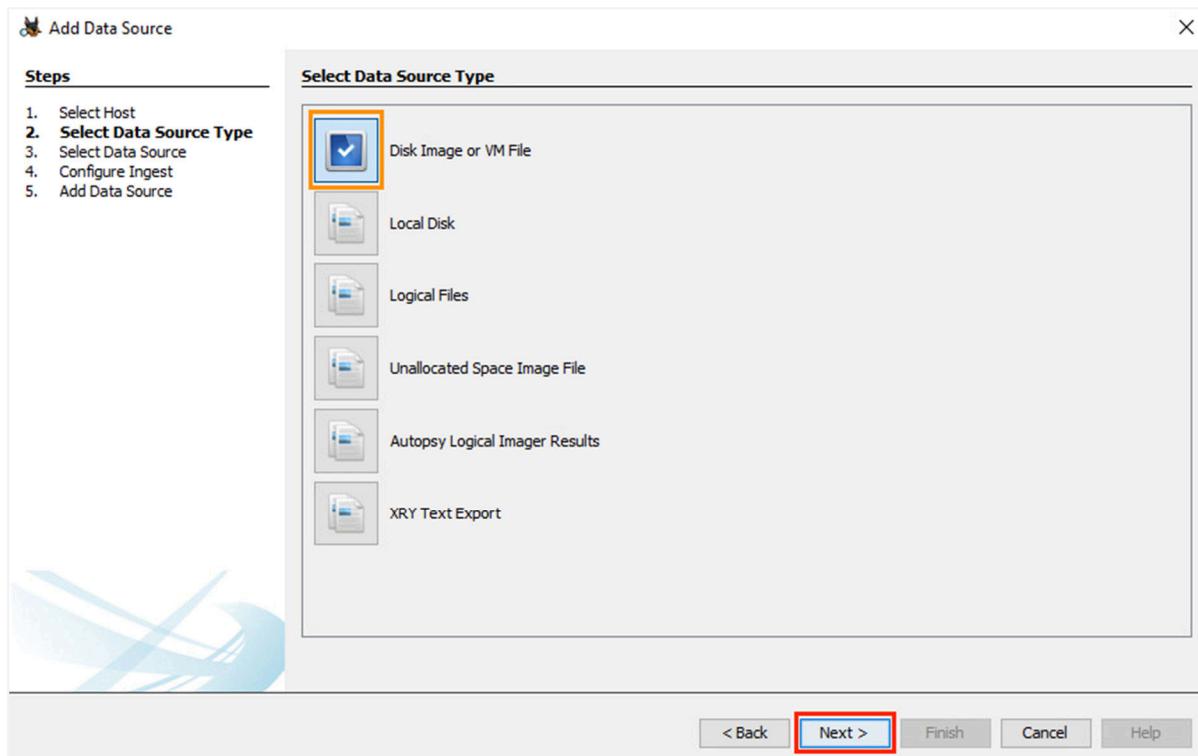
Specify new host name

Use existing host

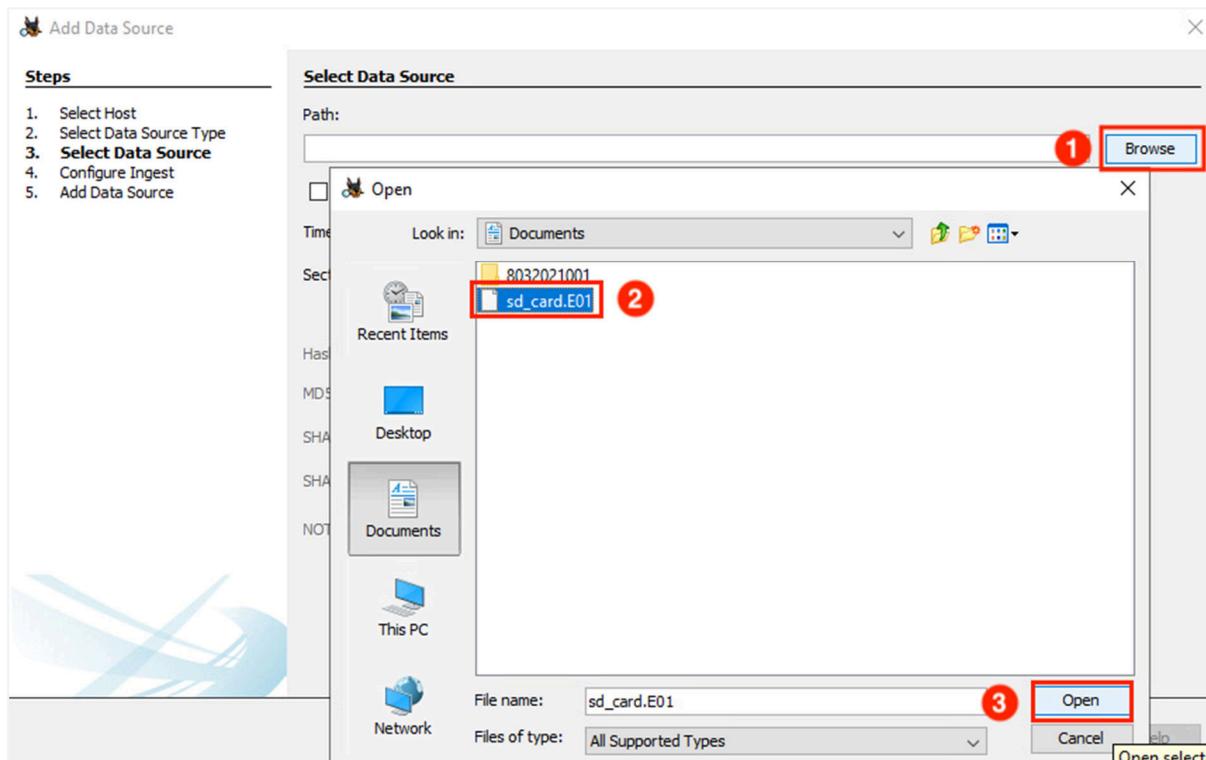
< Back **Next >** Finish Cancel Help



