Mobile Forensics

Module 13

Mobile Forensics

Mobile forensics is a methodical series of techniques and procedures for gathering evidence from mobile devices and digital media to present in a court of law in a coherent and meaningful format.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

Catherine, an incident handling manager in a brokerage firm, was notified of shares purchase at quite high prices by the firm. As an incident manager, she suspected a cyber crime and reported this to the FBI. Catherine mentioned that her accounts were also suspended due to non-payment toward the shares purchase.

A team of cybercrime investigation experts visited the firm and started their initial investigation. Later, the team found some unknown persons had hacked mobile devices that were involved in purchasing the shares at higher prices using software from the firm's network. The experts identified one person by the mobile device address utilized in the purchase as well as the service used.

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 13 Mobile Forensics

Lab Objectives

The objective of this lab is to offer complete information on mobile forensics. The tasks include viewing the mobile information messages, call logs, contact list, etc.

Lab Environment

In this lab, you need:

- A computer running **Windows 2012 virtual machine**
- A web browser with an **Internet** connection
- Administrative privileges to run the tools

Lab Duration

Time: 40 Minutes

Overview of Mobile Forensics

The need for mobile forensics has increased due to the prevalence of mobile devices, resulting in a large amount of electronic evidence. The fundamental objectives of mobile forensics are to preserve, identify, extract, document, and interpret the electronic data. It is always recommended to outline and define policies and procedures to be followed to carry out analysis for mobile forensics. Data must be retrieved and analyzed without causing any damage and ensuring its authenticity.

TASK 1

Lab Tasks

Overview

Recommended labs to assist you in mobile forensics:

- Analyzing the Forensic Image and Carving the Deleted Files Using **Autopsy**.
- Extracting the Databases of an Android Mobile Device Using **Andriller**.

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Analyzing the Forensic Image and Carving the Deleted Files Using Autopsy

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. You can even use it to recover photos from your camera's memory card.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

File carving is the process of obtaining deleted information from a hard disk or an image in the absence of the Filesystem that originally created the file. It is a forensic technique that involves recovering of files from unallocated clusters by using file signatures. File carving comes into effect during the process of investigation on a suspect device which might contain information related to terrorist activities, sexual harassments, etc. In such cases, file carving helps you in recovering deleted pictures, videos, and other file types which contain crucial information.

Being a mobile forensics expert, you need to have sound knowledge of carving data from hex codes and various file types.

Lab Objectives

In this lab, you will learn how to:

- Analyze an image and acquire the deleted files from it

Lab Environment

This lab requires:

- A **Windows Server 2012** virtual Machine.
- Autopsy located in **C:\CHFI-Tools\CHFIv9 Module 13 Mobile Forensics\File Carving Tools\Autopsy**.
- An Android device's Image file which is in E01 format.

- Administrative Privileges to run the tool.

Lab Duration

Time: 25 Minutes

Overview of the Lab

- Install and launch Autopsy
- Create a new case
- Attach the image file and analyze it

Lab Tasks

Note: You will be performing Forensic Image analysis on an image named **LG Device Image.E01** provided in the location **C:\CHFI-Tools\CHFIv9 Module 13 Mobile Forensics\Imaging Tools\AccessData FTK Imager\Images**.

TASK 1

Install Autopsy

1. Logon to Windows Server 2012 virtual machine.
2. Before beginning this lab, you need to create a folder named **Autopsy** on **Desktop**.
3. Navigate to **C:\CHFI-Tools\CHFIv9 Module 13 Mobile Forensics\File Carving Tools\Autopsy**, double-click **autopsy-4.0.0-64bit.msi** and follow the wizard-driven installation steps to install the application.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

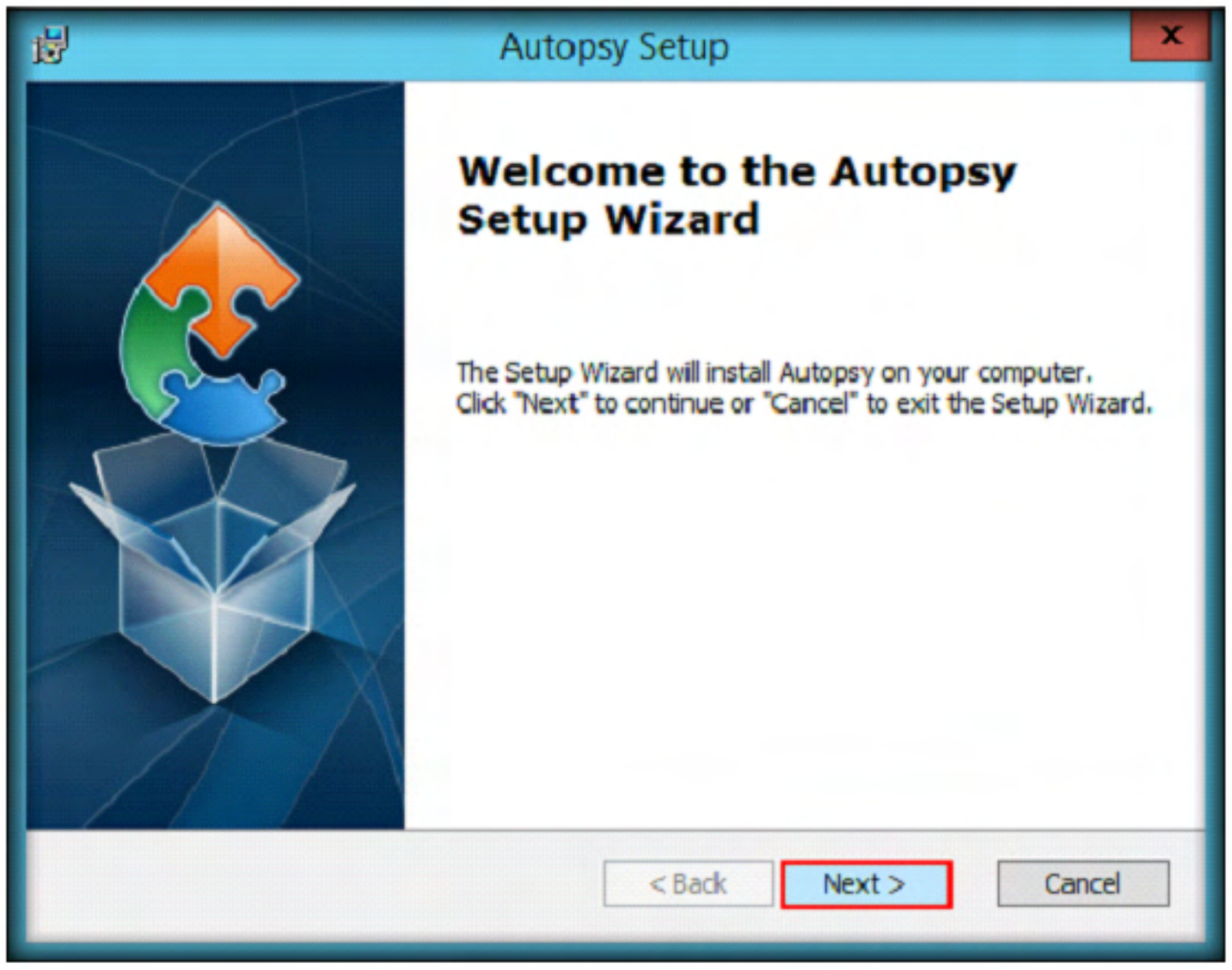


FIGURE 1.1: Autopsy Installation Wizard

4. On completing the installation, double click **Autopsy 4.0.0** icon on desktop.

FIGURE 1.2: Launching Autopsy from desktop

TASK 2

Create an Image

5. **Autopsy** main window appears along with **Welcome** dialog-box, click **Create New Case** icon to create a new case.

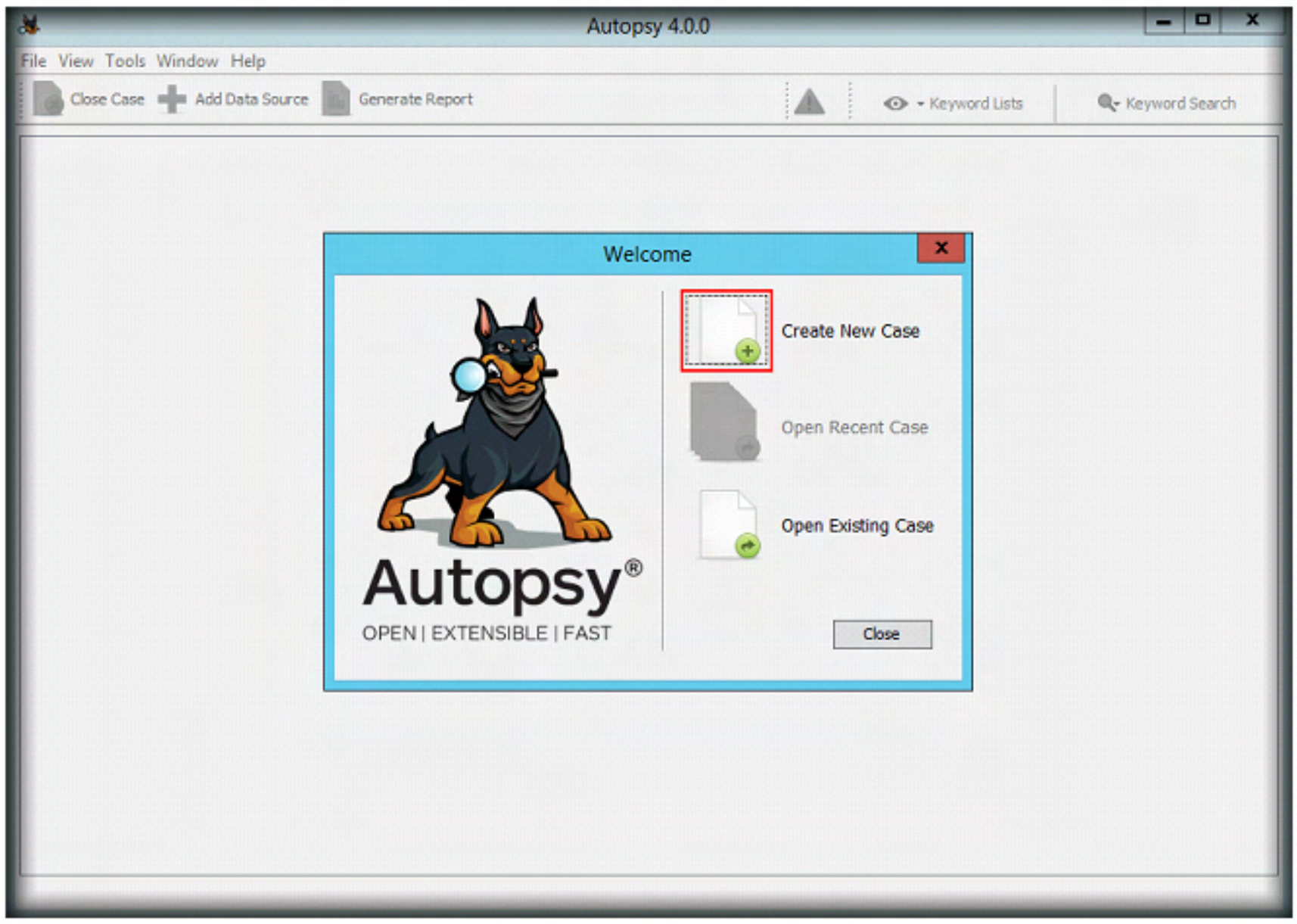


FIGURE 1.3: Autopsy Welcome dialog-box

6. **New Case Information** window appears; enter a case name (here, **LG Image Analysis**) in the **Case Name** text field and click **Browse** button to provide a path for the **Base Directory**.

