Chapter 13: Use the Autopsy Forensic Browser tool in Kali Linux

1. Start and login to your Kali Linux virtual machine as user kali with a password of **kali**.

2. From a terminal window, type **sudo autopsy**. This will start autopsy and present a message (such as http://localhost:9999/autopsy) stating how to connect to Autopsy from a web browser.

3. Right-click the listed http link and choose **Open Link**. This will take you to the local autopsy web page.

4. At the bottom center of the web page, click **New Case**. For the case name type **Case1**, then fill in fictitious description and investigator names. Click **New Case** at the bottom left.

5. Click **Add Host**. Enter a fictitious host name and click the **Add Host** button at the bottom left.

6. Click **Add Image**, then **Add Image File**.

7. For **1. Location**, type **/home/kali/samplepartition.img**. This is a sample disk partition image file of a Window NTFS file system.

8. For **2. Type**, choose **Partition**. Click **Next**.

9. Choose **Calculate the hash value for this image**. Click **Add**.

10. Once the MD5 hash is calculated, click **OK**, then click **Analyze**, then click **File Analysis**.

11. In the right panel, scroll down and click the **del1** folder listing.

12. Notice **file6.jpg** shows as red because the file is deleted.

13. Click **file6.jpg** to view the file contents in the lower panel.

14. In the middle panel, click the **Export** link to save the jpg file as a standalone file. Click **Save File** then click **OK**.

15. Click the folder icon in the upper left of the screen. Navigate to the Downloads folder in the kali home directory.

16. Double-click the jpg file to ensure it opens.