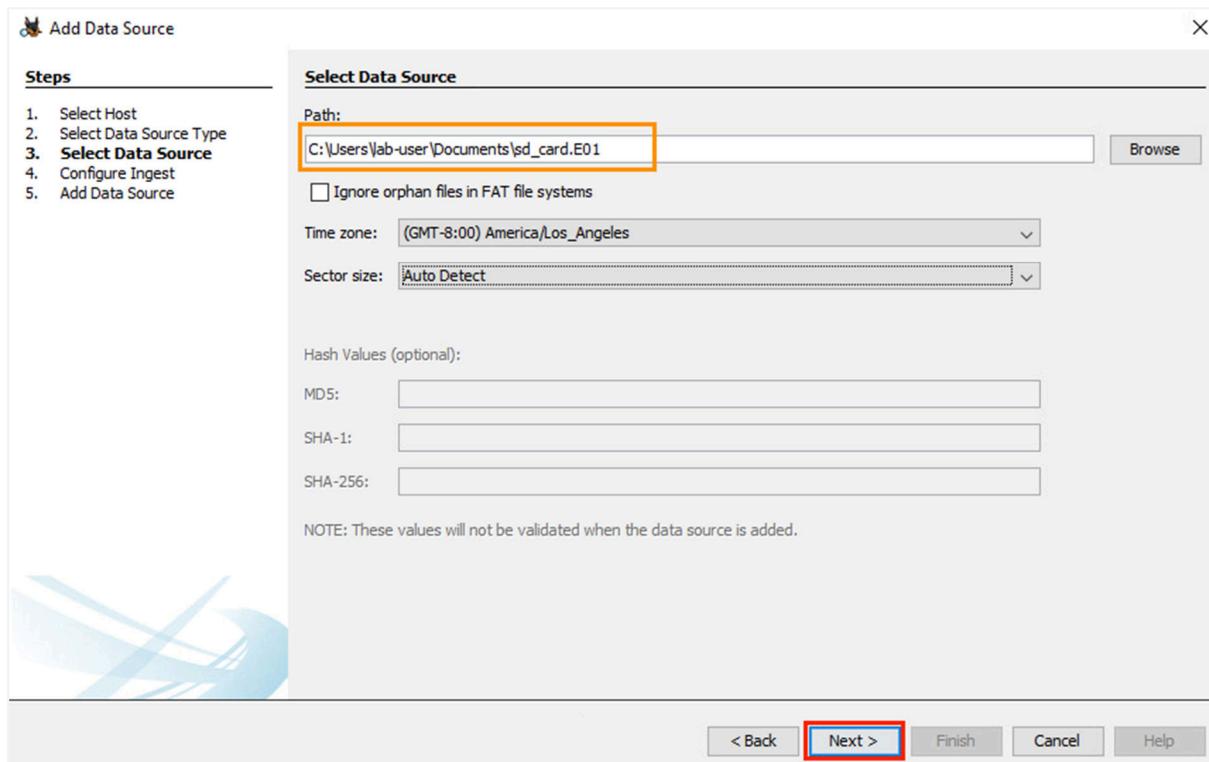
11. On the next screen, make sure the *Disk Image or VM File* option is selected and click **Next**.