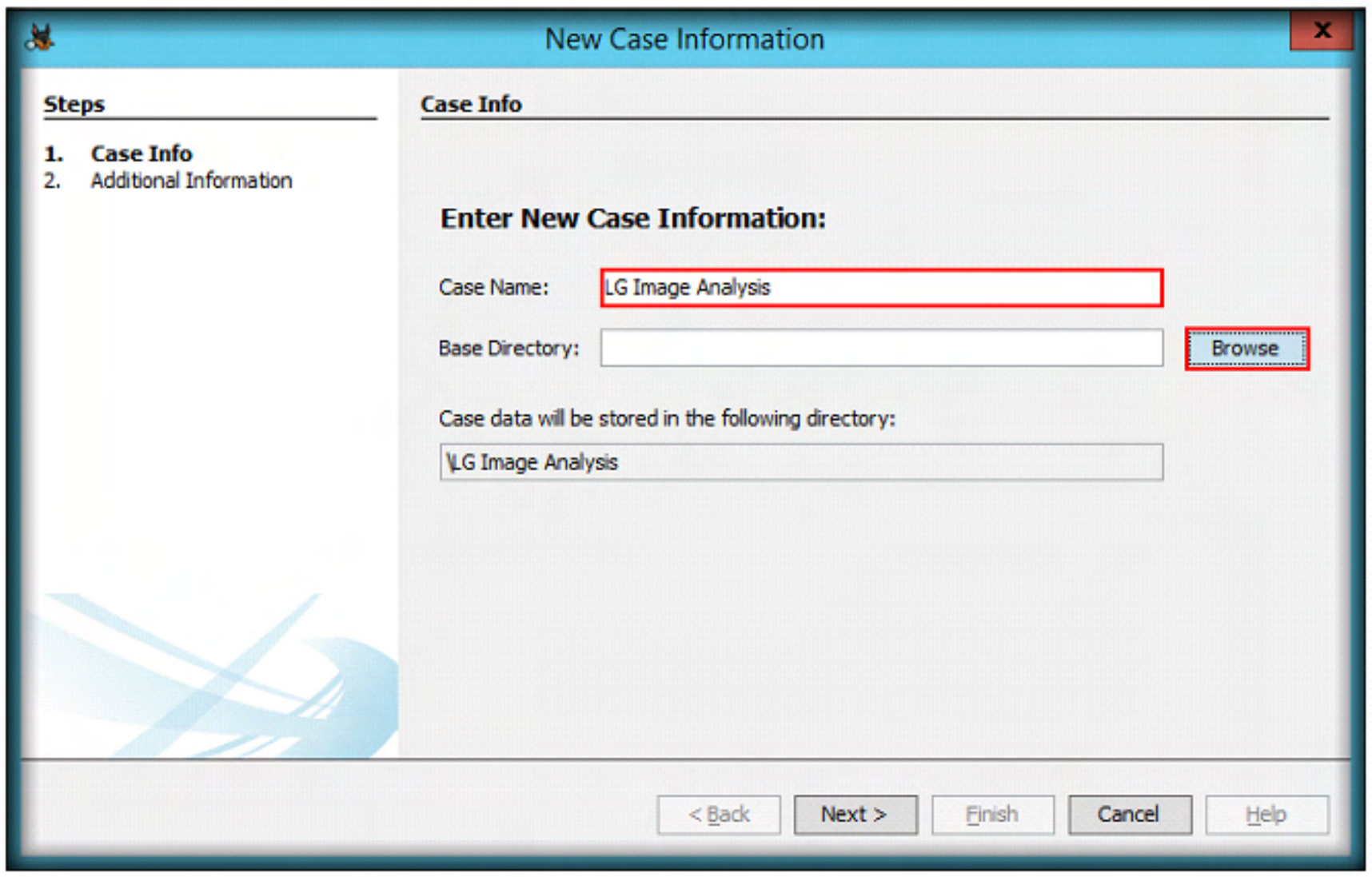


FIGURE 1.4: New Case Information window

7. A **Select** window appears, navigate to **Desktop**, select **Autopsy** folder and click **Select**.

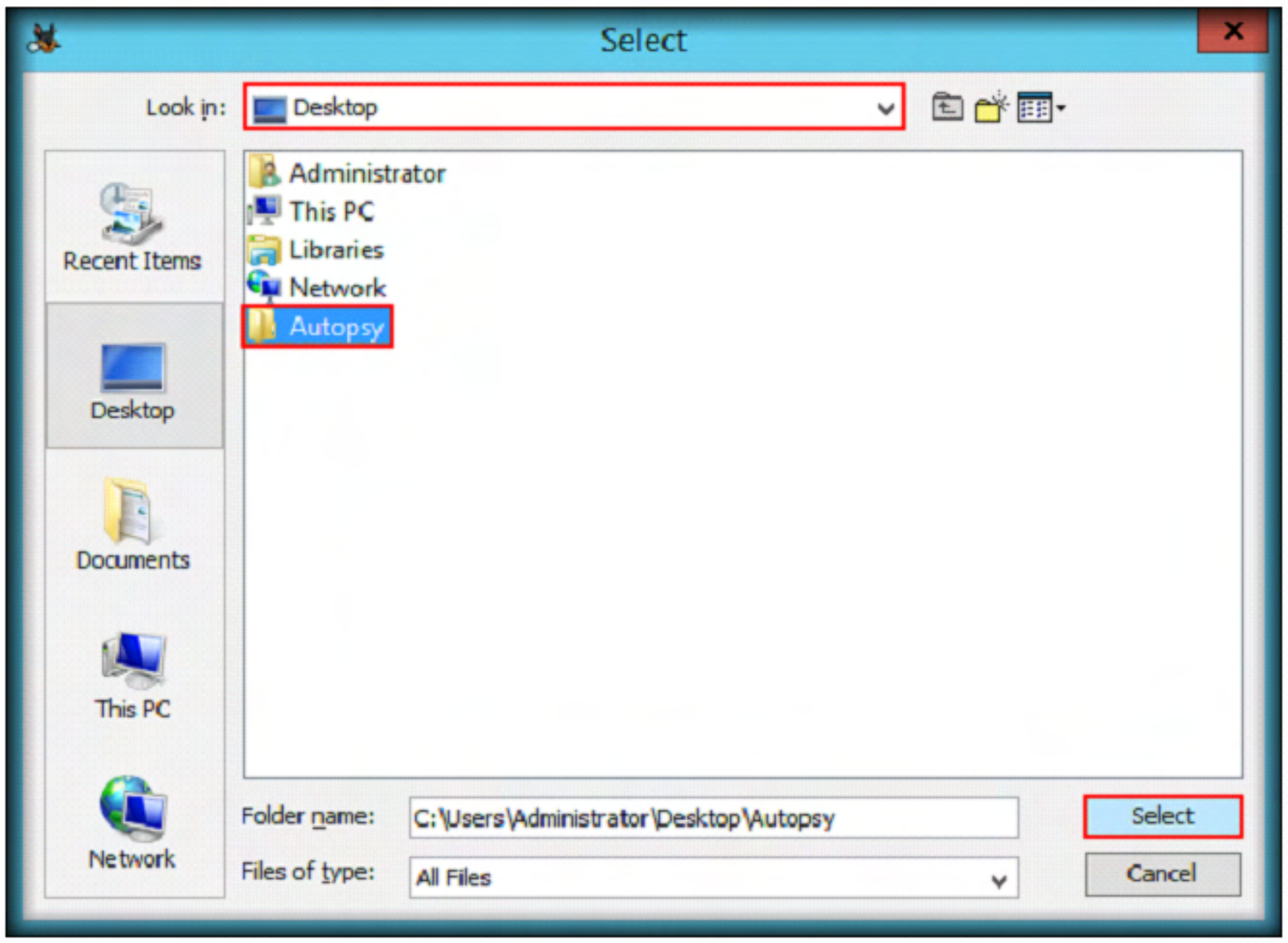


FIGURE 1.5: Select Window

8. After setting the **Base Directory**, click **Next**.

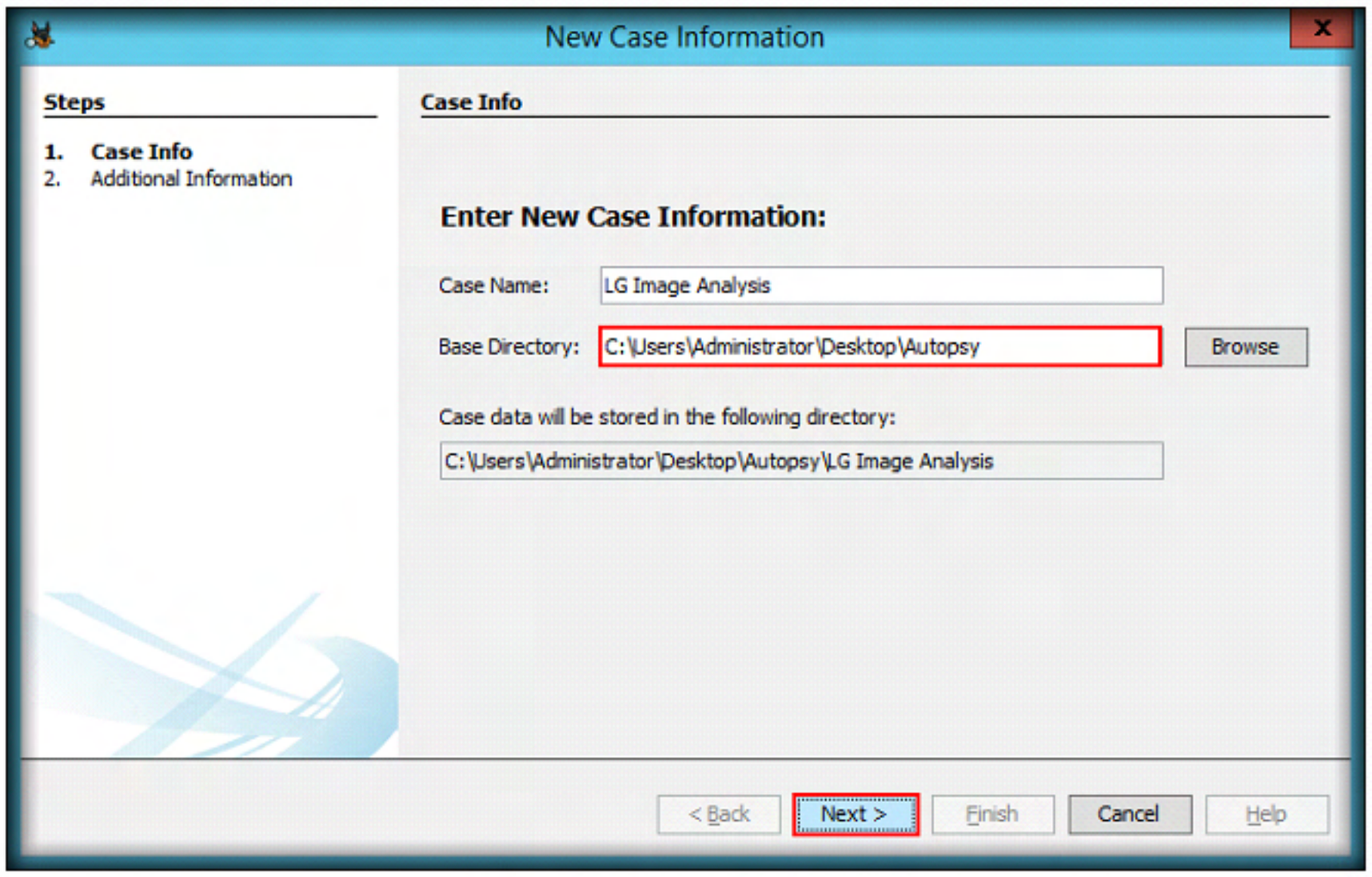


FIGURE 1.6: Setting Base Directory

9. **Additional Information** section appears, enter the **Case Number** as **01**, the name of the **Examiner** (here, **Jason**), and click **Finish**.

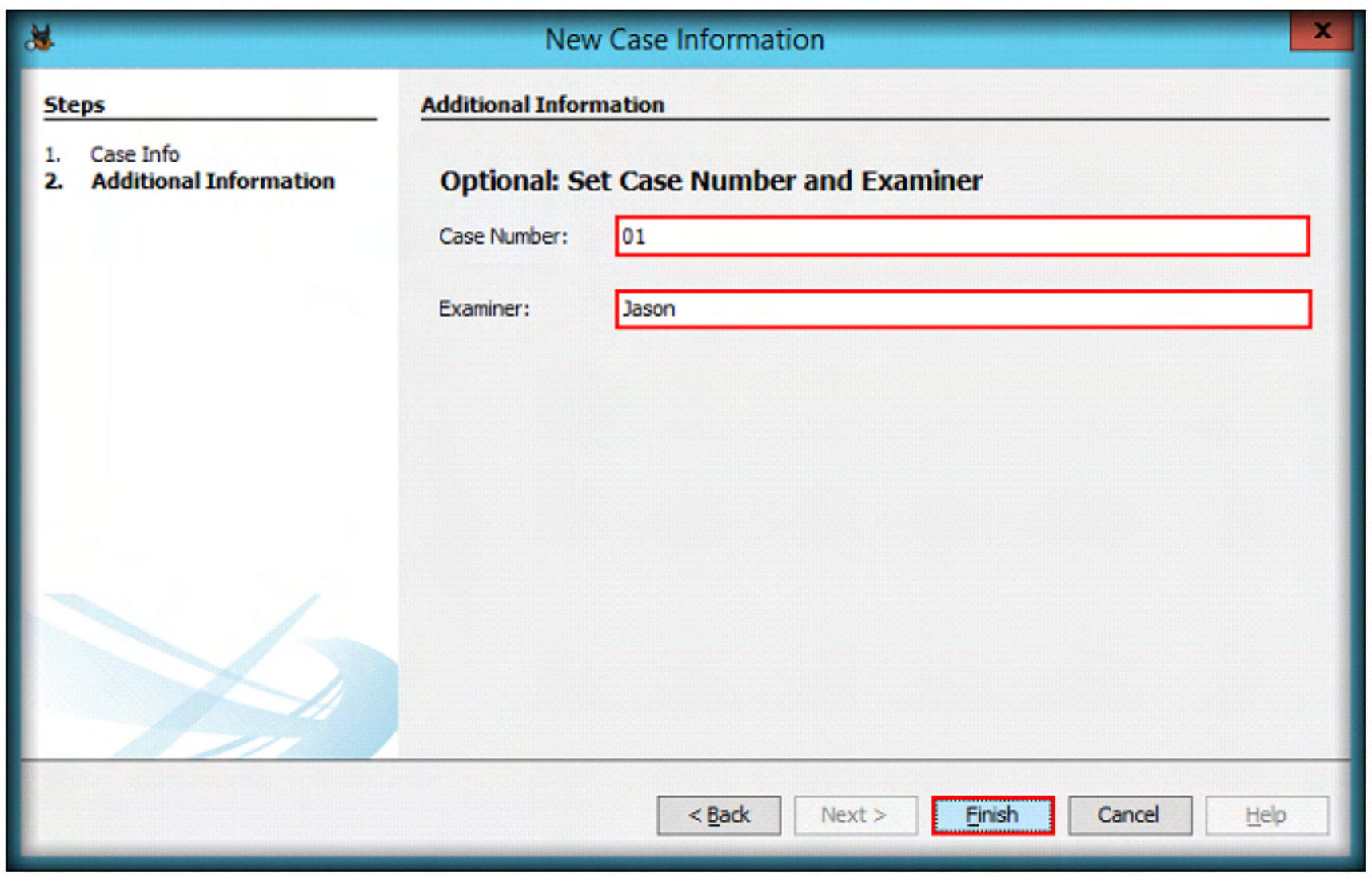


FIGURE 1.7: Additional Information section

10. Once you click Finish, **Add Data Source** window appears after some time, pointing to the **Enter Data Source Information** section.

11. Select the source type as **Image File** from the **Select source type to add** drop-down list, browse the location of the image file (**C:\CHFI-Tools\CHFIv9 Module 13 Mobile Forensics\Imaging Tools\AccessData FTK Imager\Images**) and select the image (**LG Device Image.E01**). Click **Next**.

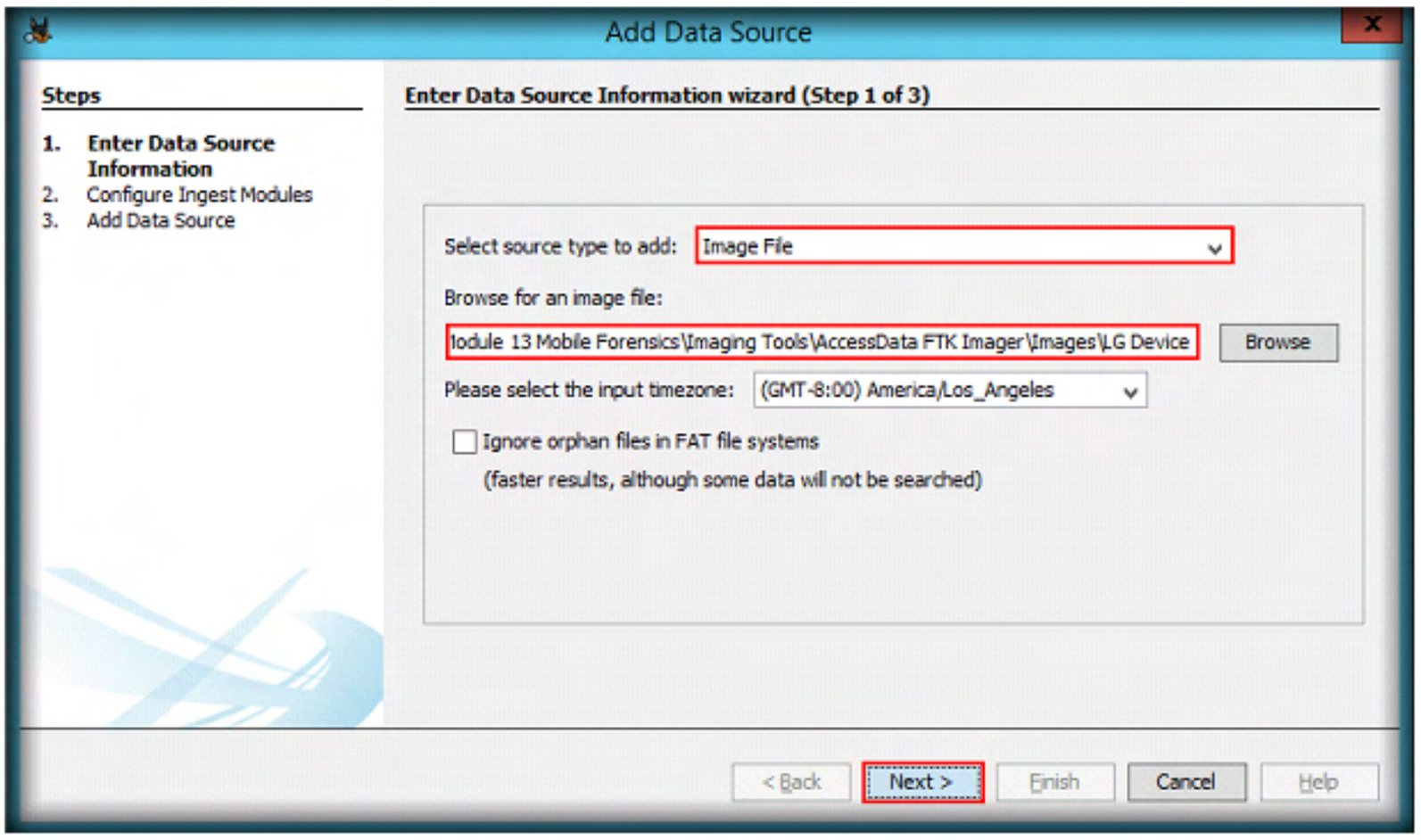


FIGURE 1.8: Enter Data Source Information wizard

12. **Configure Ingest Modules** section appears; ensure to check all the modules.

13. Later, select each module in the left pane, and their associated keywords appear in the right pane.

14. Ensure to check all the keywords for each selected module, and click **Next**.

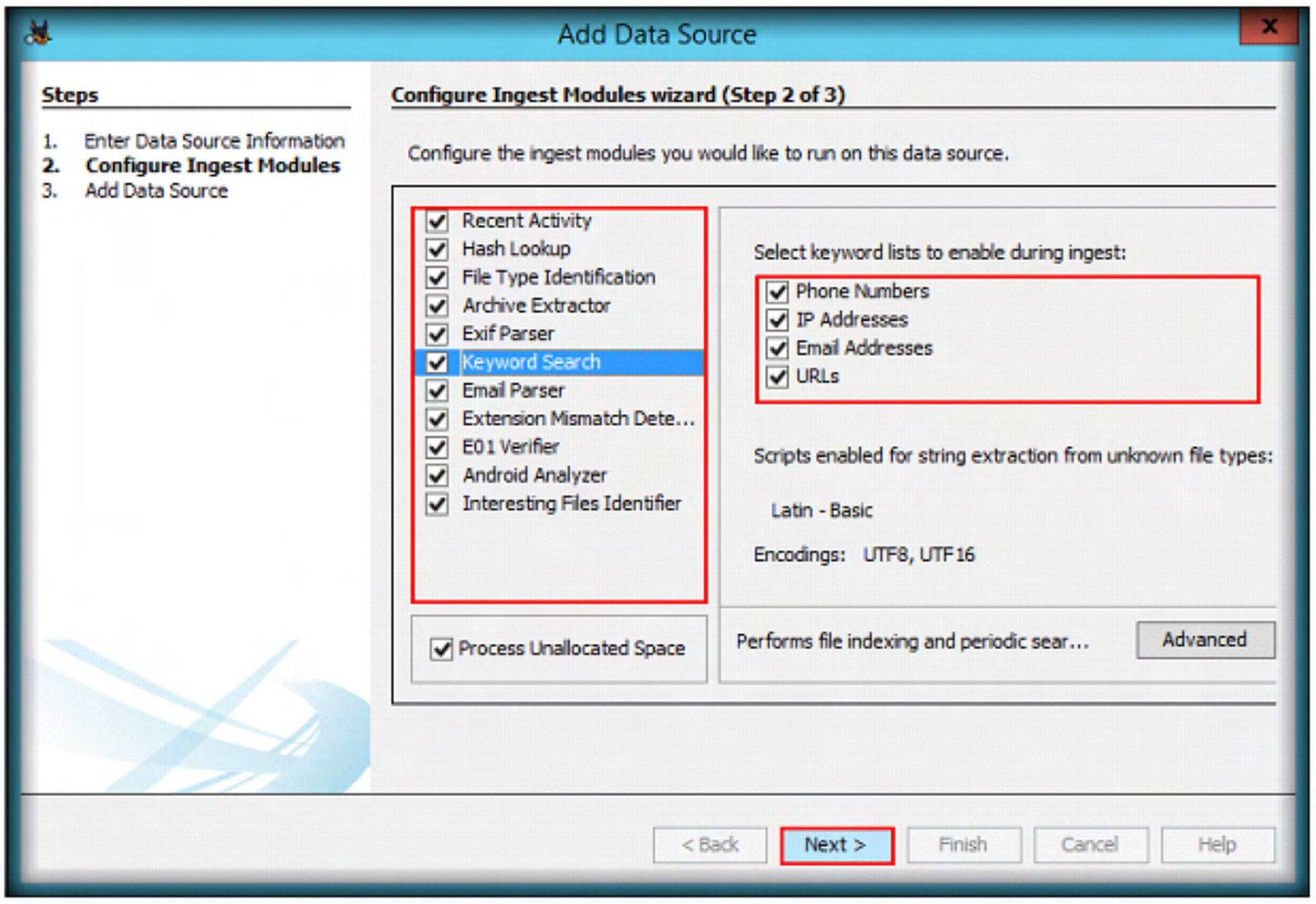


FIGURE 1.9: Configure Ingest Modules wizard

15. Autopsy begins to analyze the files in the image file.
16. **Add Data Source** wizard appears, click **Finish**.

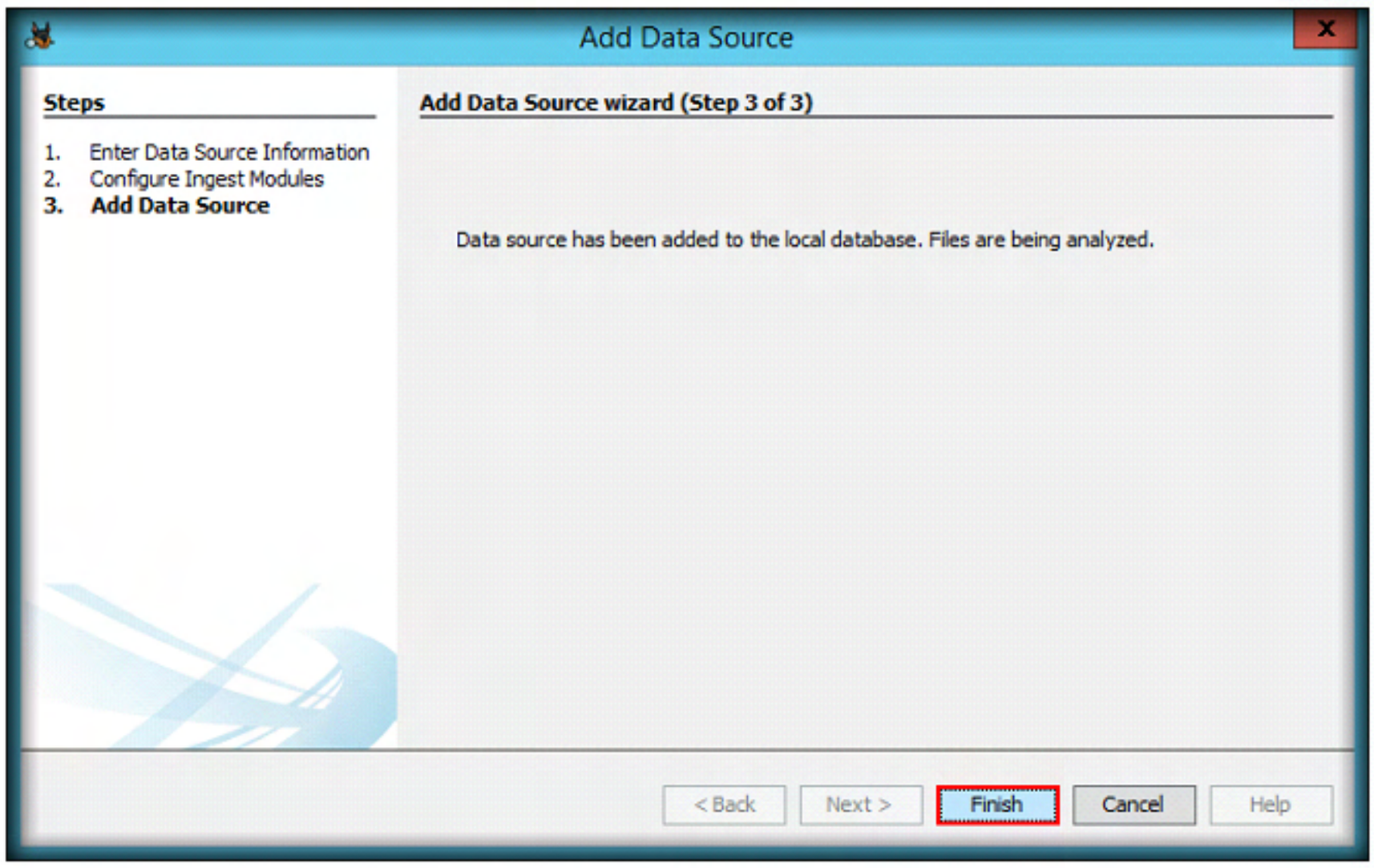


FIGURE 1.10: Add Data Source wizard

Note: Wait until Autopsy completes analyzing the image file. View the status at the lower right corner of the Autopsy Window. Once the Analysis is complete, the status disappears.

17. After analyzing all the files, autopsy displays the retrieved information as shown in the following screenshot:

Note: The screenshots and output may vary in your lab environment.

TASK 3

Examine the Image

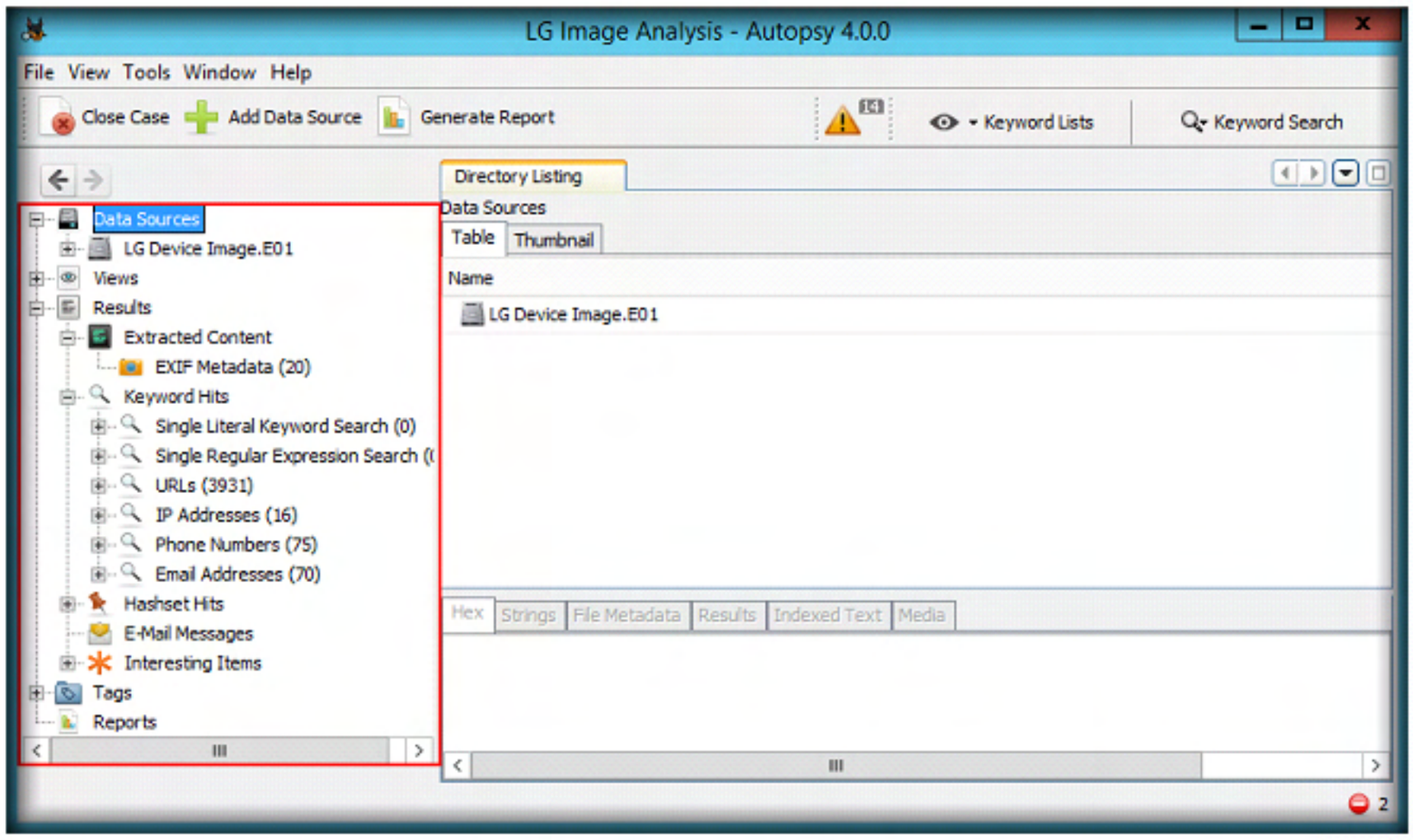


FIGURE 1.11: Information retrieved by Autopsy

18. In the left pane, expand the **Keyword Hits → Email addresses** node and select an **Email Address**. This displays important information related to the Email Address's resultant source file, keyword preview, modified time, file path, etc.

19. Autopsy even displays the **hex** data, **strings**, **metadata**, **indexed text** and **results** associated with the email address.

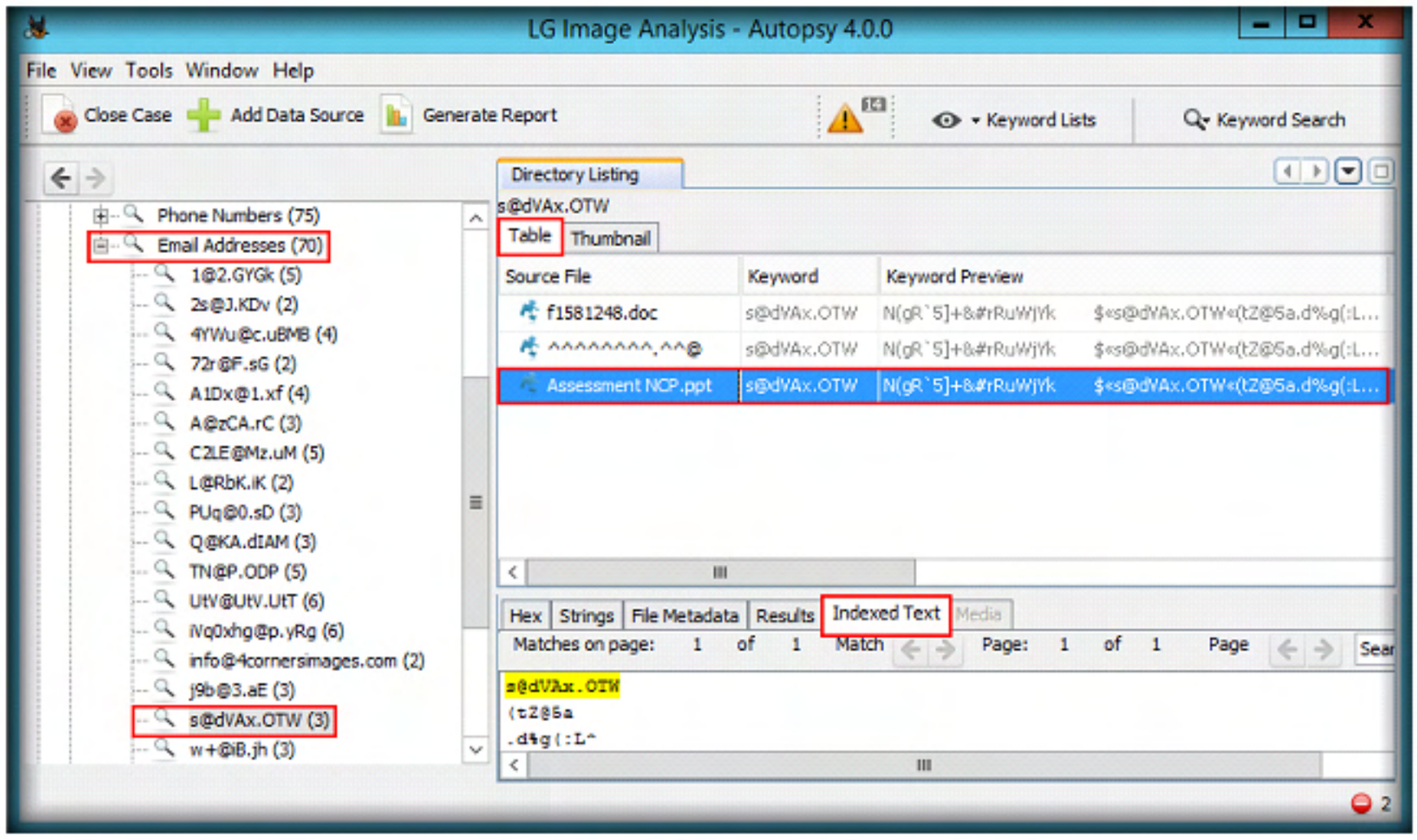


FIGURE 1.12: Information related to an email address

20. You may analyze this data to find any sensitive information hidden in the file.

21. The **URLs** node lists all the URLs contained in the image file.

22. Expand **URLs** node and select a URL from the list.

23. The files related to the URL are displayed in the right pane of the autopsy window. Select each file in the right pane, and you will be provided with the metadata, hex data, text, etc. associated with the file as shown in the following screenshot:

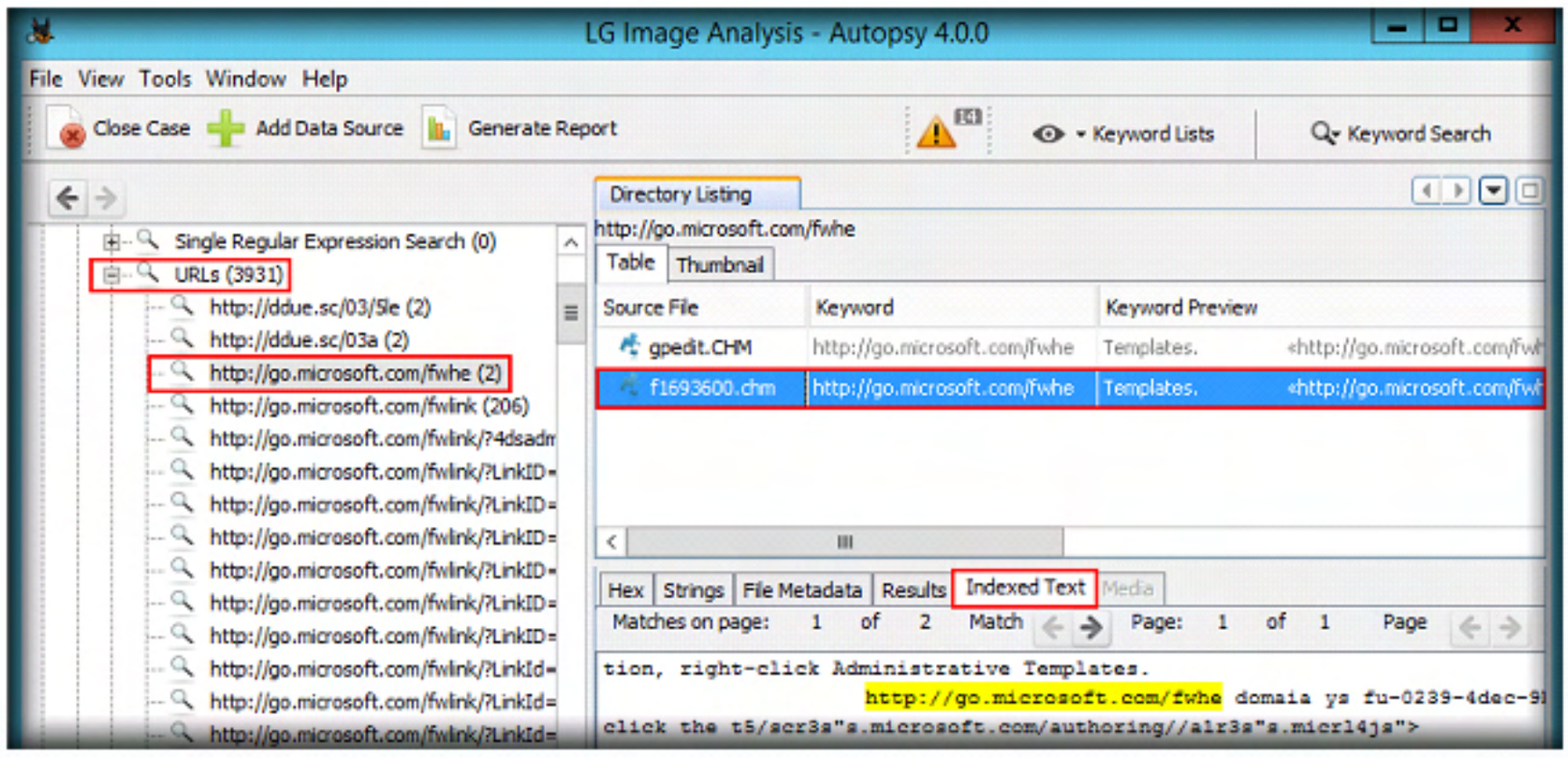


FIGURE 1.13: Information related to a URL

24. You may analyze this data to find sensitive information (if any) hidden in the file.
25. Autopsy has a feature to detect extension mismatched files in **Extension Mismatch Detected** section under **Results → Extracted Content** in the left pane. This displays the extension mismatched files.

TASK 4

Examine the Carved Files

26. Expand **Views → Deleted Files → All** in the left pane. Autopsy displays all the deleted files that have been recovered (File carving), in the right-pane. These files are indicated by a red coloured cross mark.
27. Select a carved file in the right pane to view its associated media, text, hex, string and other information.

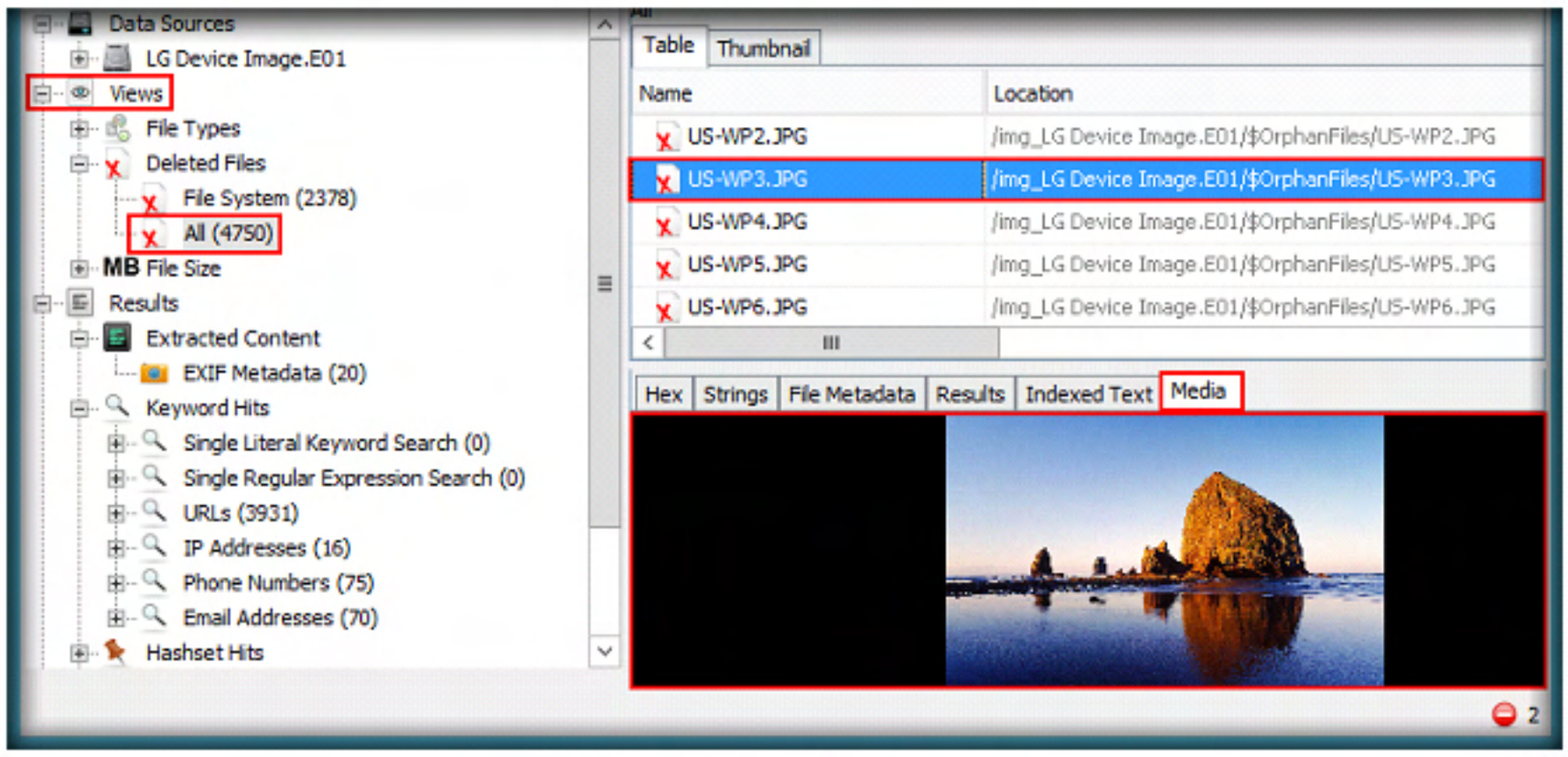


FIGURE 1.14: Examining deleted files

28. In the same way, you may even view various other files of different formats.

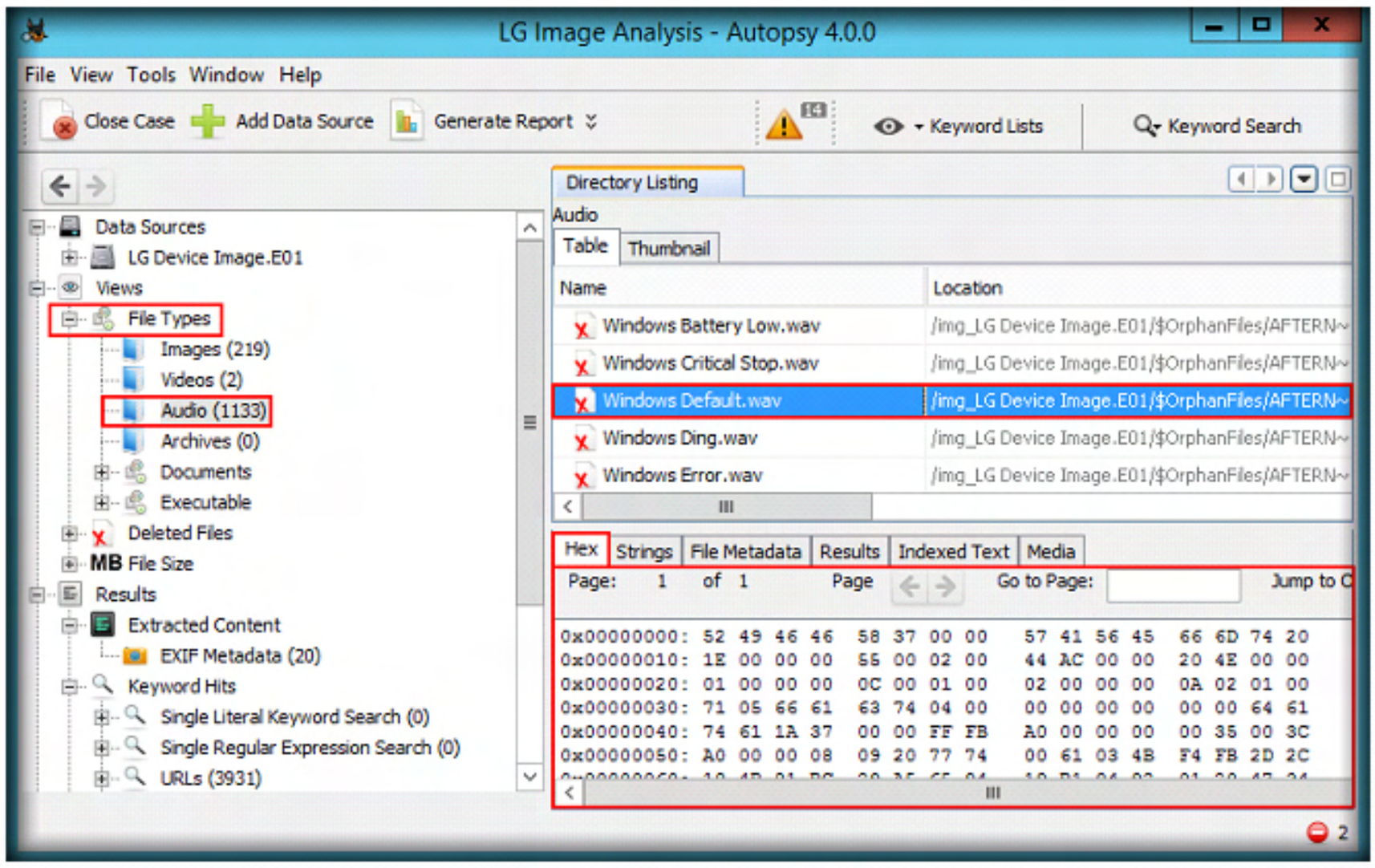


FIGURE 1.15: Examining audio files

29. Autopsy classifies files of various sizes in three sections, i.e., between 50-200 MB, 200-1 GB and 1 GB+. For instance, a carved file of size **50-200MB** is displayed in the following screenshot:

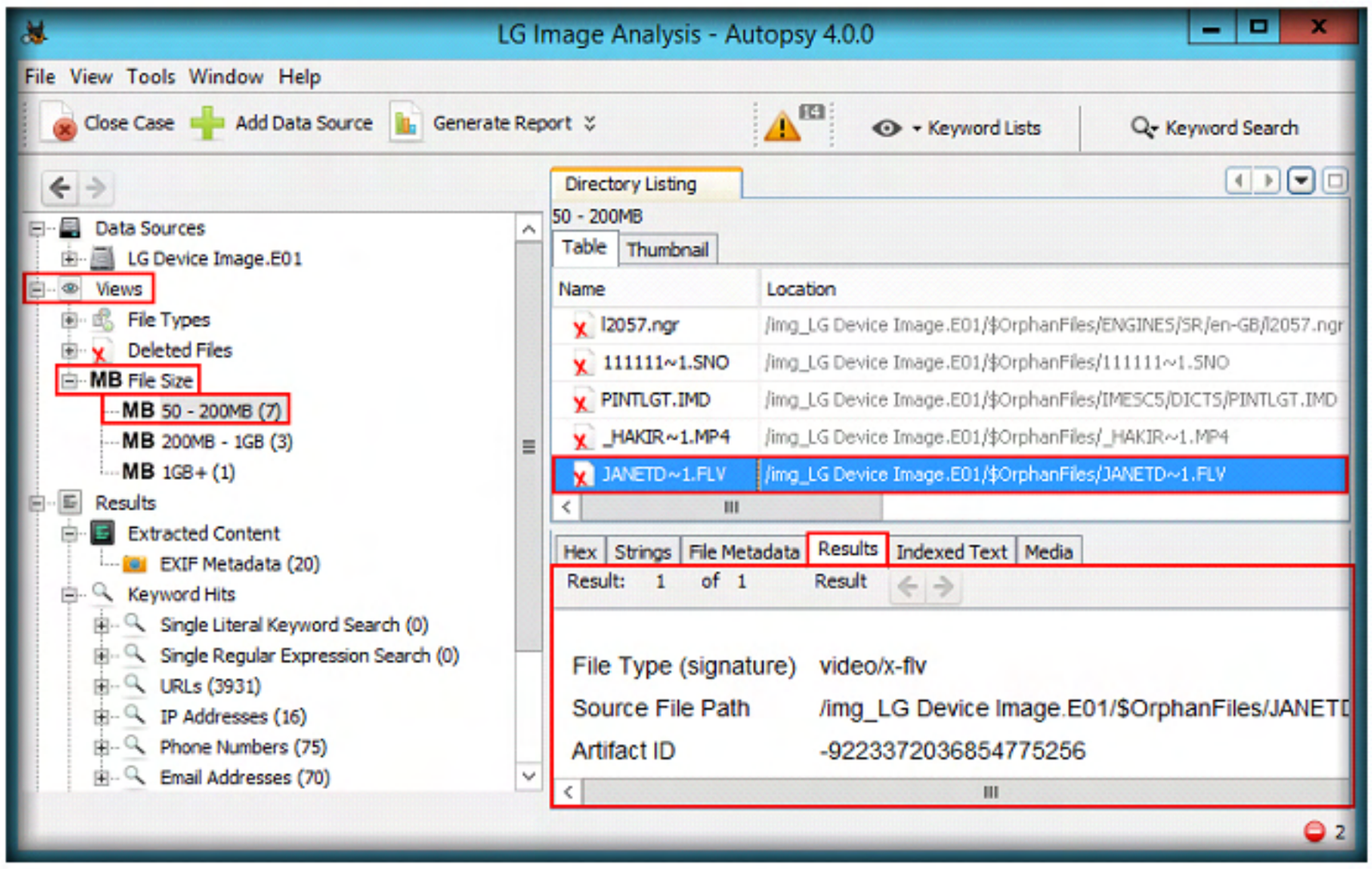


FIGURE 1.16: Classification of files based on Files Size

30. Expand **Data Sources → Image File** (LG Device Image.E01) → **Android → data → com.cooliris.media → cache**.

31. This displays all the files stored in the cache memory of the device as shown in the following screenshot:

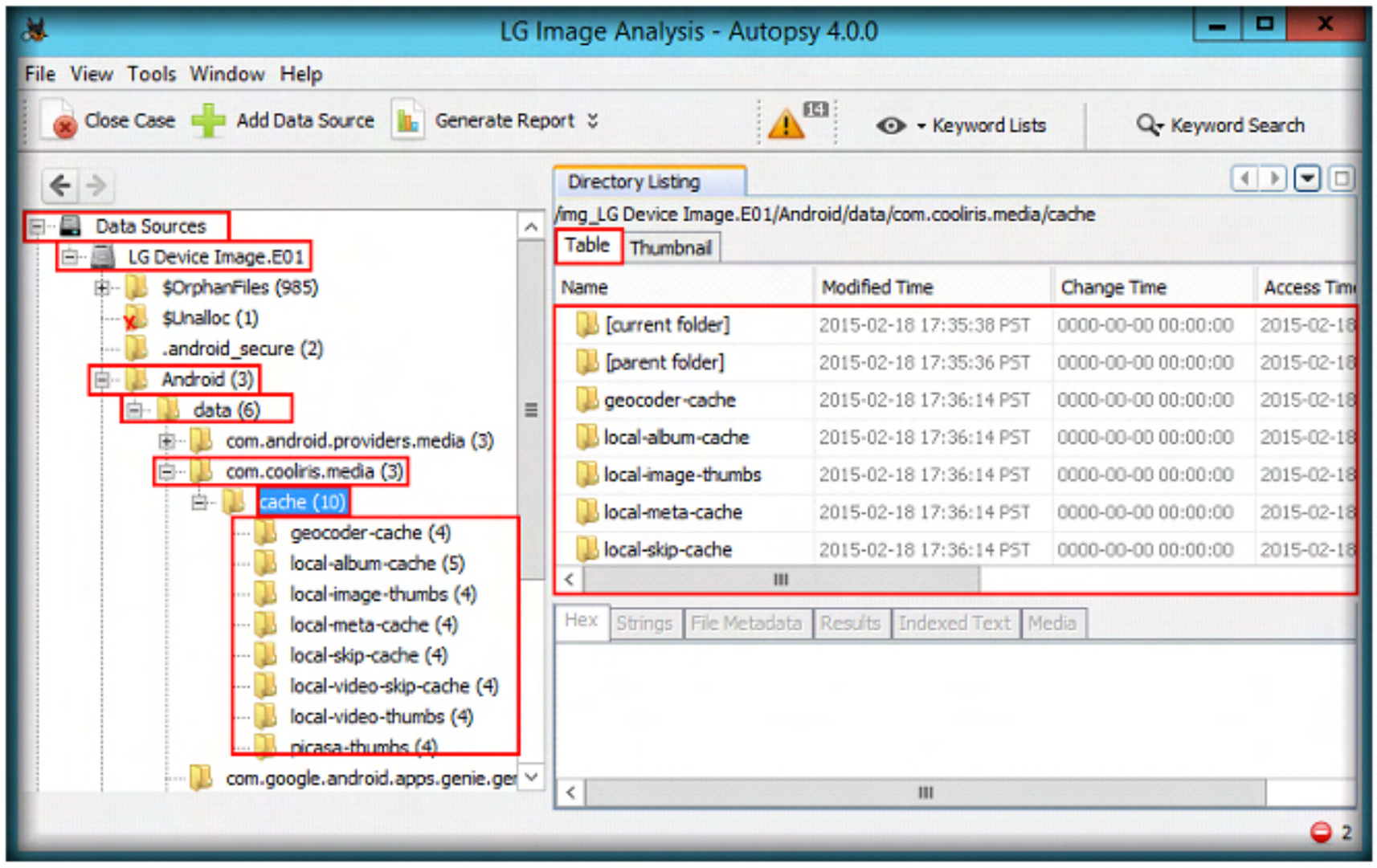


FIGURE 1.17: Examining Cache directory

32. Autopsy displays a directory named **OrphanFiles** (Under **LG Device Image.E01**) that contains broken files, i.e., incompletely carved files. You may examine even these files as a part of the forensic investigation.

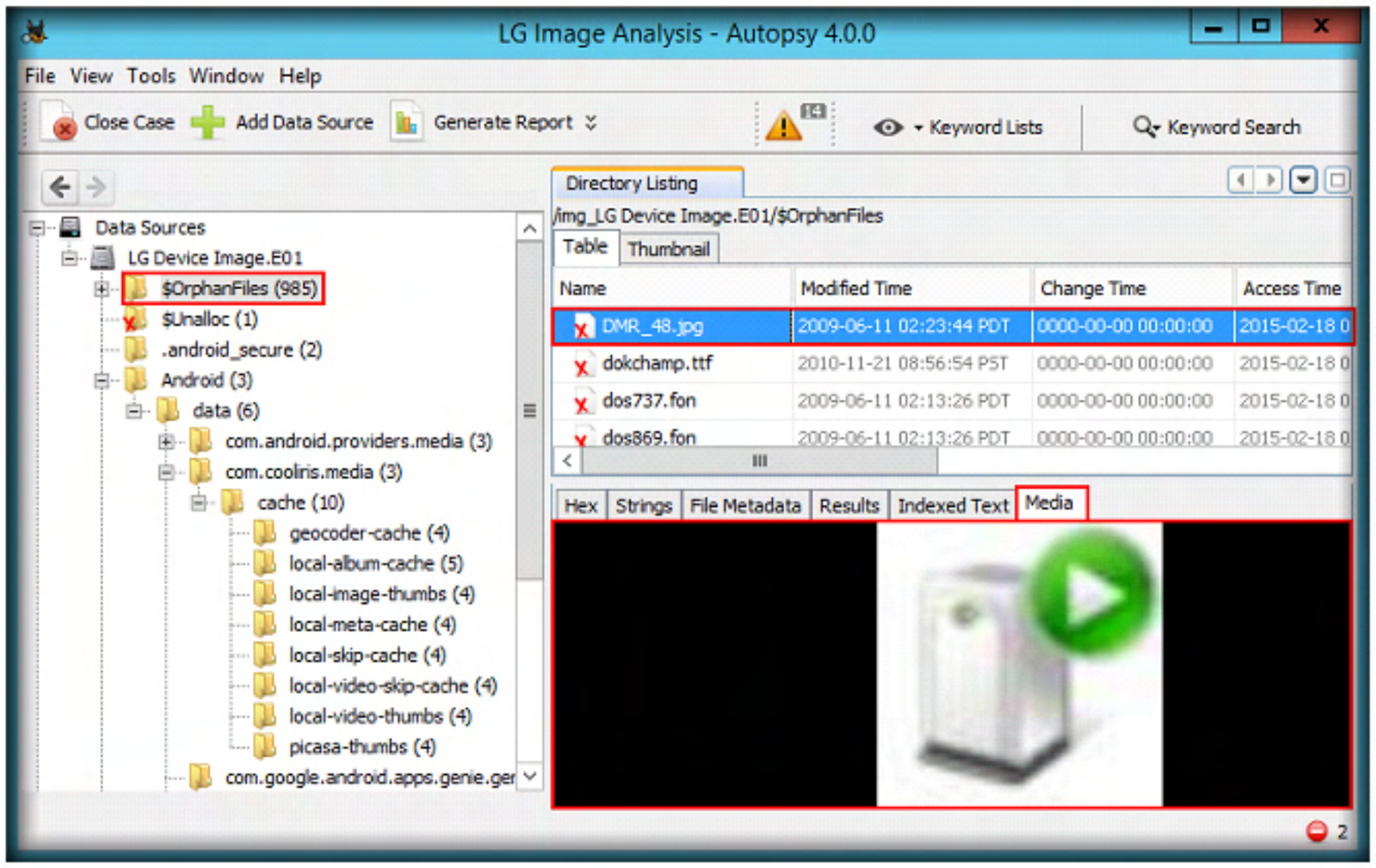


FIGURE 1.18: Examining Orphan Files

33. Autopsy also allows you to view Whatsapp, Viber and other applications' (if installed) databases which contain information, such as text and voice messages, pictures, etc.

TASK 5

Examine the Timeline

34. Timeline helps you determine the files system events on the device during a selected time period. To view the timeline, select **Tools** in the menu bar and select **Timeline**.

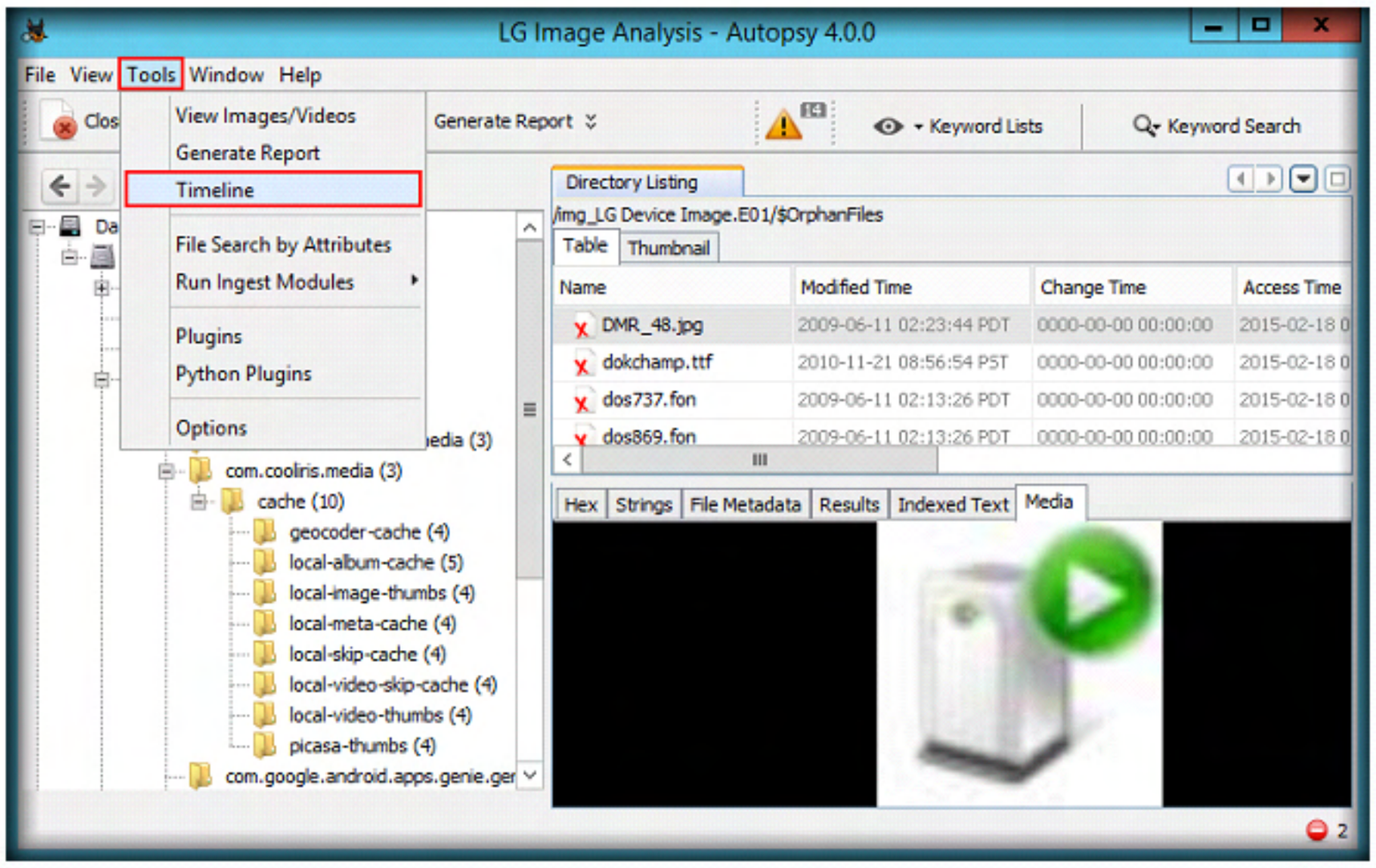


FIGURE 1.19: Examining the Timeline

35. A timeline window appears, displaying a logarithmic graph which contains all the file system events during a selected time interval.
36. In this window, you can specify a particular time interval, choose the type of files needs to be viewed, the time units, event type and description details.
37. The red colour in the bars represents the file system activity, green colour represents the web activity, and cyan represents the miscellaneous activities.

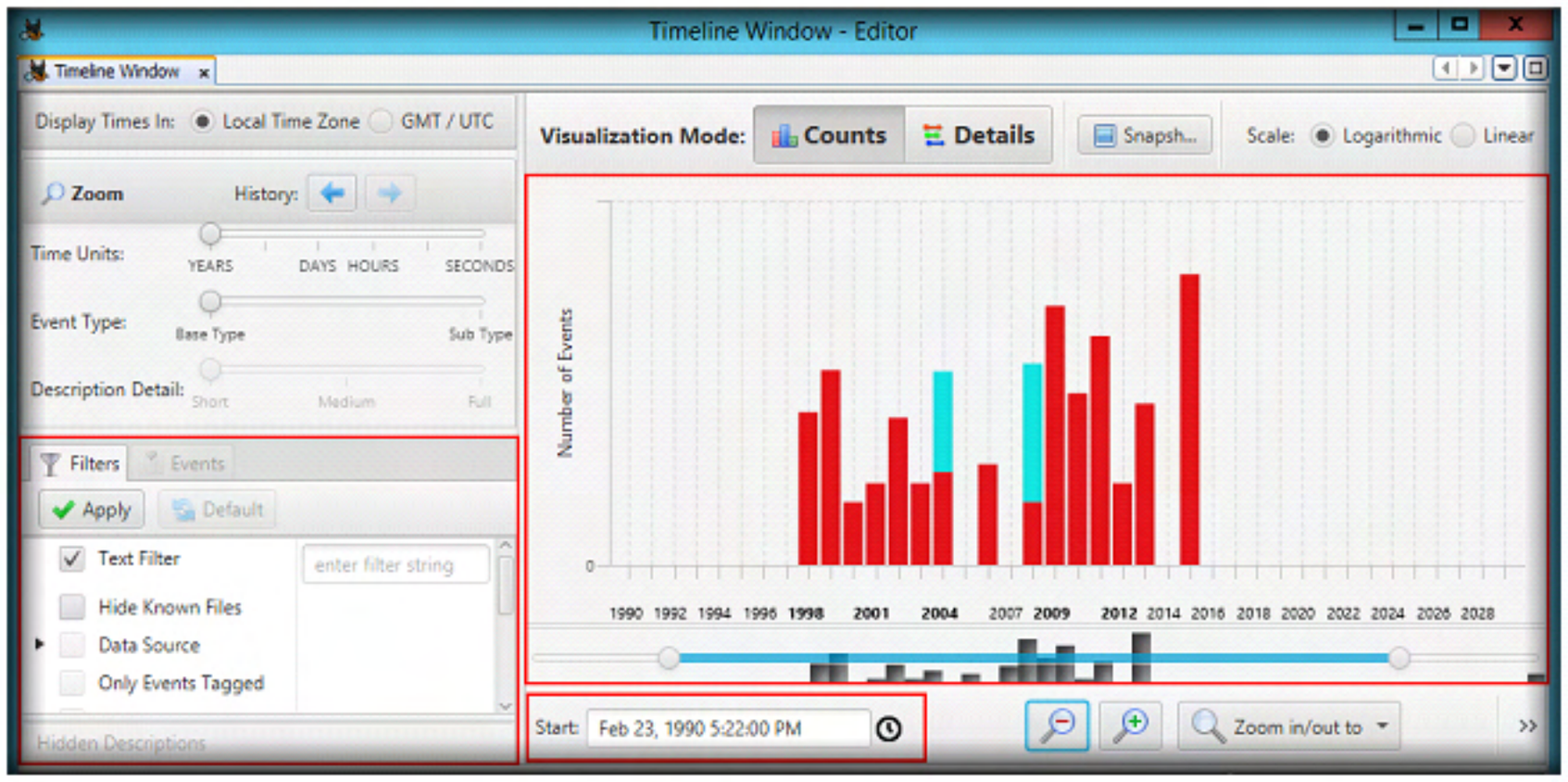


FIGURE 1.20: Examining file system events

38. Choose a time interval and select a bar from the graph. Autopsy displays all the file system events that occurred during the time interval associated with the selected bar.