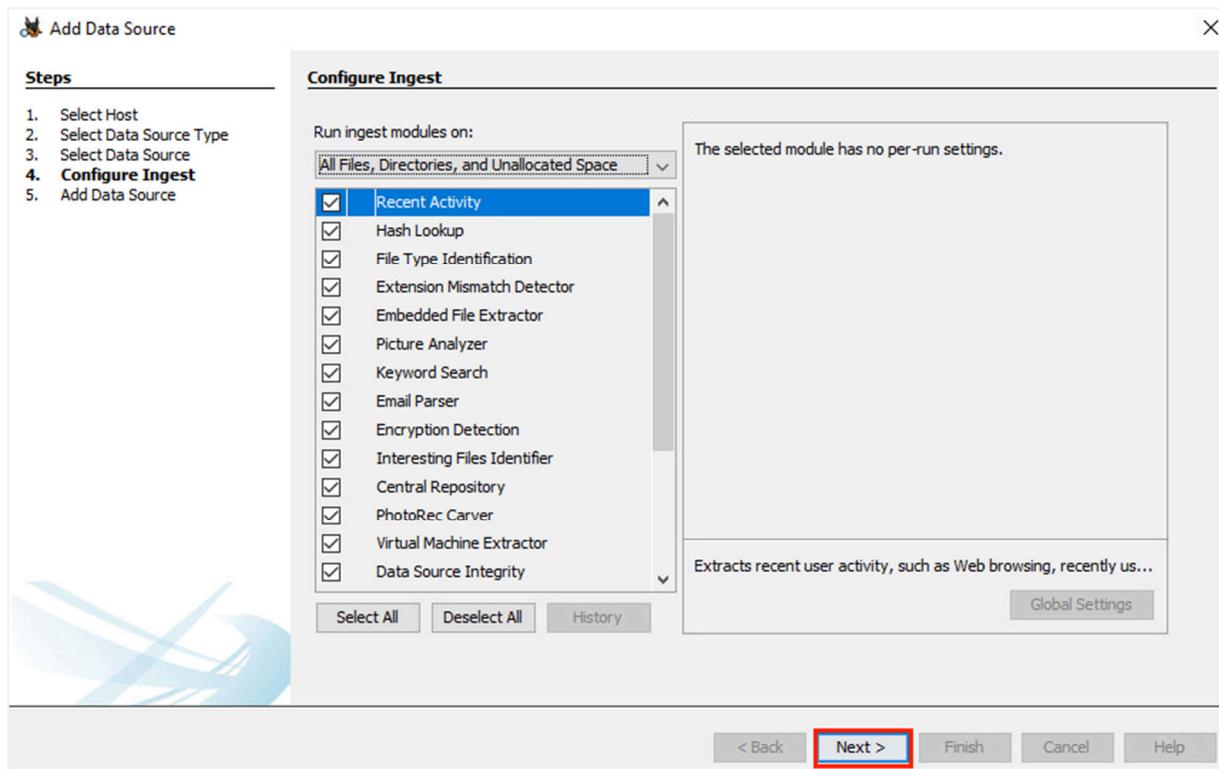
12. On the new screen, click **Browse**, then select the **sd_card.E01** file, and click **Open**.



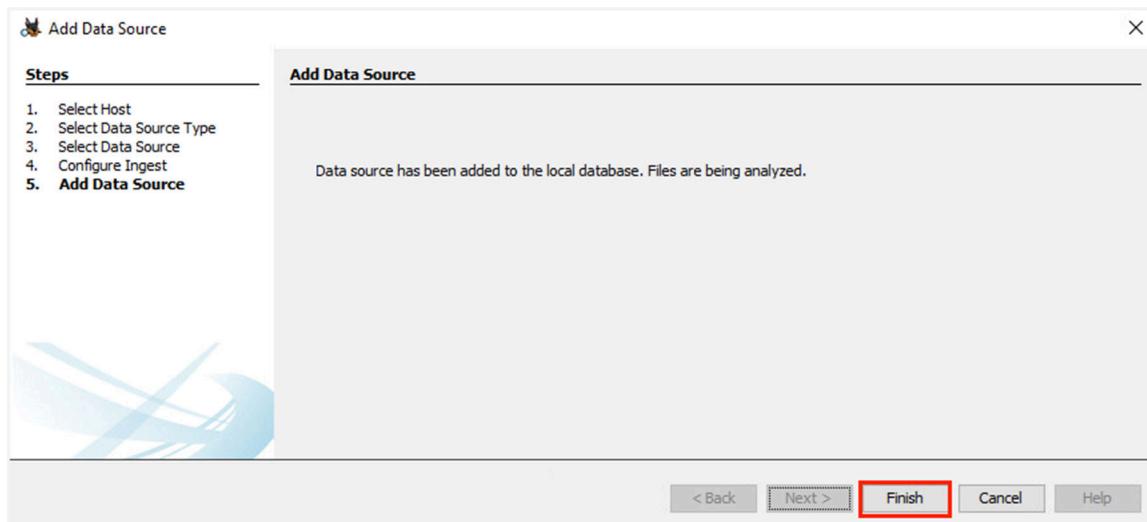
13. Review the information, then click **Next**.



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

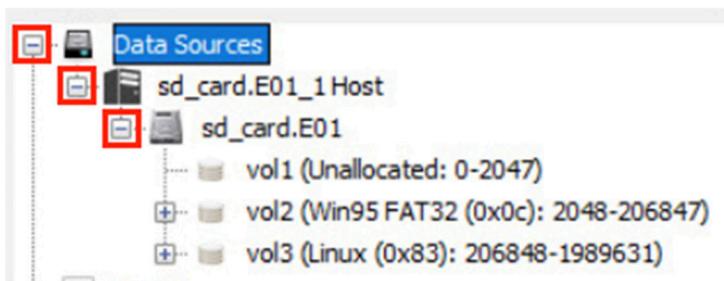
- Now, we are in the *Autopsy* software, with the image loaded as our case evidence file. Notice, in the lower-right corner, it indicates that the software is still analyzing the files found from the evidence image.



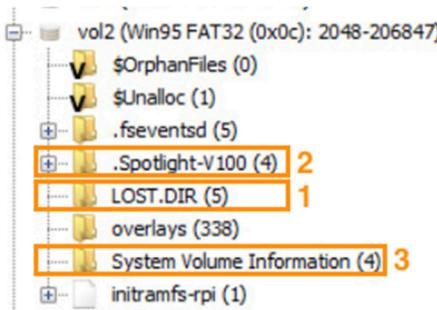
- At the top-right corner of the *Autopsy* window, click the square to maximize the window, so we get a bigger view of the program. This will help to view the files if there is a long list to display.