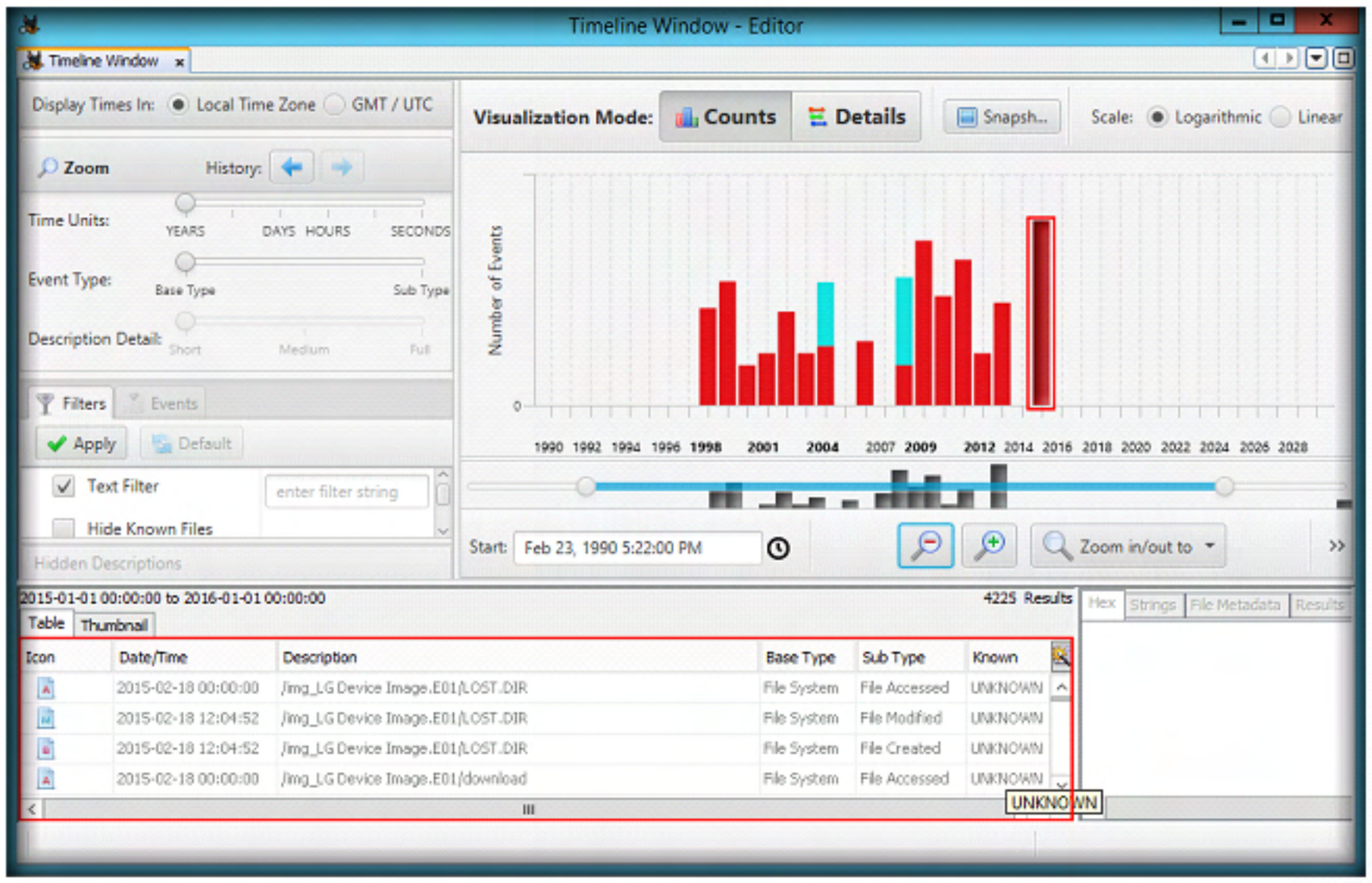


FIGURE 1.21: Examining file system events of a particular bar from the graph

39. This way, you can analyse an image and examine the file system of the target device during the process of forensic investigation.

Lab Analysis

Analyze the result and Document the findings of the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Investigating an Android Device using Andriller

Andriller is an application that performs read-only, forensically sound, non-destructive acquisition from Android devices. Extraction and decoders produce reports in HTML and Excel (.xlsx) formats.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Databases play a vital role in storing user and application information on an Android device. The information stored in these databases includes Phonebook contacts, Call logs, SMS, Synchronized accounts, WhatsApp chat messages, Viber call logs (if installed on the device), Wi-Fi passwords, etc. During the process of forensic investigation, these databases can be acquired and examined to obtain crucial information related to the owner of the acquired mobile device.

Being an expert forensic investigator, your main job is to acquire as much information as possible from the mobile device and analyze it in search of valuable information.

Lab Objectives

In this lab, you will learn how to:

- Extract Databases and other sensitive information from an Android emulator using Andriller

Lab Environment

This lab requires:

- A Windows Server 2012 Host Machine.
- Andriller located in **C:\CHFI-Tools\CHFIv9 Module 13 Mobile Forensics\Mobile Forensics Tools\Andriller**.
- Administrative Privileges to run the tools.

Lab Duration

Time: 15 Minutes

Overview of the Lab

- Ensure that you are using an emulated Android device
- Extract the databases using **Andriller**

Lab Tasks

TASK 1

Install Andriller

1. Before beginning this lab, logon to **Windows Server 2012** virtual machine and create a folder named **Andriller** on the desktop.
2. Launch **AVD Manager** from the **Apps** screen.
3. Select **Test_Emulator** and click **Start...**.

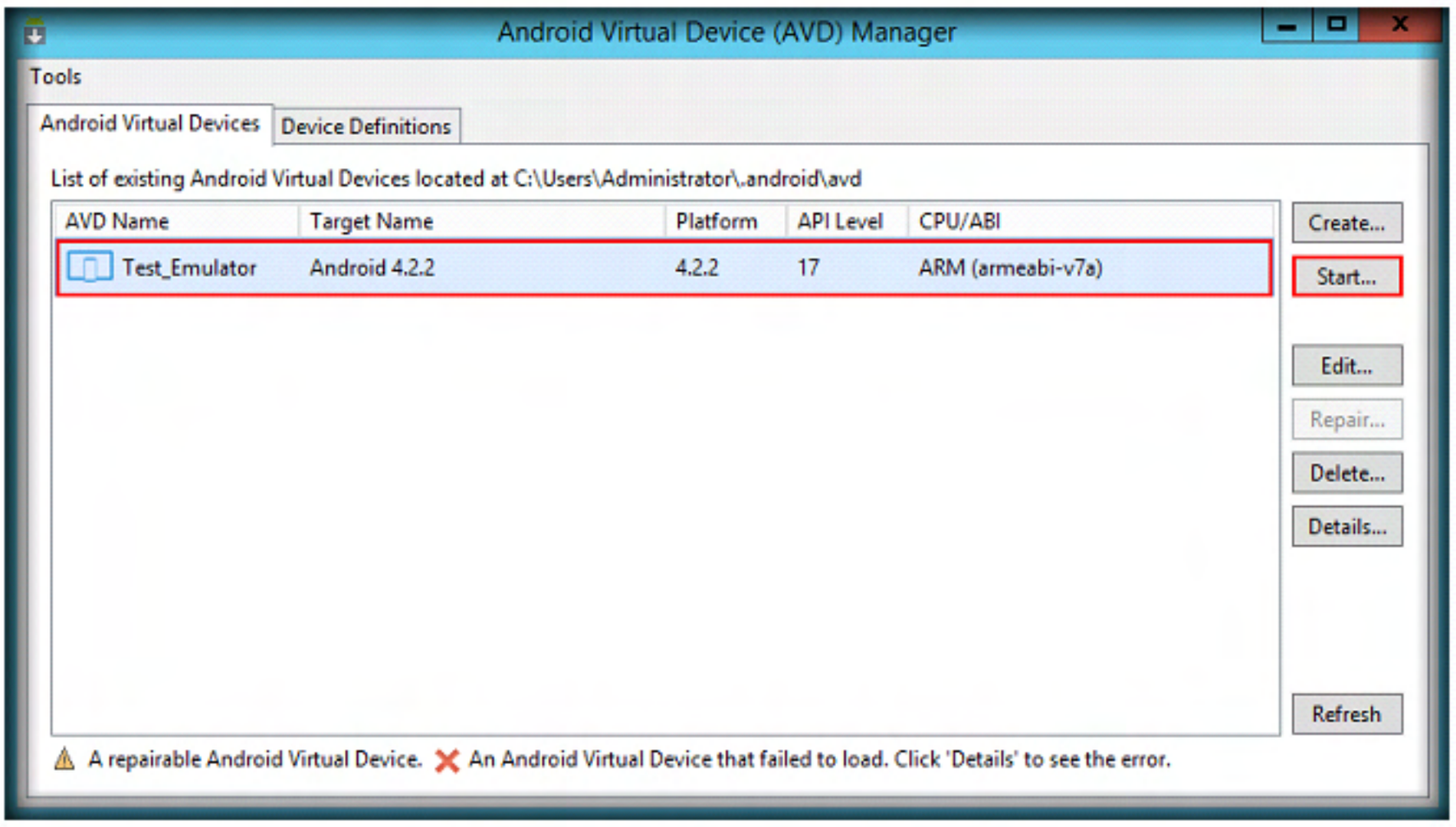


FIGURE 2.1: Android Virtual Manager (AVD) window

4. **Launch Options** window appears, check **Scale display to real size** option, specify the Screen Size as **6.5** inches and click **Launch**.

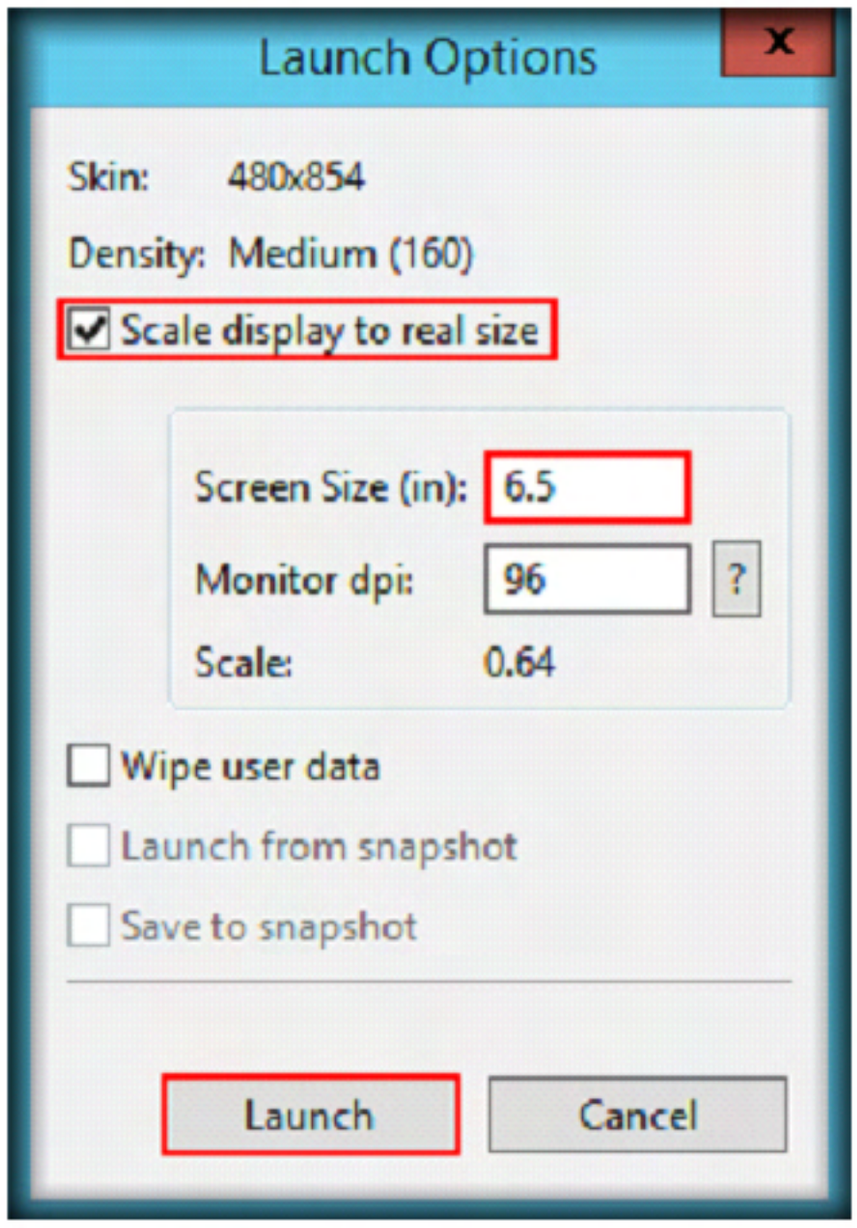


FIGURE 2.2: Launch Options window

5. Navigate to **C:\CHFI-Tools\CHFIv9 Module 13 Mobile Forensics\Mobile Forensics Tools\Andriller**, double-click **Andriller_v2.6.0.1_Setup.exe** and follow the wizard-driven installation steps to install the application.

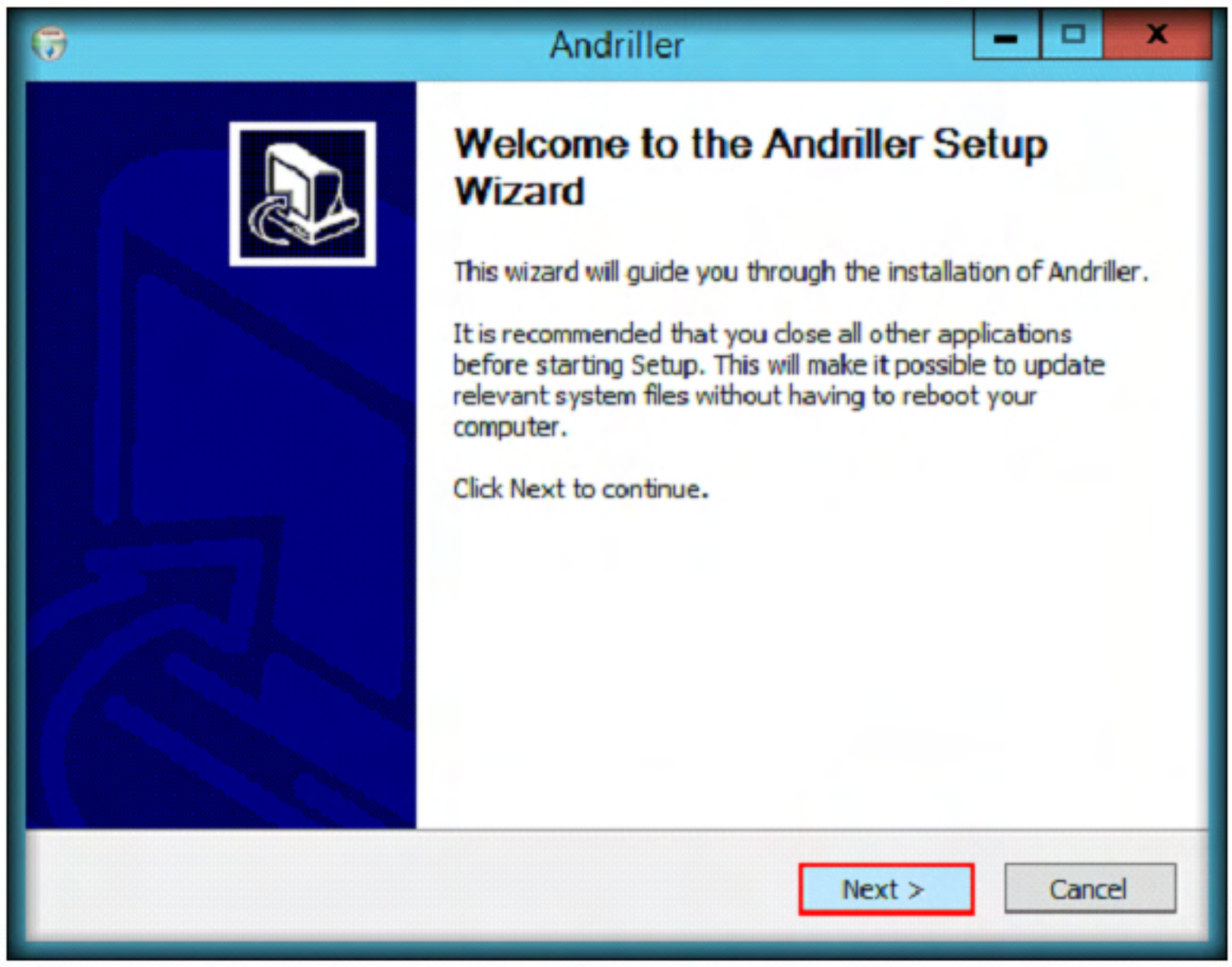


FIGURE 2.3: Installing Andriller

6. On completing the installation, launch Andriller application from the **Apps** screen.

FIGURE 2.4: Launching Andriller from Apps screen

7. If a **Check New Versions?** dialog-box appears, click **No**.

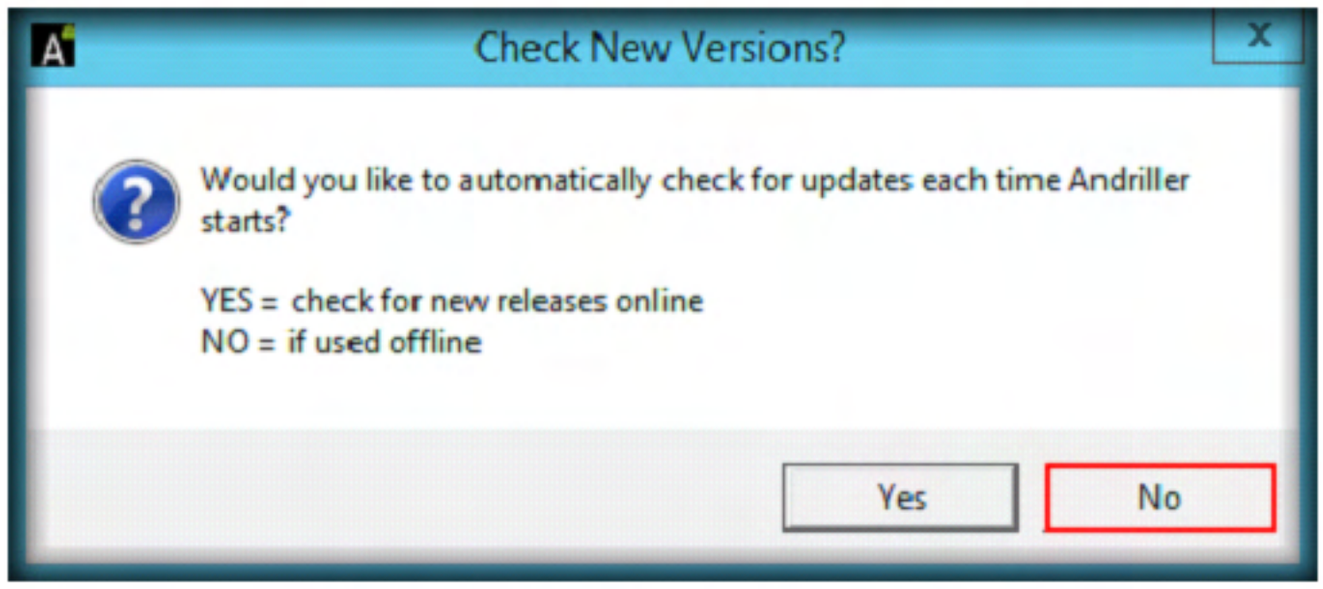


FIGURE 2.5: Check New Versions? dialog-box

8. If a **Preferences Menu** dialog-box appears, click **OK**.

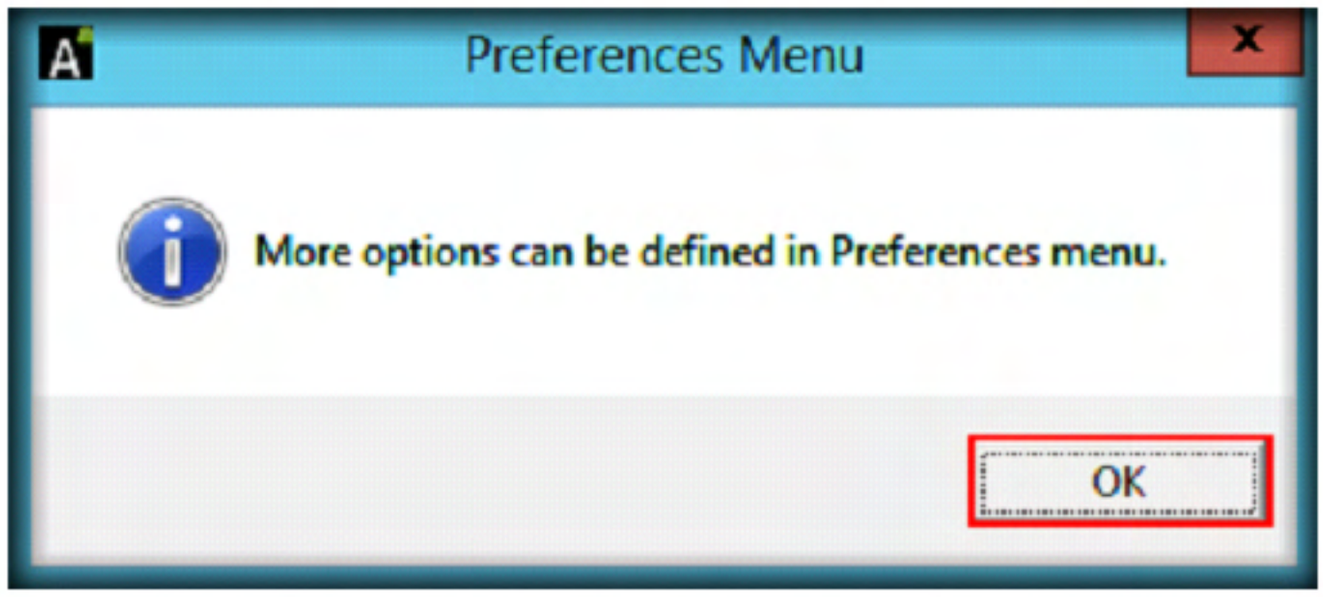


FIGURE 2.6: Preferences Menu dialog-box

9. Andriller main window appears as shown in the following screenshot:

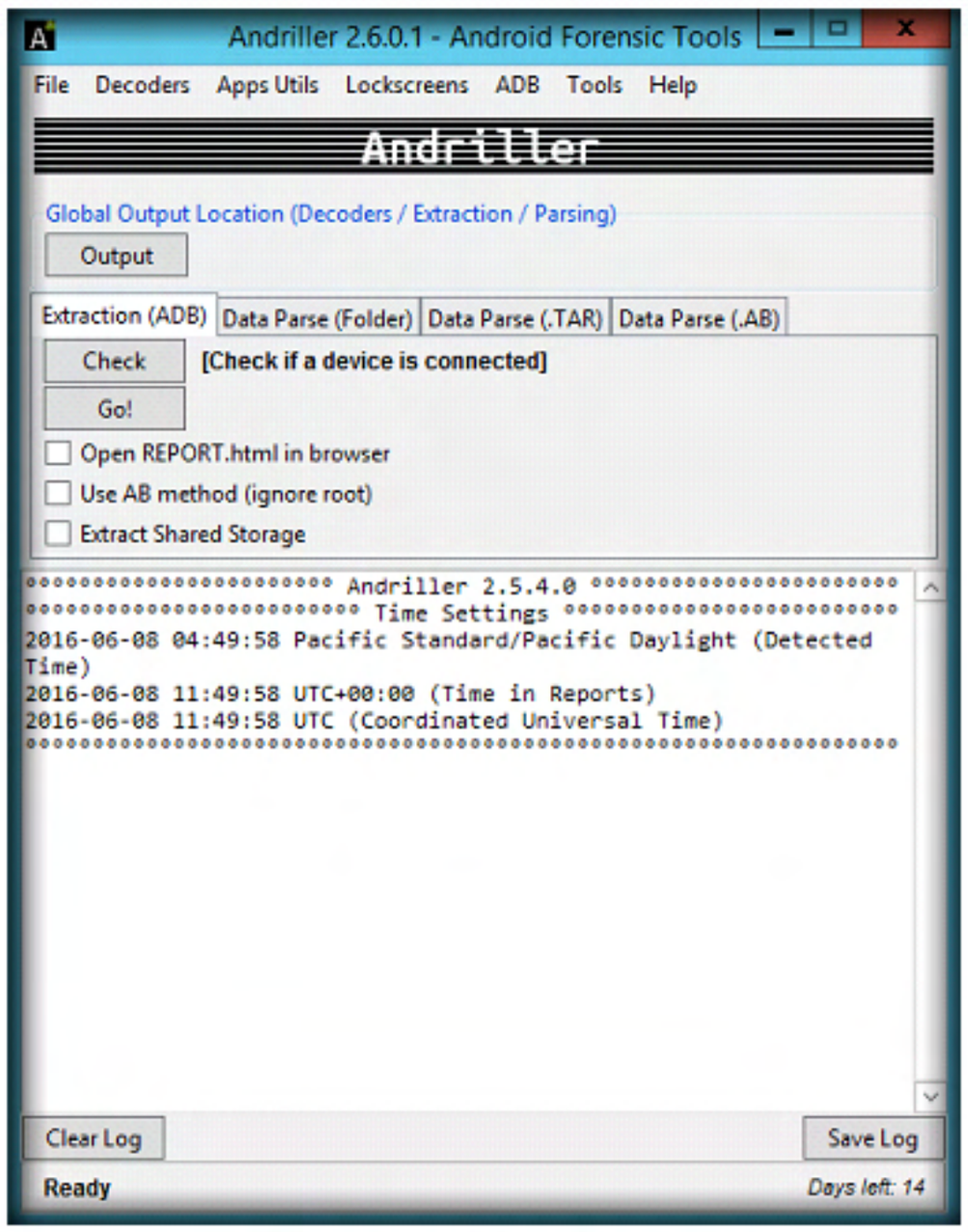


FIGURE 2.7: Andriller main window

TASK 2

Configure Andriller

10. You need to specify an output location for Andriller to store all the logs and data. Click **Output** button in the Andriller window.

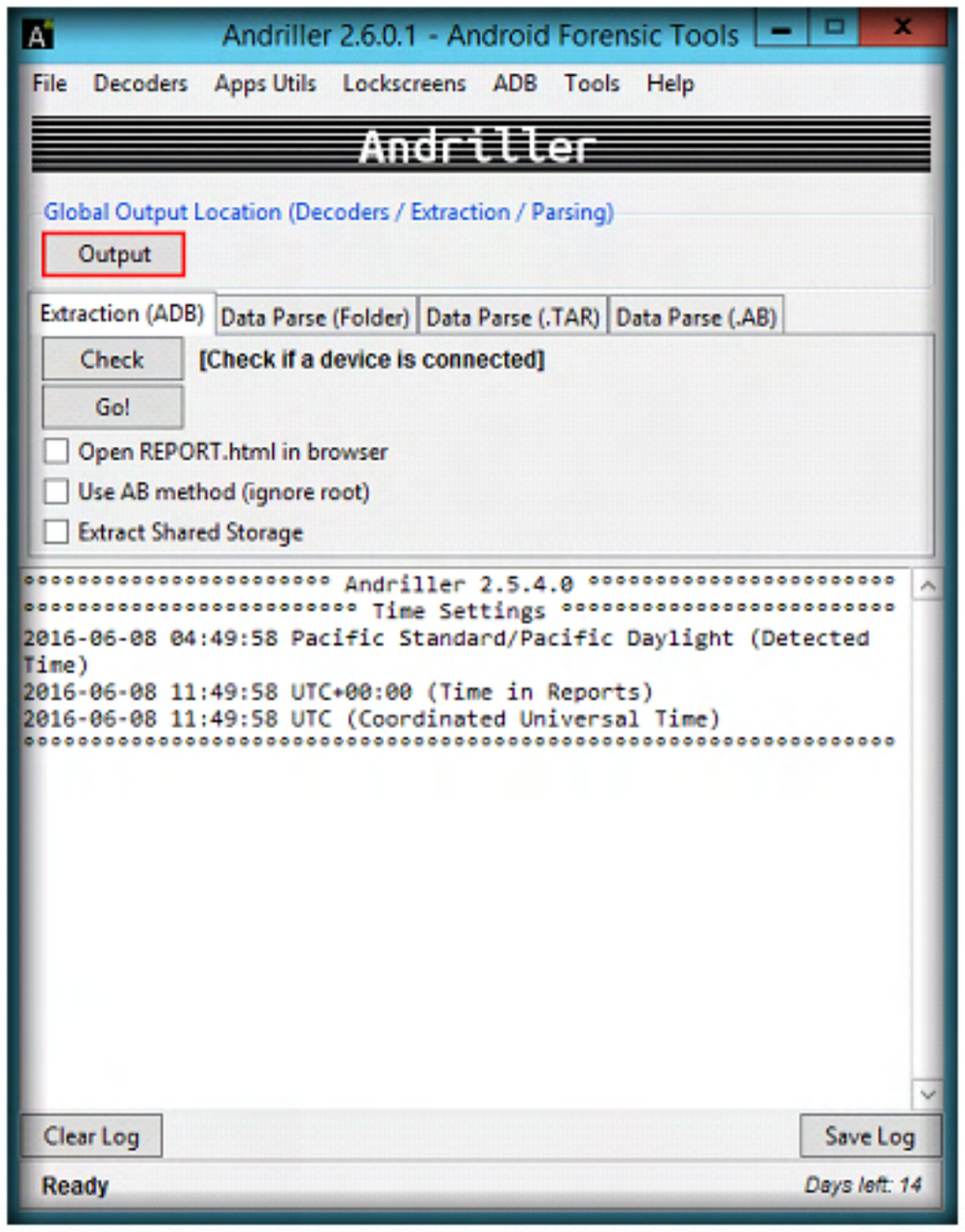


FIGURE 2.8: Configuring Output folder

11. Navigate to the **Desktop**, Select the **Andriller** folder which was created before installing the application and click **OK**.

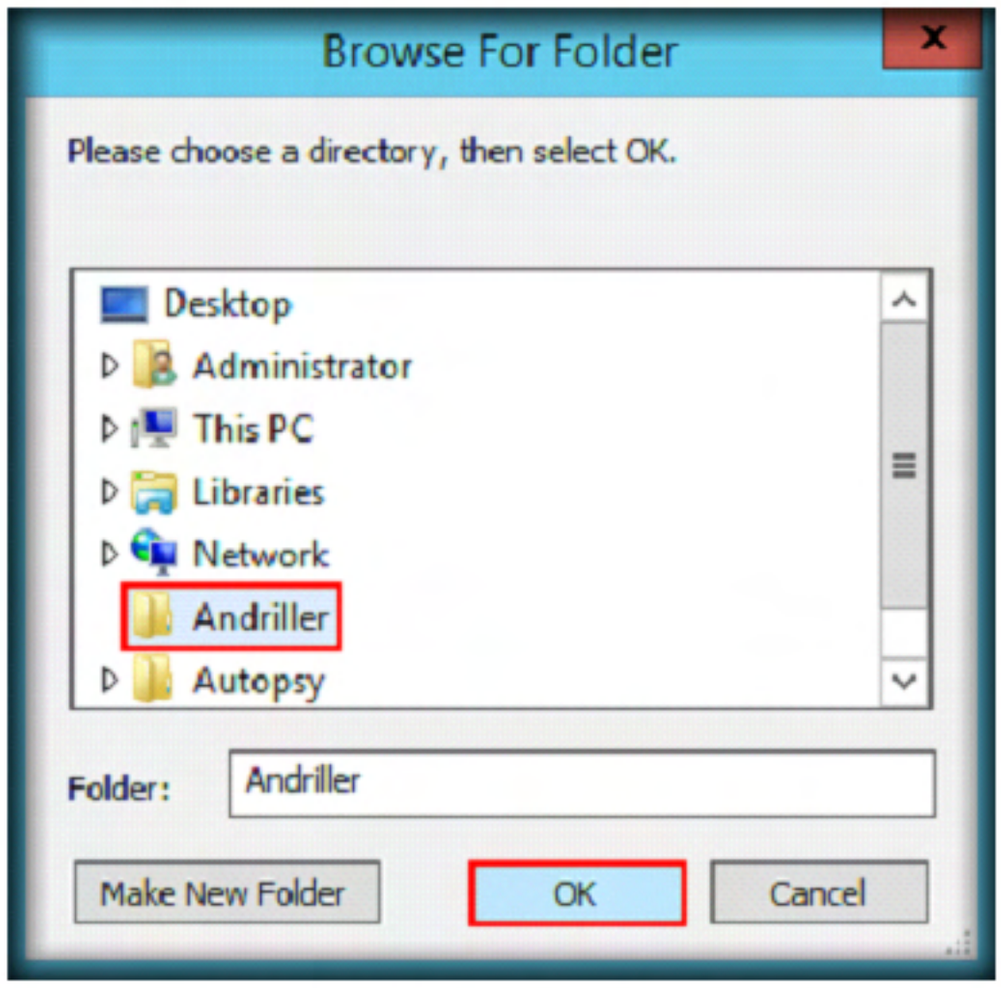


FIGURE 2.9: Browse For Folder window

12. Now, click **Check** button to see if the Android Emulator is connected to Andriller.

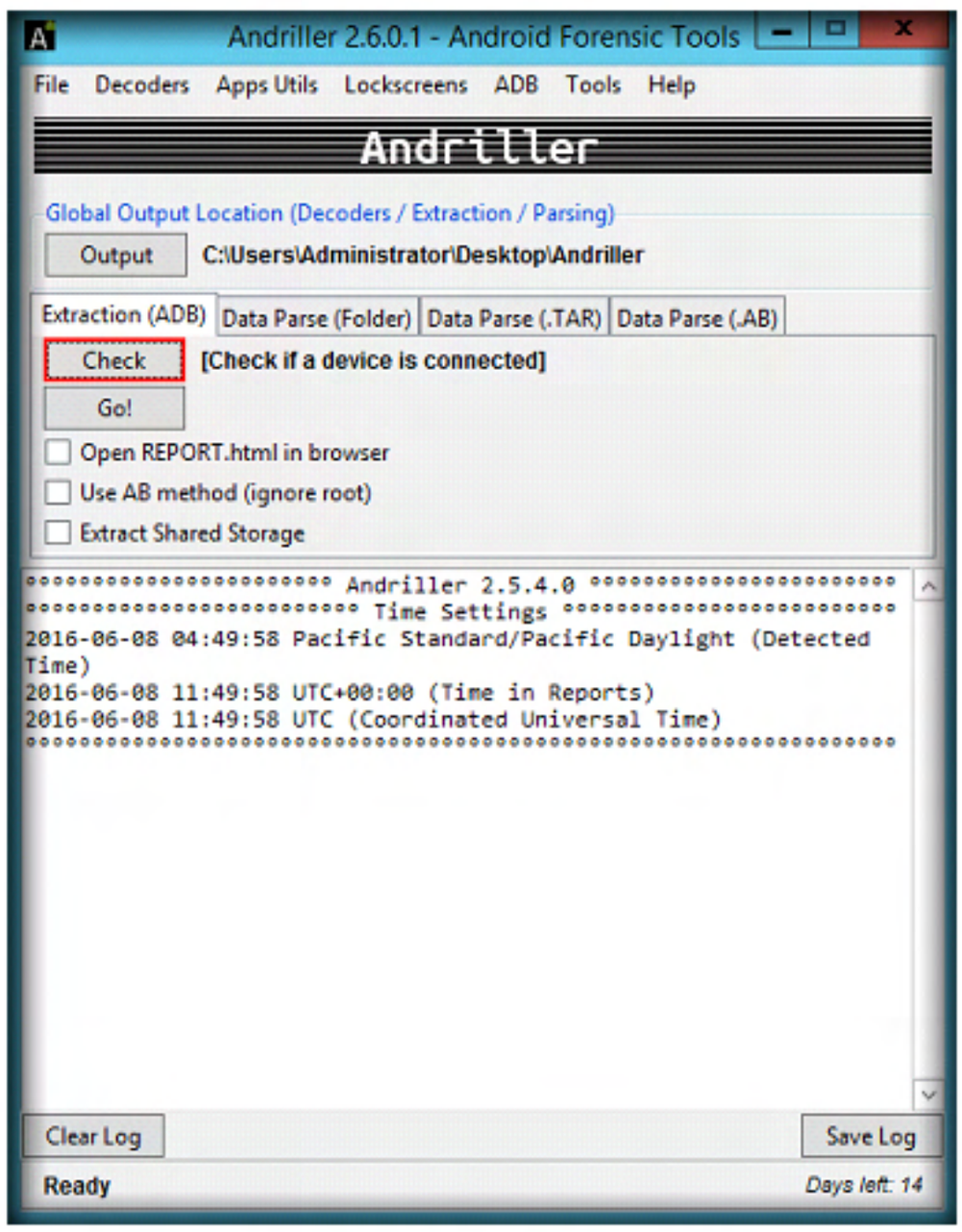


FIGURE 2.10: Checking for the device

Note: From here on, the output illustrated in the screenshots may vary in your lab environment.