- 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.

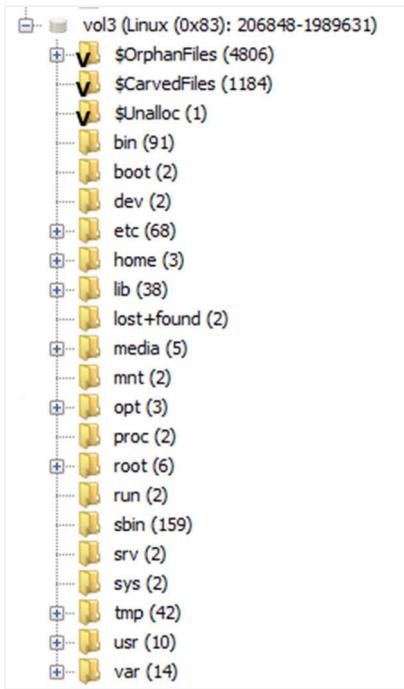


- Click the + in front of *Vol2*; we can see that the evidence was once plugged into 1)an Android device; 2) a Mac computer; 3) a Windows computer. Feel Free to expand different folders in *Vol2* to explore the files found.



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.

The screenshot shows the expanded 'home' directory under 'Vol3'. A specific folder named 'alpine (6)' is highlighted with a red box. To the right, a detailed file list table is shown for this folder:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2021-01-05 11:40:13 PST	2021-01-05 11:40:13 PST	2021-01-05 11:59:03 PST	2021-01-05 11:35:34 PST	4096	Allocated
[parent folder]				2021-01-05 11:35:34 PST	2021-01-05 11:35:34 PST	2021-01-05 10:14:54 PST	2021-01-18 13:57:41 PST	4096	Allocated
l3				2021-01-05 12:05:39 PST	2021-01-05 12:05:39 PST	2021-01-05 11:58:07 PST	2021-01-05 11:58:07 PST	4096	Unallocated
merged				2021-01-05 11:58:08 PST	2021-01-05 11:58:08 PST	2021-01-05 11:58:08 PST	2021-01-05 11:58:08 PST	4096	Unallocated
work				2021-01-05 11:58:08 PST	2021-01-05 11:58:08 PST	2021-01-05 11:58:07 PST	2021-01-05 11:58:07 PST	4096	Unallocated
.ash_history	1			2021-01-05 12:11:09 PST	2021-01-05 12:11:09 PST	2021-01-05 11:54:47 PST	2021-01-05 11:40:13 PST	62	Allocated

The bottom section of the interface shows the contents of the '.ash_history' file in a text editor. The text area contains the following command history:

```
vi /etc/motd
sudo vi /etc/motd
su
whoami
exit
su
exit
su
exit
```

A red box highlights the '.ash_history' file entry in the table, and an orange box highlights the command history text.

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.

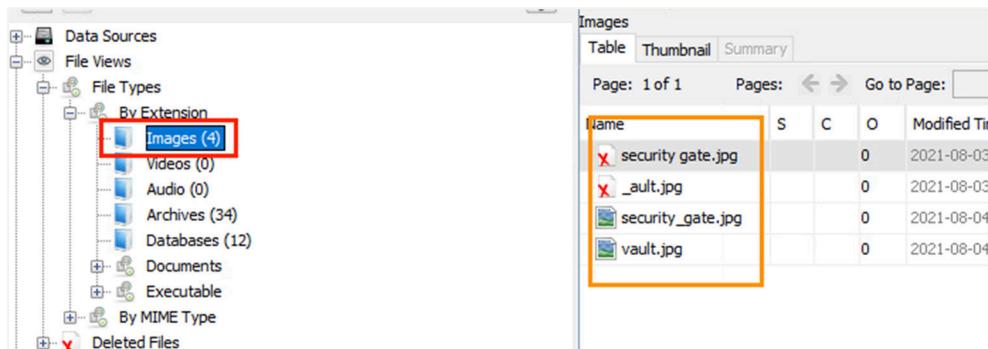
	modules	1	2020-06-19 03:32:48 PDT	2021-01-18 13:57:41 PST	2020-06-19 03:32:48 PDT	2021-01-18 13:57:41 PST
etc (68)	motd	1	2021-01-05 11:42:41 PST	2021-01-05 11:42:41 PST	2021-01-05 11:43:28 PST	2021-01-18 13:57:41 PST
	os-release	1	2021-01-14 03:48:14 PST	2021-01-18 13:57:43 PST	2021-01-05 12:10:57 PST	2021-01-18 13:57:41 PST
	passwd	1	2021-01-05 11:39:21 PST	2021-01-05 11:39:21 PST	2021-01-05 11:39:21 PST	2021-01-05 11:39:21 PST
	passwd+	1	2021-01-05 11:39:21 PST	2021-01-05 11:39:21 PST	2021-01-05 11:39:21 PST	2021-01-05 11:39:21 PST
	passwd-	1	2021-01-05 11:35:34 PST	2021-01-05 11:39:21 PST	2021-01-05 11:39:21 PST	2021-01-05 11:39:21 PST

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.

	chroot	2021-01-18 13:57:43 PST	2021-01-18 13:58:14 PST	2021-01-18 13:57:41 PST
var (14)	acpid.log	0	2021-01-05 10:01:37 PST	2021-01-05 10:01:37 PST
	dmesg	1	2021-01-05 11:37:03 PST	2021-01-05 11:37:03 PST
	docker.log	1	2021-01-05 12:05:40 PST	2021-01-05 12:05:40 PST
	messages	1	2021-01-05 12:15:00 PST	2021-01-05 12:15:00 PST
	wtmp	0	2021-01-05 10:01:35 PST	2021-01-05 10:01:35 PST

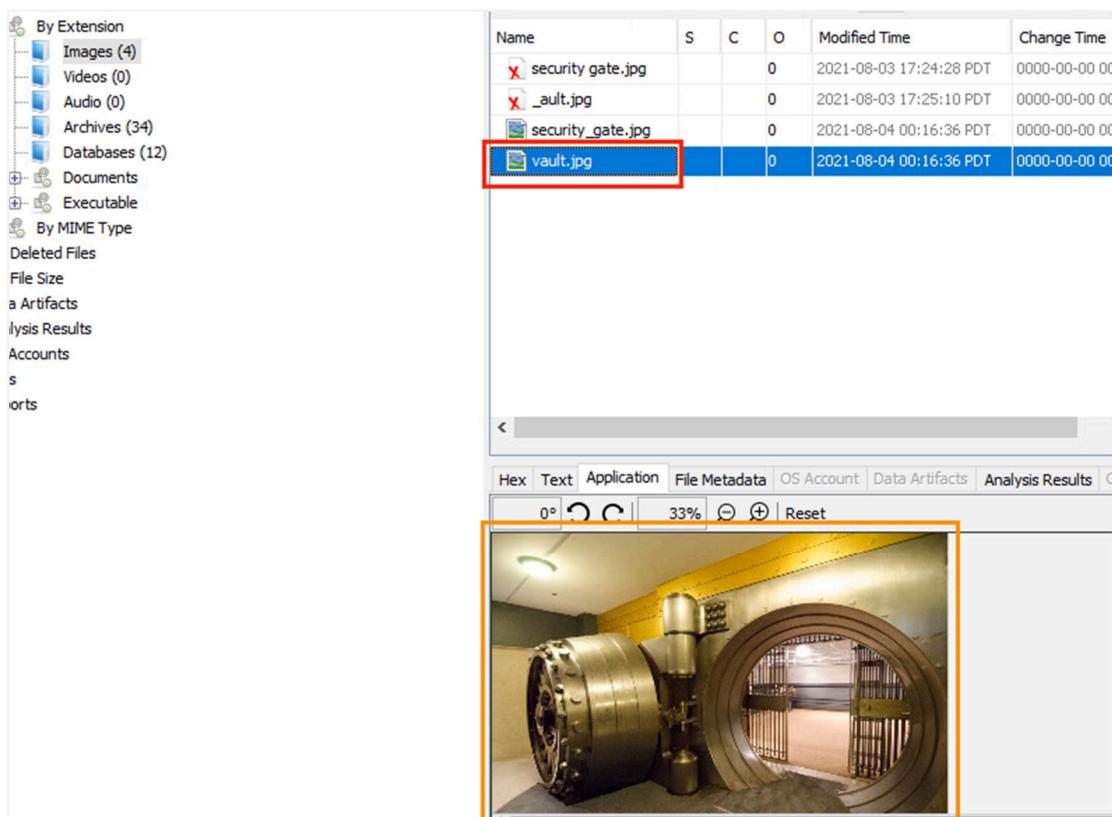
10. To the left side, scroll to the top, then click the - in front of the *Data Source* to compress the folder, so it is easier to navigate. Next, we will pay attention to the *File Views* section.

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



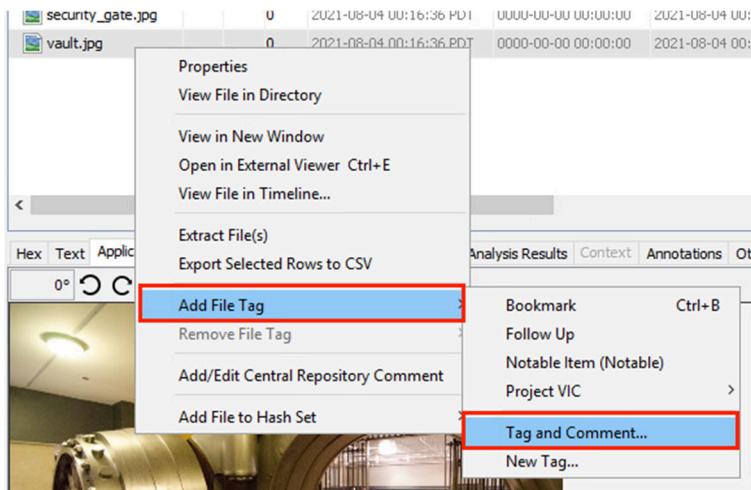
Name	S	C	O	Modified Time
security_gate.jpg		0		2021-08-03
_ault.jpg		0		2021-08-03
security_gate.jpg		0		2021-08-04
vault.jpg		0		2021-08-04

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.

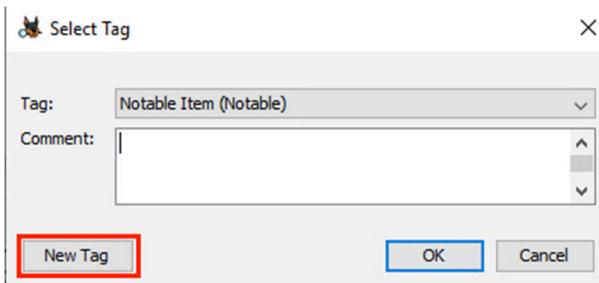


Name	S	C	O	Modified Time	Change Time
security_gate.jpg		0		2021-08-03 17:24:28 PDT	0000-00-00 00:00:00
_ault.jpg		0		2021-08-03 17:25:10 PDT	0000-00-00 00:00:00
security_gate.jpg		0		2021-08-04 00:16:36 PDT	0000-00-00 00:00:00
vault.jpg		0		2021-08-04 00:16:36 PDT	0000-00-00 00:00:00

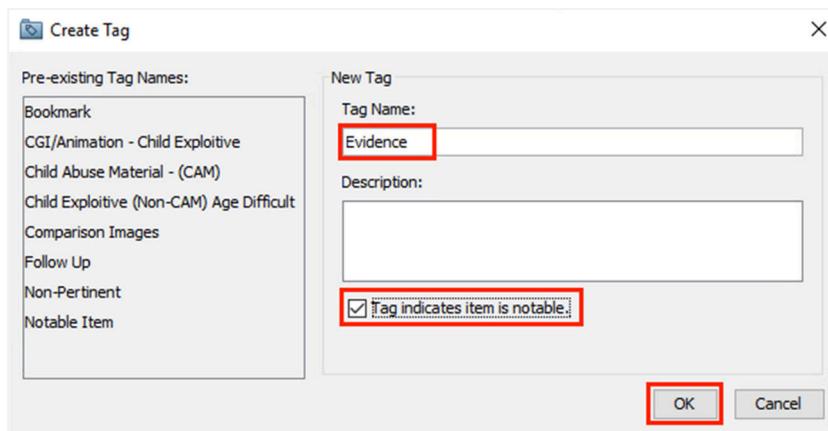
13. Right-click on **vault.jpg**, select **Add File Tag > Tag and Comment**.



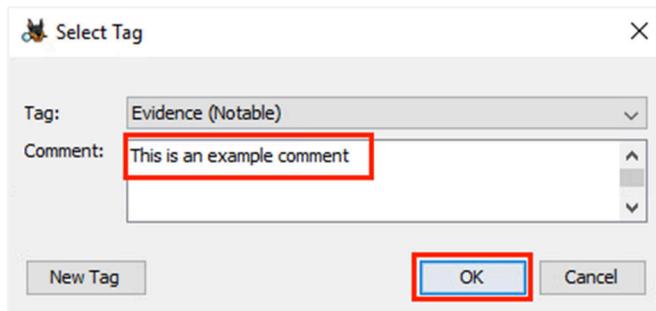
14. In the pop-up window, we are going to add a new tag. Click the **New Tag** button.



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.

A screenshot of the "File Types" section in the Autopsy interface. On the left, there's a tree view under "File Types" with categories like "By Extension" (Images, Videos, Audio, Archives, Databases), "Documents" (HTML, Office, PDF), and "Executable". The "PDF (2)" folder under "Documents" is highlighted with a red rectangular box. On the right, a preview pane shows a table with two entries: "blue_print.pdf" and "blue print.pdf". The first entry has a red checkmark icon and the number "1" in the "O" column. The second entry has a red X icon and the number "0" in the "O" column. The preview pane also shows "Page: 1 of 1" and "Pages: < > G".

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.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
blue_print.pdf		1		2021-08-04 00:16:36 PDT	0000-00-00 00:00:00	2021-08-04 00:00:00 PDT	2021-08-04 00:16:36 PDT
blue print.pdf		0		2021-08-03 17:13:52 PDT	0000-00-00 00:00:00	2021-08-03 00:00:00 PDT	2021-08-03 17:55:42 PDT

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Main floor

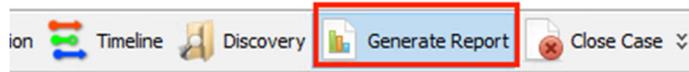
20. Repeat the tag-adding step to add tag and comments to the PDF file.

Name	S	C	O	Modified Time
blue_print.pdf		!	1	2021-08-04
blue print.pdf			0	2021-08-03

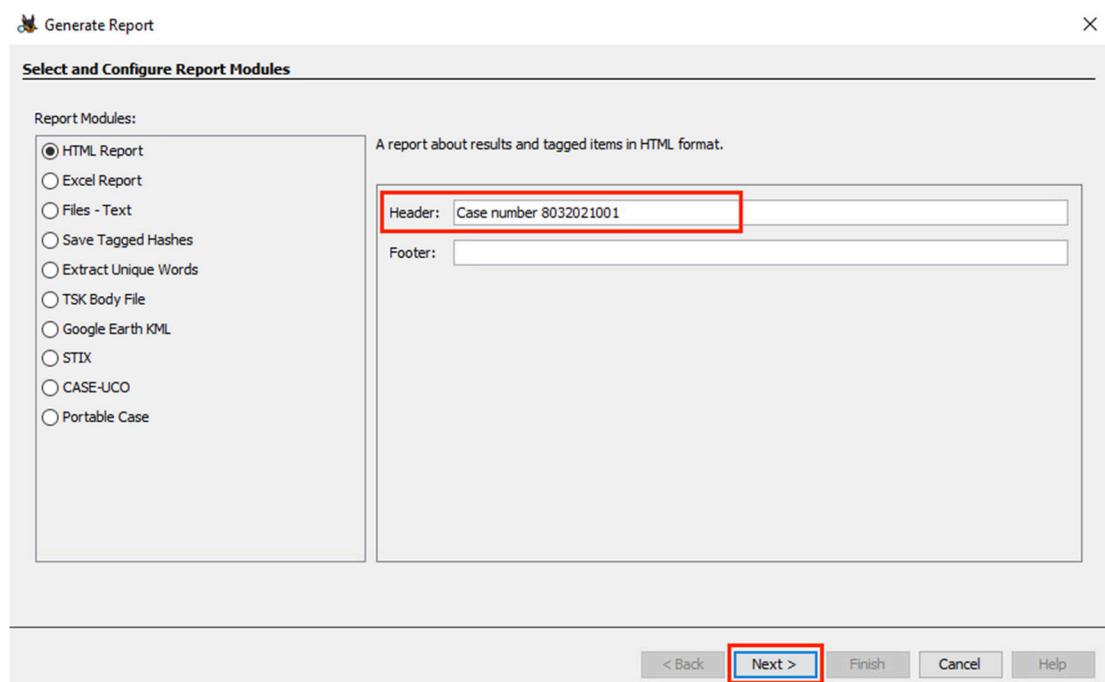
21. The investigation section is finished. Continue to the next section to generate a report.

3 Generating a Report

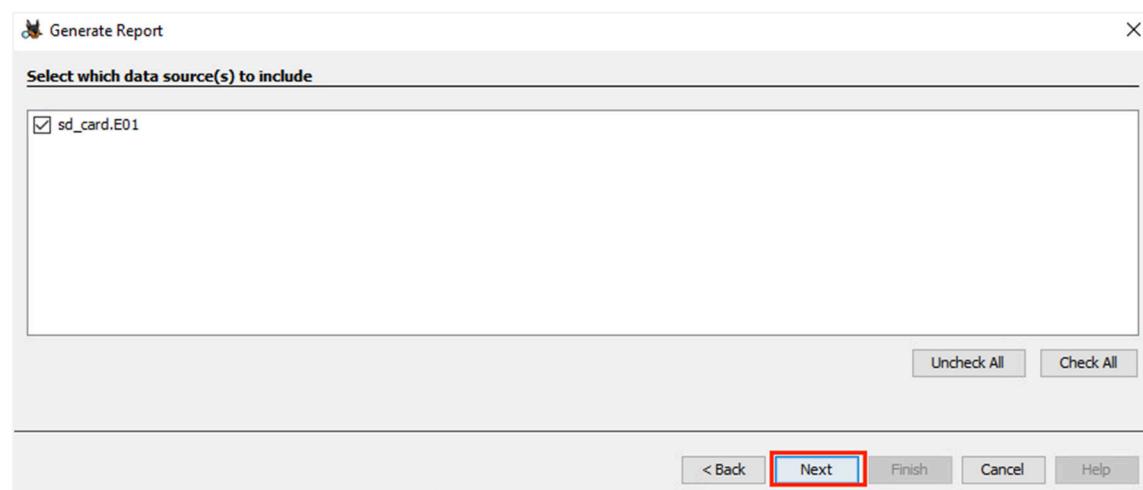
- Let's say that we did more investigation and did not find any other evidence. It is now a good time to generate the report. Click on the **Generate Report** button in the toolbar.



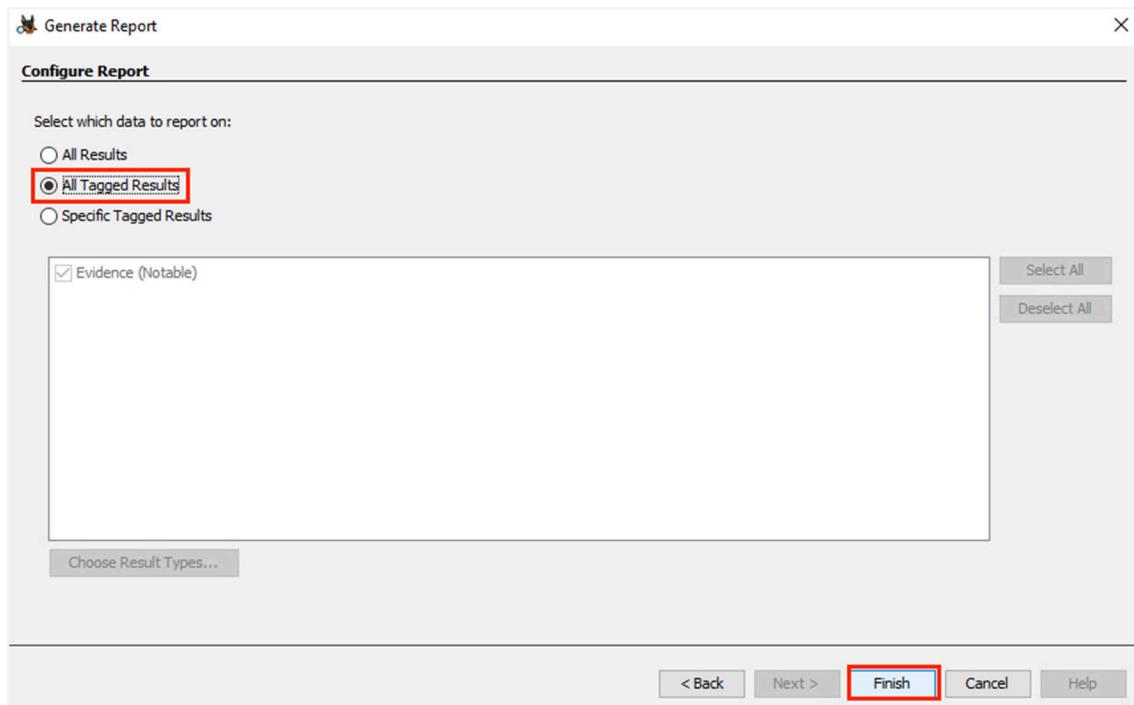
- A window will pop up, and we will be creating an HTML Report. We will put **Case number 8032021001** as our *Header* and leave the *Footer* blank. Click **Next**.



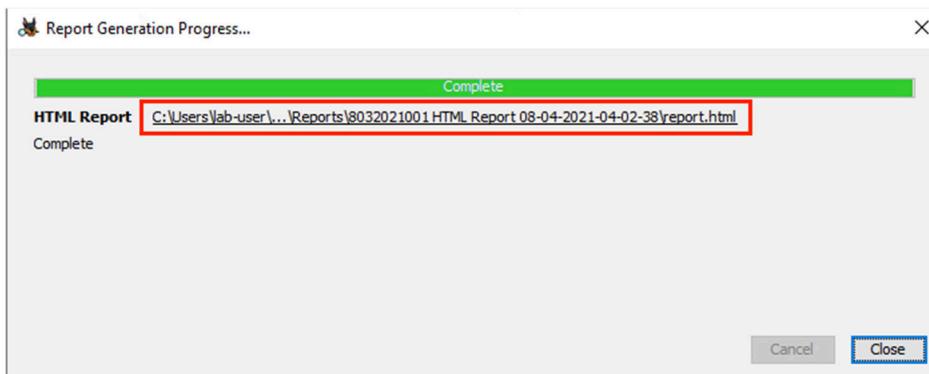
- On the *Select which data source(s) to include* step, leave the default setting, click **Next**.



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.



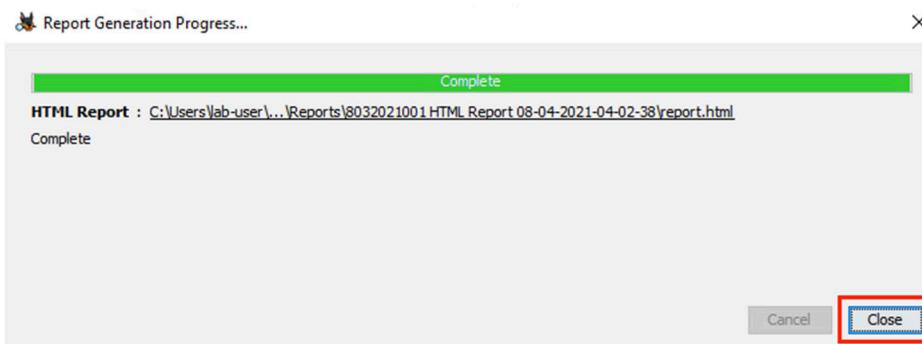
6. Feel free to scroll down and explore the HTML report. The previously tagged files will be pulled out as the evidence image. You can check them by clicking on the **Tagged Files** link on the left side of the page.

The screenshot shows the Autopsy Forensic Report interface. On the left, a sidebar titled "Report Navigation" lists "Case Summary", "Keyword Hits (0)", and three items under "Tagged Files": "Tagged Files (3)" (highlighted with an orange box), "Tagged Images (2)", and "Tagged Results (0)". The main content area displays the "Autopsy Forensic Report" for Case number 8032021001, generated on 2021/08/04 04:02:38. The report details include:

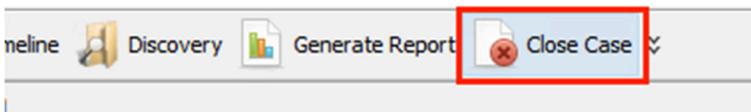
Case:	8032021001
Case Number:	8032021001
Number of data sources in case:	1
Notes:	SD card evidence inspection
Examiner:	Will Smith

Below this, sections for "Image Information" (listing "sd_card.E01") and "Software Information" (listing Autopsy Version 4.19.0, Android Analyzer Module 4.19.0, and Android Analyzer (aLEAPP) Module 4.19.0) are shown.

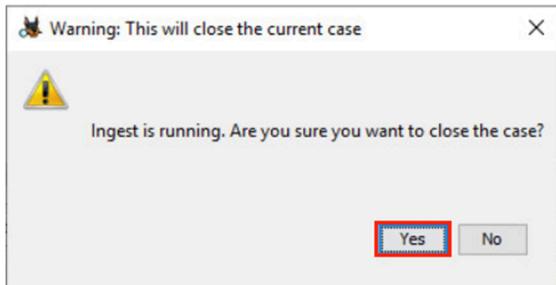
7. Close the browser window. Then close the report generation window.



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.