13. On clicking the **Check** button, Andriller should display a serial ID of the emulator as shown in the following screenshot:

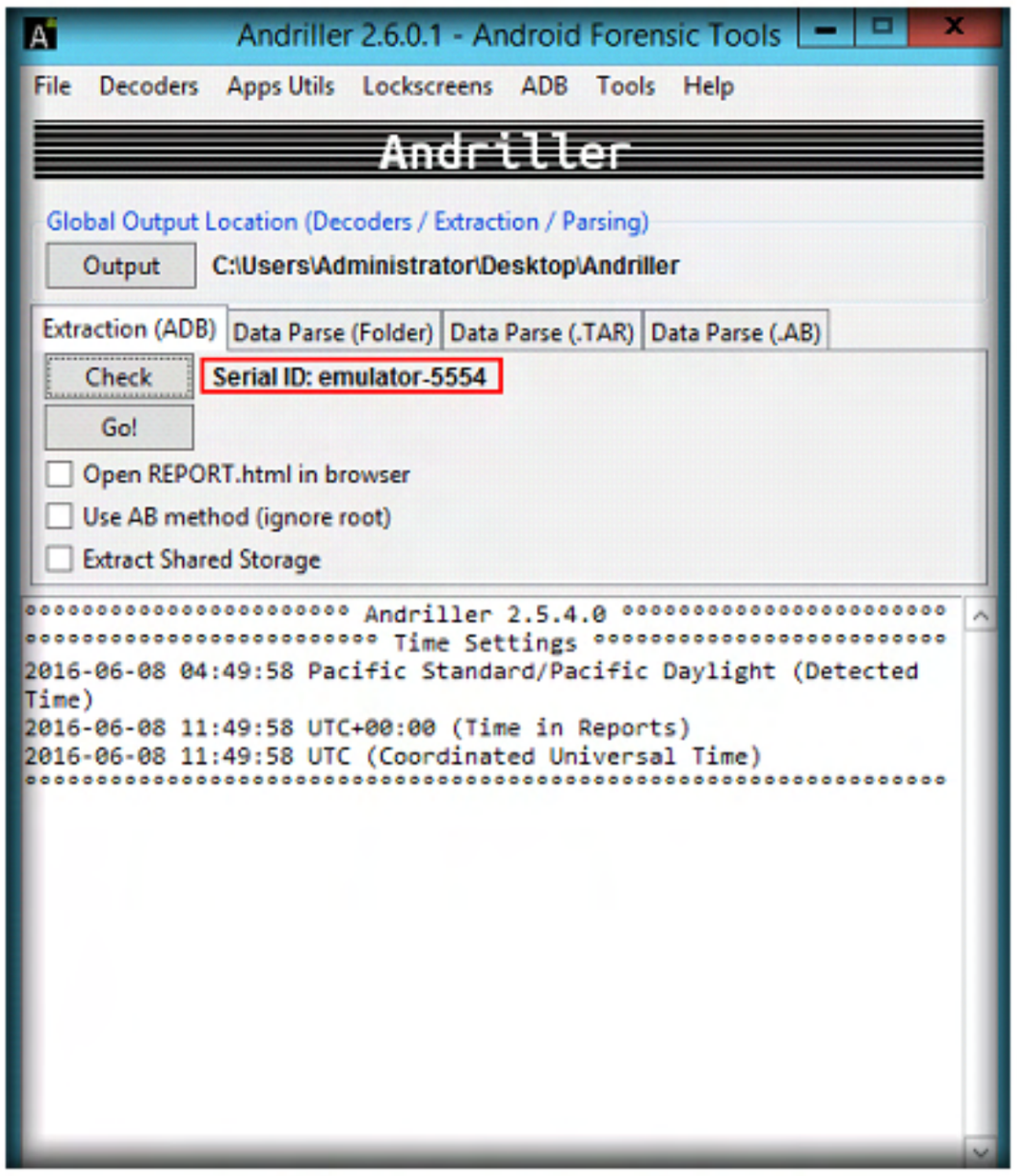


FIGURE 2.11: Device successfully detected

TASK 3

Begin Data Acquisition

14. Once Andriller detects the device, click **Go!** button to begin data extraction.

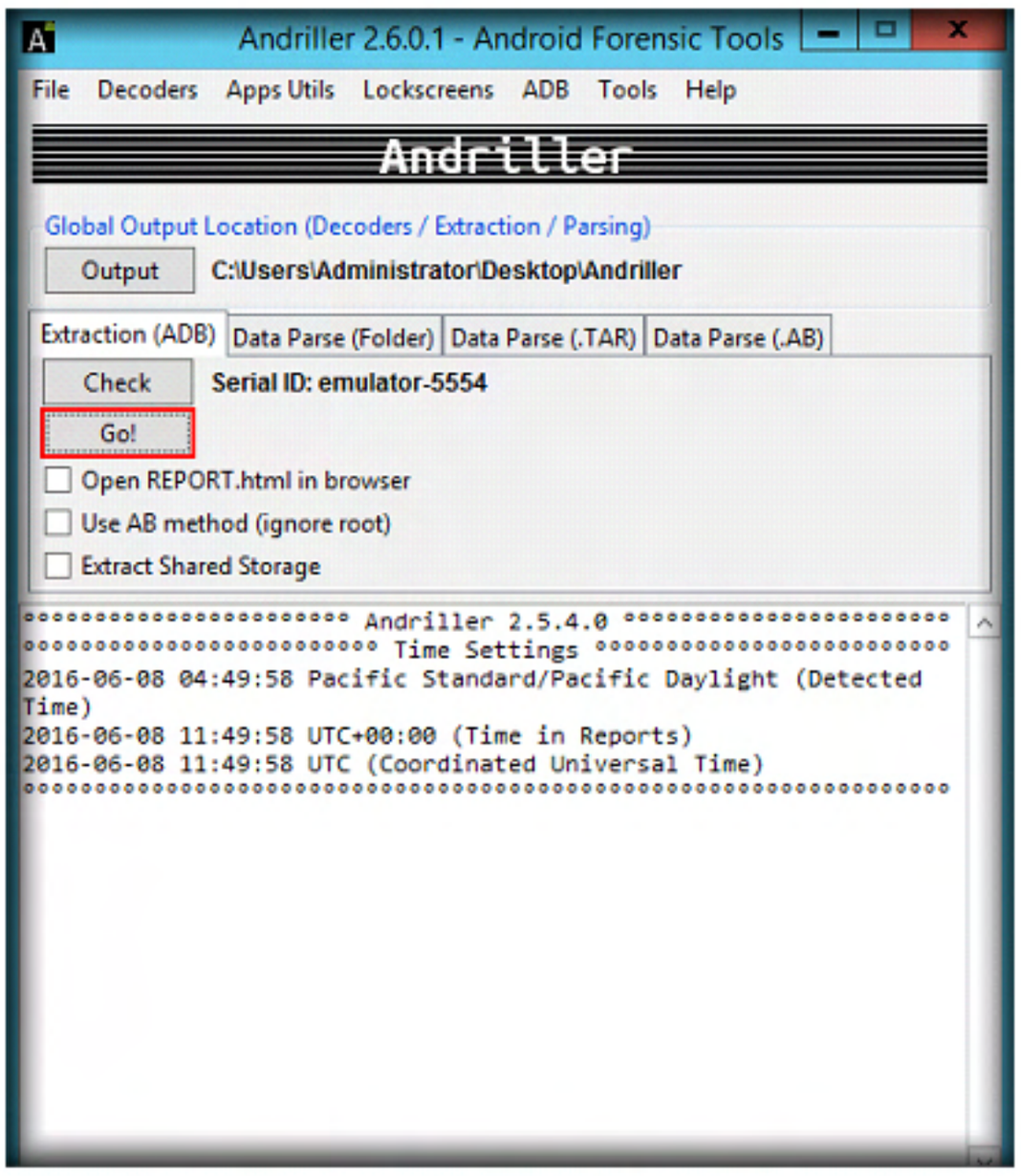


FIGURE 2.12: Beginning data extraction

15. Andriller begins to extract the databases and other useful information as shown in the following screenshot:

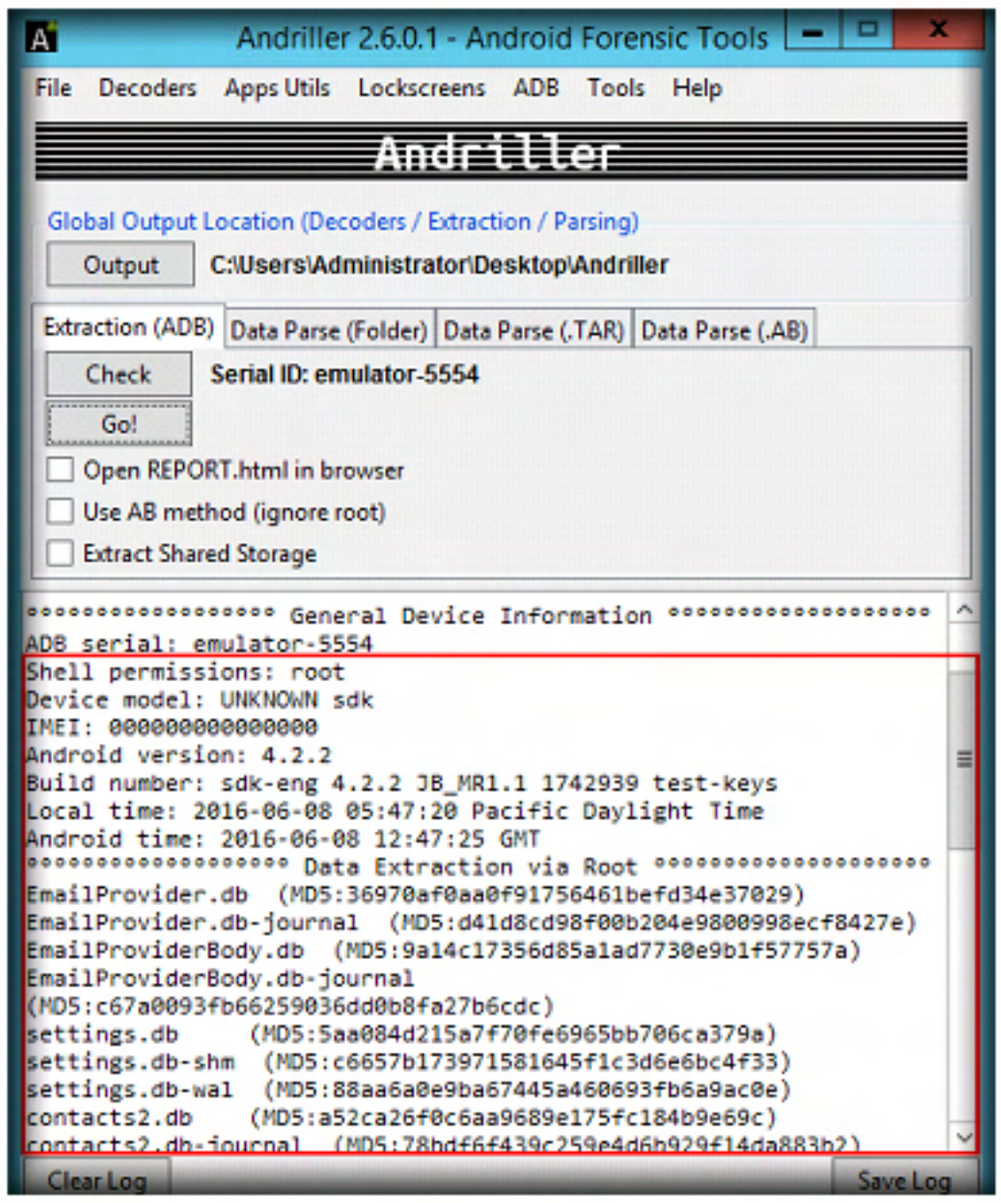


FIGURE 2.13: Screenshot showing extracted data

16. Andriller creates a directory inside the Andriller folder with the name of the device followed by the timestamp as shown in the following screenshot:

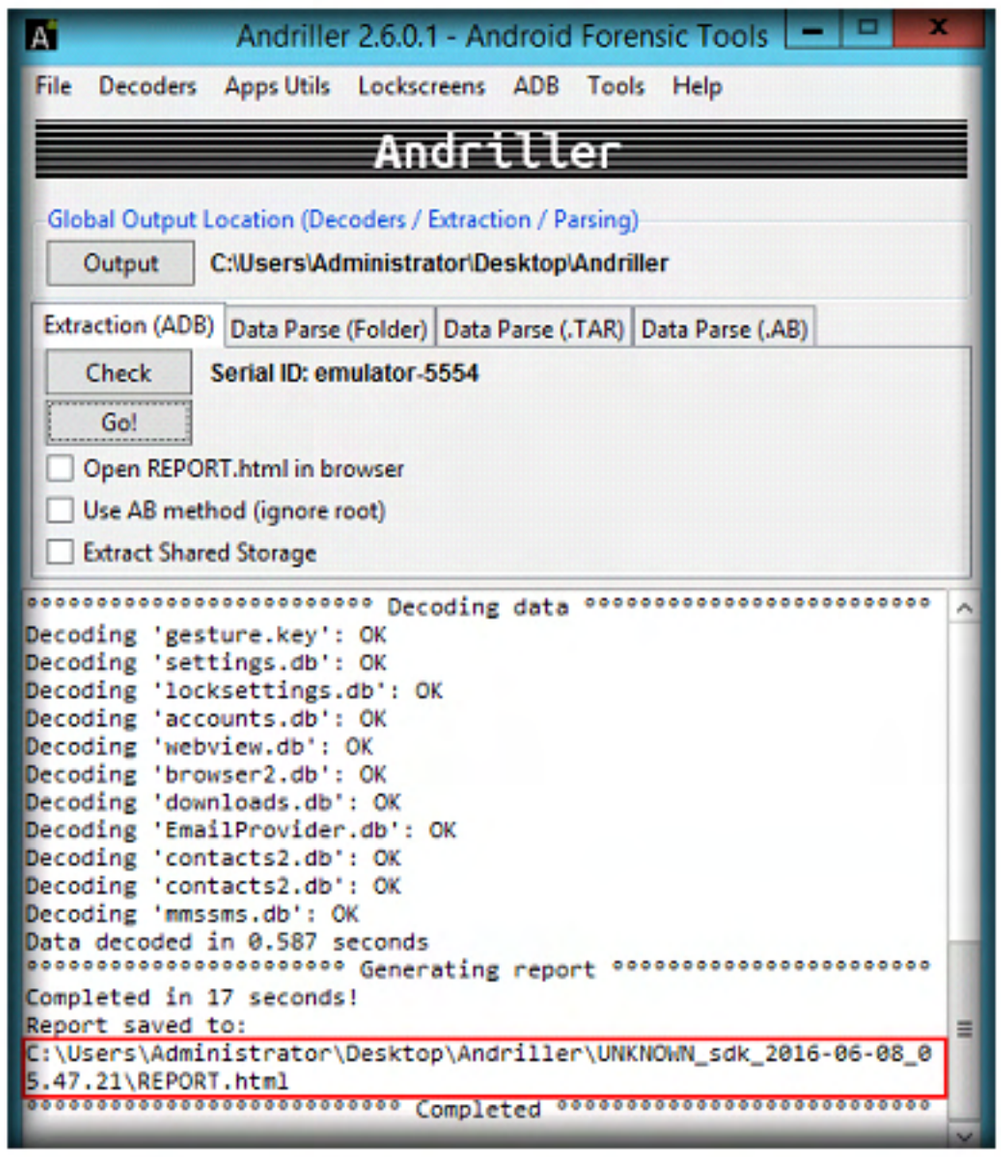


FIGURE 2.14: Directory path and completion status

Note: The folder name varies according to the device used in this lab.

TASK 4

View the Acquired Files

17. Navigate to the **Andriller** folder located on the **Desktop** and open the folder which stored the extracted files and databases.

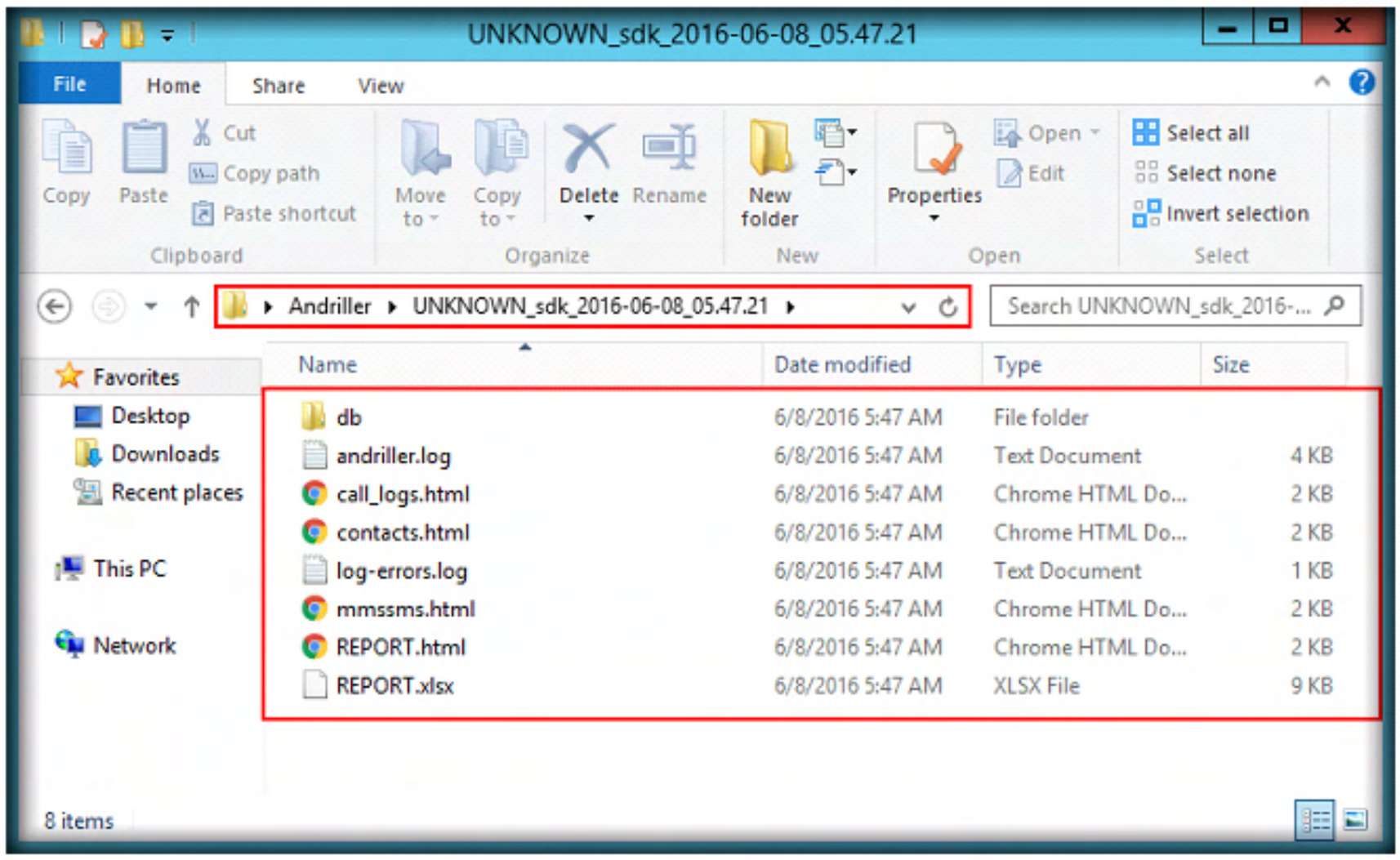


FIGURE 2.15: Viewing extracted files in Andriller folder

TASK 5

Examine the Report

18. Double-click **REPORT.html** file to open it. This file appears in the default web browser and displays important information like device ID, its version, associated accounts, etc.

19. Open **Contacts** link in a new tab to view the contacts stored in the device.

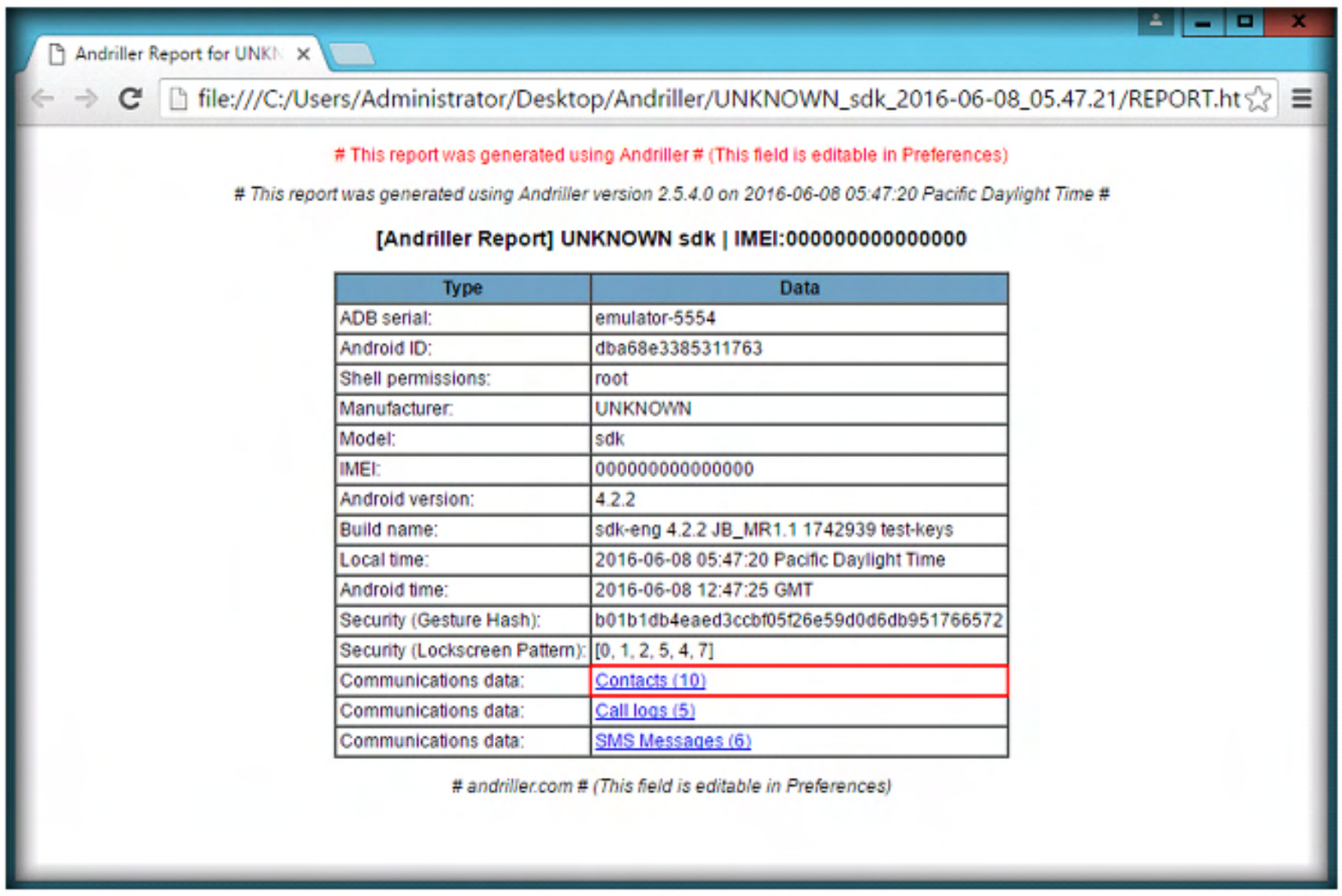
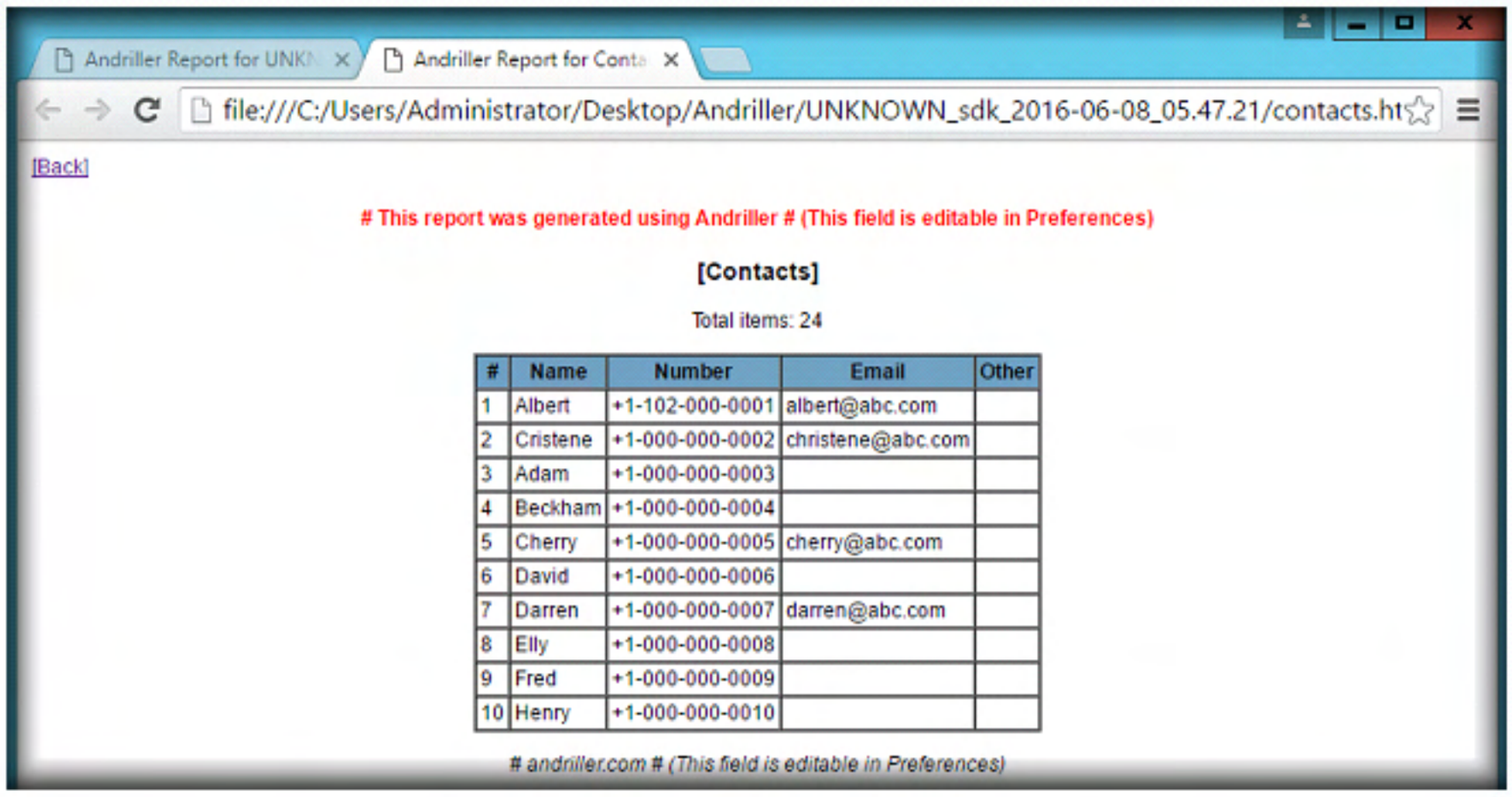


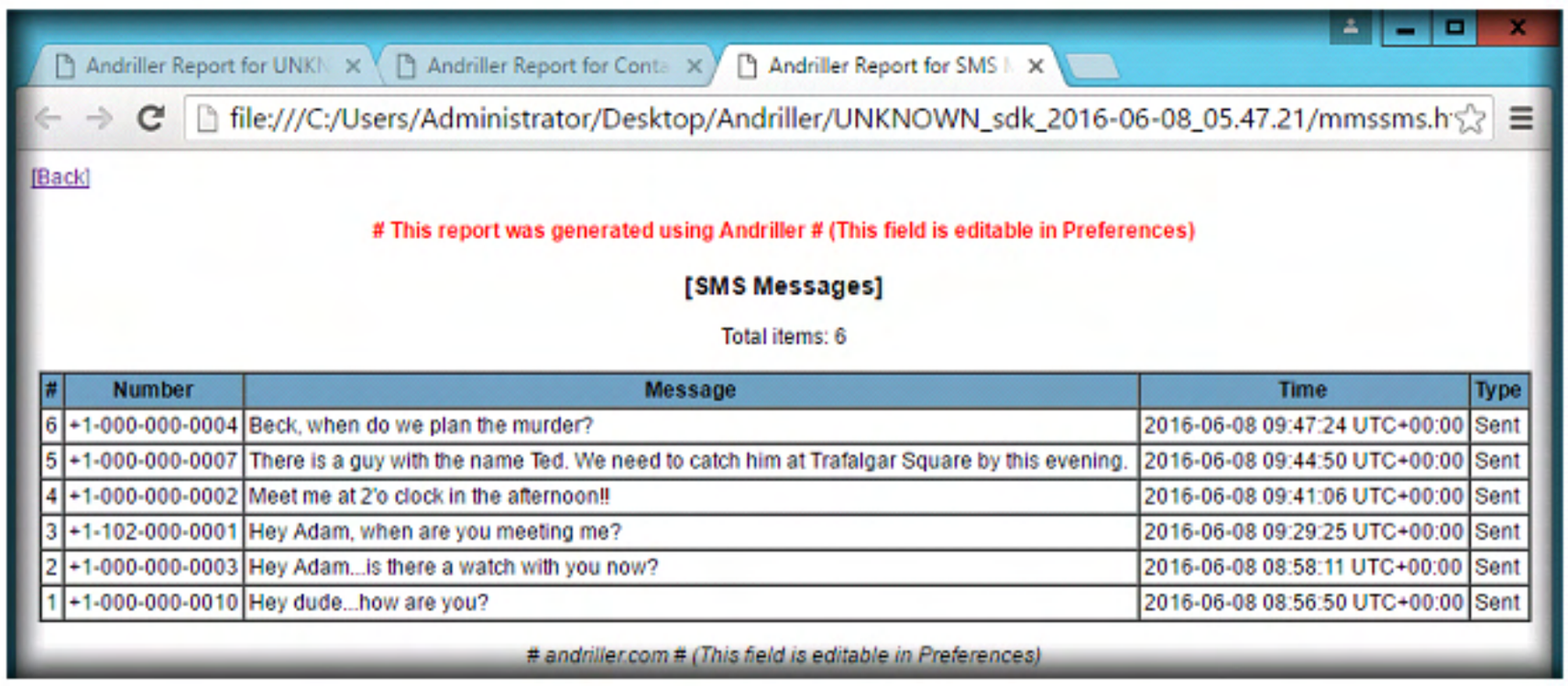
FIGURE 2.16: Viewing Contacts



#	Name	Number	Email	Other
1	Albert	+1-102-000-0001	albert@abc.com	
2	Cristene	+1-000-000-0002	christene@abc.com	
3	Adam	+1-000-000-0003		
4	Beckham	+1-000-000-0004		
5	Cherry	+1-000-000-0005	cherry@abc.com	
6	David	+1-000-000-0006		
7	Darren	+1-000-000-0007	darren@abc.com	
8	Elly	+1-000-000-0008		
9	Fred	+1-000-000-0009		
10	Henry	+1-000-000-0010		

FIGURE 2.17: Viewing Contacts

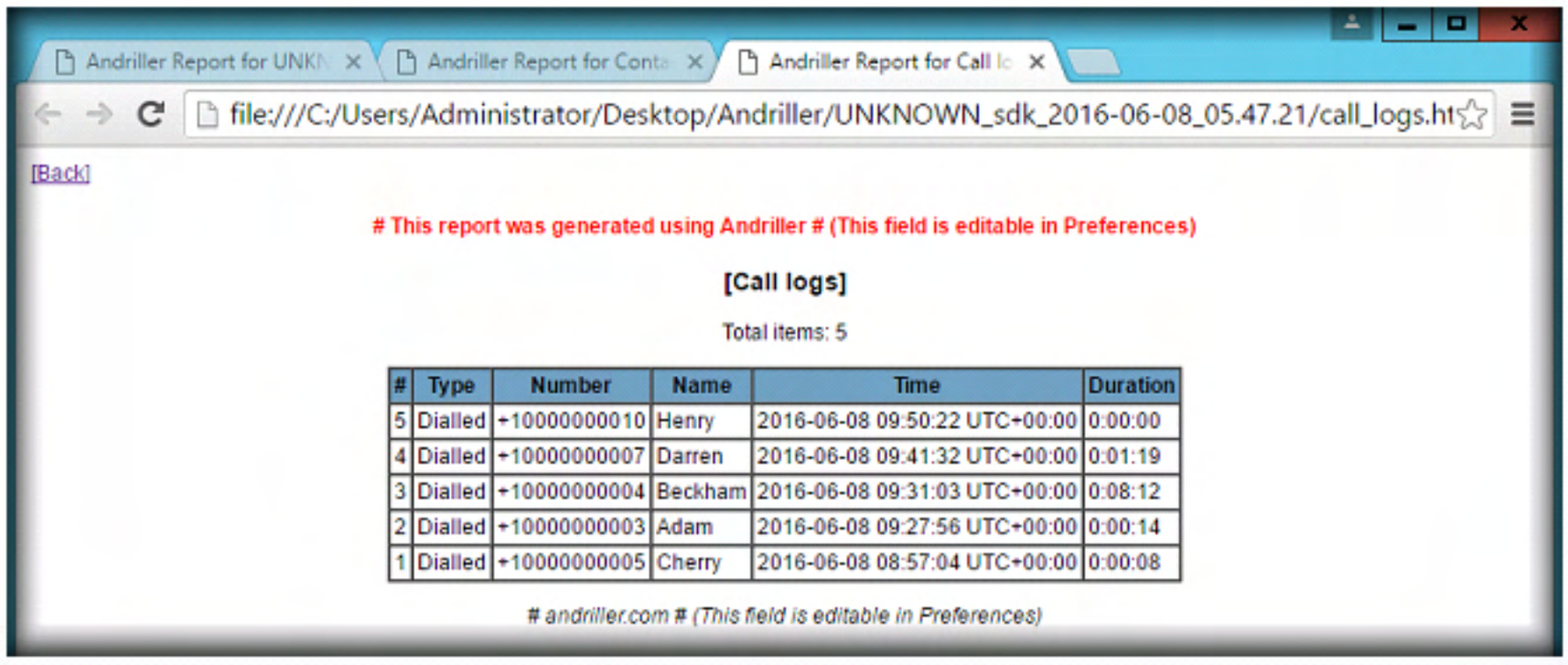
20. Go back to the previous **REPORT.html** Web page; open **SMS Messages** link in a new tab to view all the contacts stored on the phone as shown in the following screenshot:



#	Number	Message	Time	Type
6	+1-000-000-0004	Beck, when do we plan the murder?	2016-06-08 09:47:24 UTC+00:00	Sent
5	+1-000-000-0007	There is a guy with the name Ted. We need to catch him at Trafalgar Square by this evening.	2016-06-08 09:44:50 UTC+00:00	Sent
4	+1-000-000-0002	Meet me at 2'o clock in the afternoon!!	2016-06-08 09:41:06 UTC+00:00	Sent
3	+1-102-000-0001	Hey Adam, when are you meeting me?	2016-06-08 09:29:25 UTC+00:00	Sent
2	+1-000-000-0003	Hey Adam...is there a watch with you now?	2016-06-08 08:58:11 UTC+00:00	Sent
1	+1-000-000-0010	Hey dude...how are you?	2016-06-08 08:56:50 UTC+00:00	Sent

FIGURE 2.18: Viewing SMS Messages

21. In the same way, open **Call logs** link in a new tab to view all the calls received and dialed as shown in the following screenshot:



#	Type	Number	Name	Time	Duration
5	Dialled	+10000000010	Henry	2016-06-08 09:50:22 UTC+00:00	0:00:00
4	Dialled	+10000000007	Darren	2016-06-08 09:41:32 UTC+00:00	0:01:19
3	Dialled	+10000000004	Beckham	2016-06-08 09:31:03 UTC+00:00	0:08:12
2	Dialled	+10000000003	Adam	2016-06-08 09:27:56 UTC+00:00	0:00:14
1	Dialled	+10000000005	Cherry	2016-06-08 08:57:04 UTC+00:00	0:00:08

FIGURE 2.19: Viewing Call Logs

22. In real-time, if the mobile device has WhatsApp or any other messenger services like Viber, etc installed in it, Andriller displays separate columns for those applications.

23. An example of Andriller displaying Whatsapp messages is shown in the following screenshot:

Note: Since WhatsApp has implemented end to end encryption, Andriller may not be able to display clear text messages for those devices running the latest version of WhatsApp messenger.

[WhatsApp Messages]

Total items: 11

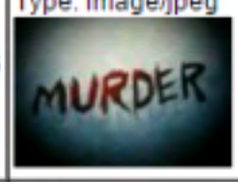
#	Number	Message	Time	Type
12	+[redacted]9956	Filename: IMG-20141231-WA0001.jpg Type: image/jpeg 	2014-12-31 10:40:20 UTC	Sent
11	+[redacted]9956	Filename: IMG-20141231-WA0000.jpg Type: image/jpeg 	2014-12-31 10:39:08 UTC	Sent
10	+[redacted]9956	Cya	2014-12-31 08:02:59 UTC	Inbox
9	+[redacted]9956	Ok...keep working. I'll see you later.	2014-12-31 08:02:49 UTC	Sent
8	+[redacted]9956	I m finding possible ways to bring him out,	2014-12-31 08:02:18 UTC	Inbox
7	+[redacted]9956	Yes yes...i am. How abt d murder case lodged on jimmy?	2014-12-31 08:01:58 UTC	Sent
6	+[redacted]9956	U find a way to social engineer on him	2014-12-31 08:00:31 UTC	Inbox
5	+[redacted]9956	I'll give d exploit asap	2014-12-31 08:00:12 UTC	Inbox
4	+[redacted]9956	His mobile might contain very important sensitive information like credit and debit card numbers. Make it fast	2014-12-31 07:59:43 UTC	Sent
3	+[redacted]9956	I am working on it...will write a suitable exploit soon	2014-12-31 07:58:41 UTC	Inbox

FIGURE 2.20: Viewing Call Logs

24. Andriller stores all the multimedia files shared via messenger applications in separate directories.

25. For instance, if the device has WhatsApp application installed in it, Andriller creates a directory named **wa_media**, creates subfolders for images, audio and video clips and places the respective files in them.

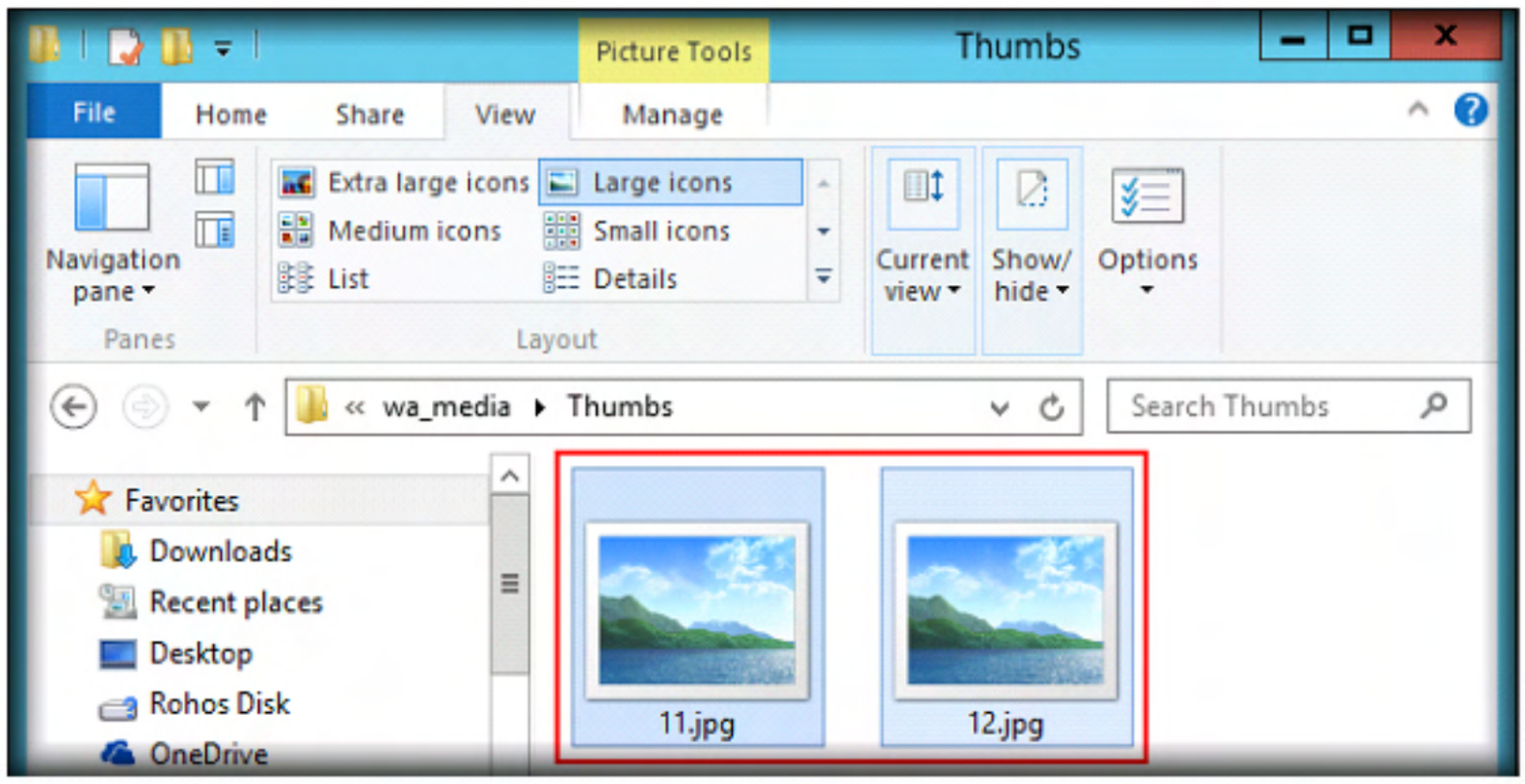


FIGURE 2.21: Viewing the WhatsApp media files

26. This way, you can use the Andriller tool to grab sensitive information like contacts, call logs, messages, decrypted Wi-Fi passwords, etc.
27. If you are performing a forensic investigation on a device locked with a gesture or a password, you can use this tool to bypass the locks and gain direct access to the mobile device.

Lab Analysis

Analyze the result and Document the findings of the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs