

Cloud Forensics

Module 10

Investigating Cloud Storage Services

Cloud Forensics is the process of identifying criminal activity and the people behind the crime performed over a cloud storage service. It includes the processes of sniffing, recording, acquisition, and analysis of the traffic and events to investigate the incident.

Lab Scenario

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Nathan, who is working as a software developer at an Austrian firm, has found that the files he had placed on the cloud storage are missing frequently. He has lodged a complaint with the company's administration team, which has hired an investigator to look into the matter. According to Nathan, the missing files are pretty important and the investigator needs to recover them if possible.

To perform an investigation over the cloud storage services, the investigator needs to have deep knowledge of their working as well as know how they allow users to store, access, and modify the data over the cloud.

The labs in this module will help you understand the working of the most used cloud storage services, such as Google Drive and Dropbox.

Lab Objectives

The objective of this lab is to help students in conducting investigation of cloud storage services such as Google Drive and Dropbox.

Lab Environment

In this lab, you need:

- A computer running Windows 10 virtual machine
- A Web browser with Internet access
- Administrative privileges to run tools and perform scans

Lab Duration

Time: 75 Minutes

Overview of Investigating Cloud Storage Services

Investigating Cloud Storage Services is a process of finding the source of attack over a cloud storage. The process includes analysis of accounts, devices, and applications used to access the accounts linked to clouds as well as traffic and events to identify the perpetrator.

 **Tools demonstrated in this lab are available in Z:\CHFIv9 Module 10 Cloud Forensics**

**T A S K 1****Overview**

Lab Tasks

Recommended labs to assist you in investigating cloud storage services:

- Forensic investigation of Dropbox.
- Forensic investigation of Google Drive.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

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

Lab

1

Forensic investigation of Dropbox

Dropbox offers a variety of access options such as desktop client, mobile application, and through a web browser. Every option leaves traces of Dropbox access that you can recover.

Lab Scenario

Forensics investigation of Dropbox will include the process of knowing whether the user had used a client or browser to access the Dropbox account. This lab will help in understanding the changes Dropbox makes in a system when a user tries to access through all the possible sources.

If the perpetrator has uninstalled the Dropbox client from the system, you should be able to gather data about the usage of the cloud storage service. During the process of uninstalling a client or application, the system would only delete some files such as config and retain the remaining ones. This lab will help you understand which files the system would delete and retain.

Lab Objectives

This lab will help you understand how to perform system scanning to find the files, folders, registry, and other resources modified when someone tries to access a Dropbox account. This knowledge will help you trace and gather all the possible evidences of an attack on Dropbox and investigate further.

Lab Environment

To carry out the lab, you need:

- A computer running Windows 10.
- Admin Rights to run the tools.
- Tools including Regshot, WhatChanged, Disk Pulse, RAM Capturer, HxD and WebBrowserPassView.

ICON KEY



Valuable
information



Test
knowledge



Web exercise



Workbook review



**Tools
demonstrated in
this lab are
available in
Z:\CEHv9 Module
10 Cloud
Forensics**

Lab Duration

Time: 40 Minutes

Overview of Dropbox Investigation

The process includes searching of system files, registries, history, and cache folders to find the traces of Dropbox and use them as evidence to proceed.

Lab Tasks



TASK 1

Launch Regshot

1. Before beginning this lab, log in to **Windows 10** virtual machine and install WhatChanged, Disk Pulse, Directory Monitor, RAM Capturer, HxD, and WebBrowserPassView tools from the location: **Z:\CHFIV9 Module 10 Cloud Forensics**
 - a. WhatChanged: **Z:\CHFIV9 Module 10 Cloud Forensics\Registry Changes Tracking Tools\WhatChanged Portable**
 - b. Disk Pulse: **Z:\CHFIV9 Module 10 Cloud Forensics\Registry Changes Tracking Tools\Disk Pulse**
 - c. Directory Monitor: **Z:\CHFIV9 Module 10 Cloud Forensics\Registry Changes Tracking Tools\Directory Monitor**
 - d. RAM Capturer: **Z:\CHFIV9 Module 10 Cloud Forensics\RAM Capturer**
 - e. HxD: **Z:\CHFIV9 Module 10 Cloud Forensics\Hex Editor Tools\HxD**
 - f. WebBrowserPassView: **Z:\CHFIV9 Module 10 Cloud Forensics>Password Recovery Tools\WebBrowserPassView**
2. The regshot tool allows you to compare the amount of registry entries that have been changed during an installation or a change in your system settings. So, we shall install Dropbox client on the machine.
3. Navigate to **Z:\CHFIV9 Module 10 Cloud Forensics\Dropbox Investigation Tools\Regshot**, and double-click **Regshot-x64-ANSI.exe** to launch the application.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**. If a **User Account Control** pop-up appears, click **Yes**.

- To capture the snapshot of the system, click the **1st shot** button and select the **Shot** option from the drop-down list.

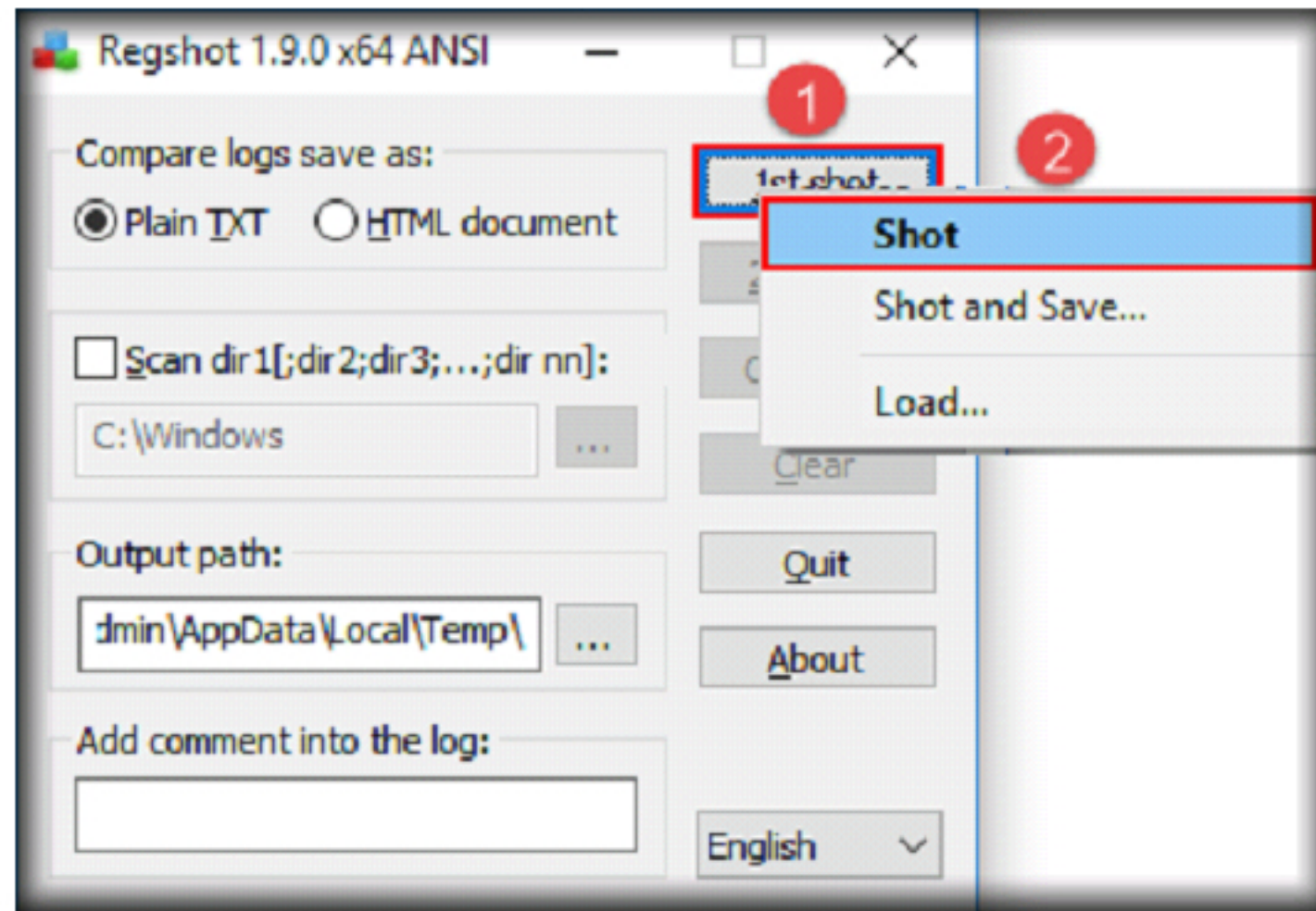


FIGURE 1.1: Capturing a snapshot of the system using Regshot

- After taking the snapshot, investigator needs to find the files that change when an user installs a cloud application.
- Navigate to the following location: **Z:\CHFIV9 Module 10 Cloud Forensics\Registry Changes Tracking Tools\WhatChanged Portable**, and double-click **WhatChangedPortable.exe** to launch the application. WhatChanged GUI appears; check the **Scan Registry** and **LOCAL MACHINE** options from **Scan Items**.
- Click the **Step #1: Get Baseline State** button.

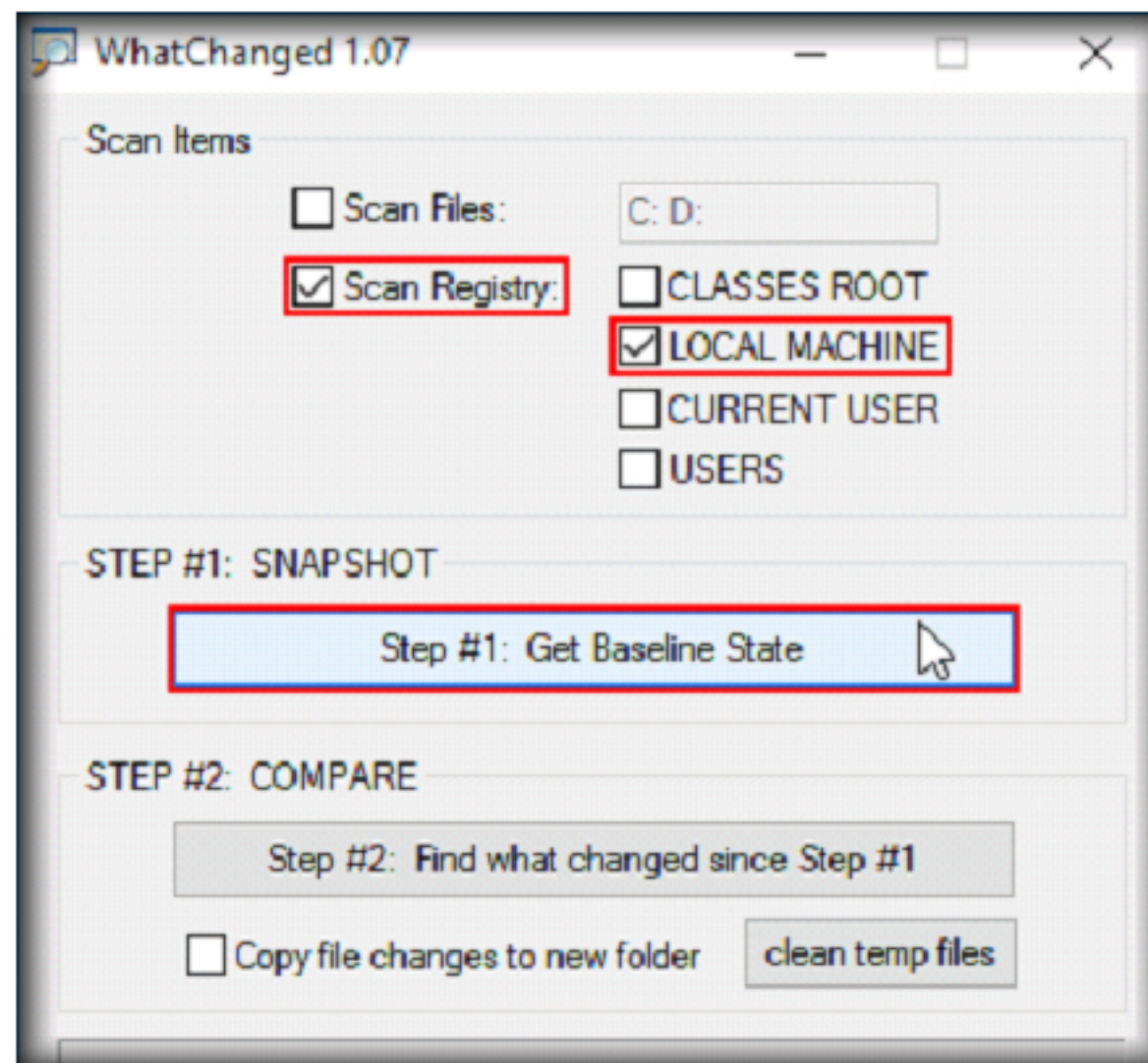


FIGURE 1.2: Performing step 1 in WhatChanged tool

8. The tool will also generate a notepad file with the name **WhatChanged_Snapshot1_Registry_HKLM** in same folder as the location of the executable. The notepad contains all the local machine addresses.

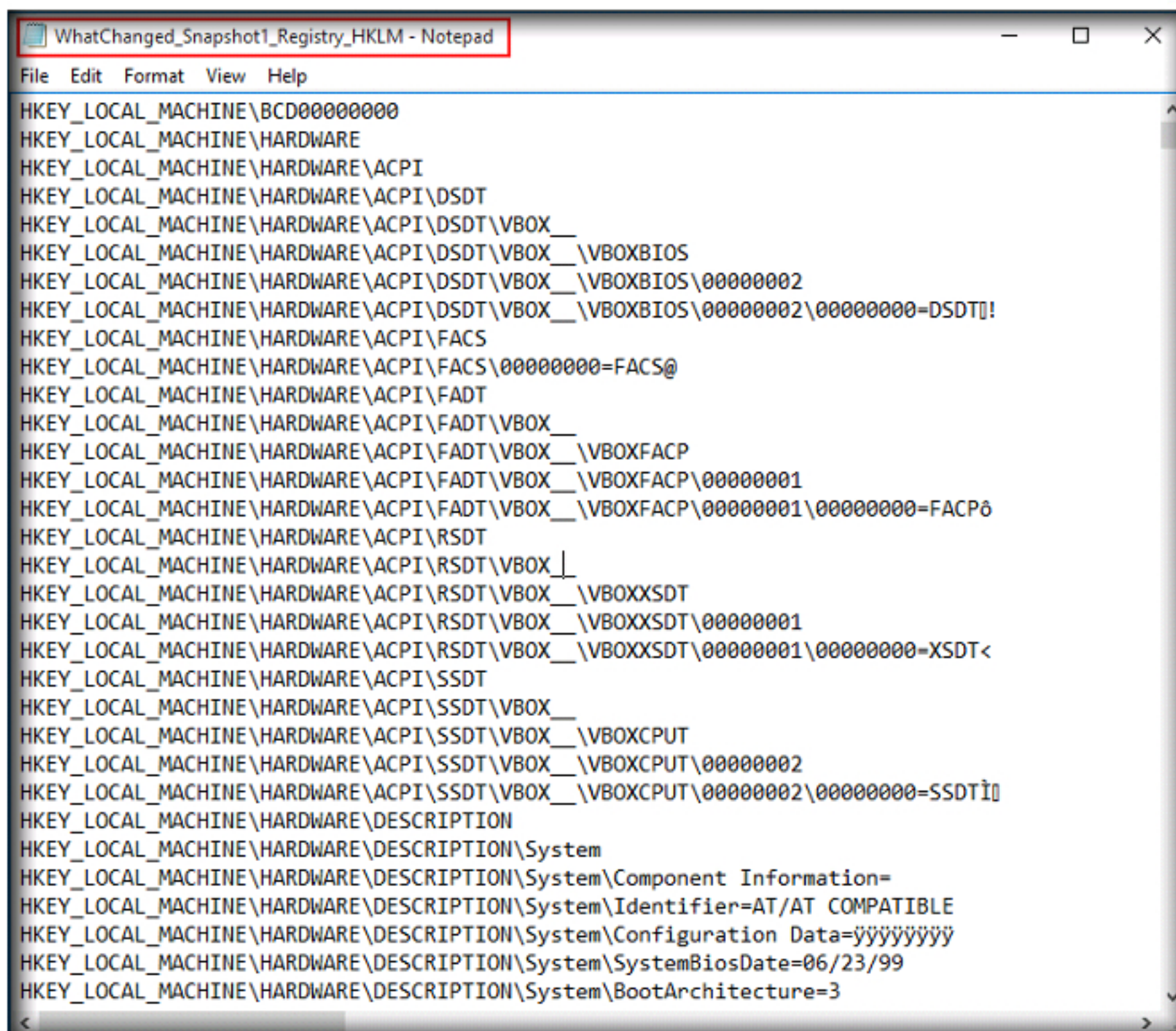


FIGURE 1.3: Notepad file containing all the local machine addresses

9. Navigate to **Z:\CHFIv9 Module 10 Cloud Forensics\Registry Changes Tracking Tools\Disk Pulse**, double-click **diskpulse_setup_v8.7.26.exe** and follow the wizard driven installation steps to install the application. At the final step of installation, ensure that both the options Run Disk Pulse 8.7.26 and Add Disk Pulse Desktop Icon are checked and click **Finish**.
10. **Disk Pulse** GUI appears, click the **Monitor** icon from the toolbar.

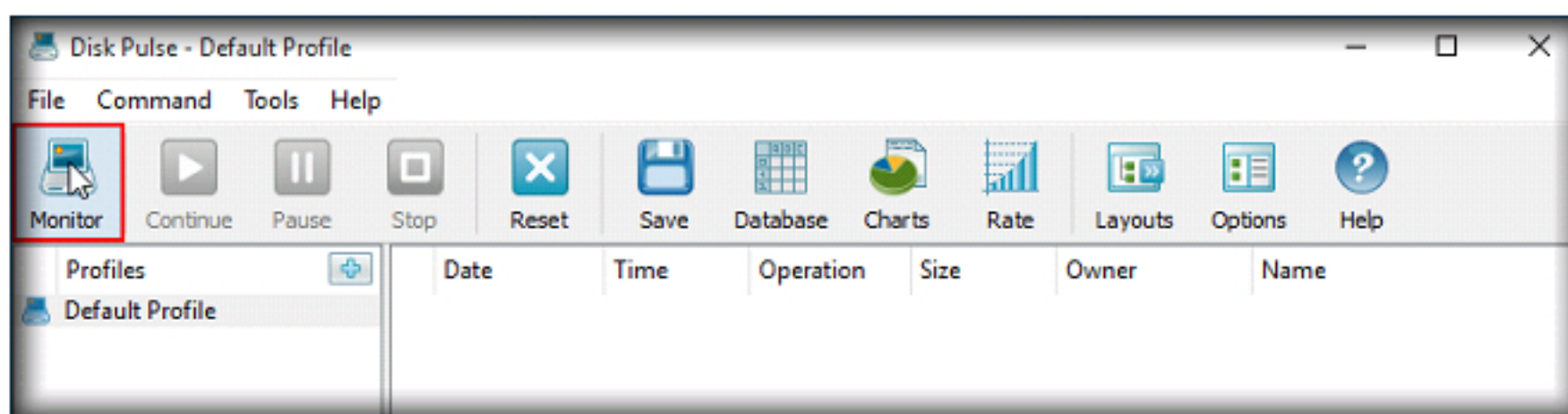


FIGURE 1.4: Clicking on Monitor option in Disk Pulse tool

11. The tool will display a window to add folders that you need to monitor. The tool adds **C:** folder by default. Click the **Add** button to add new folders.
12. Click **Start** button to initiate monitoring of the **C:** folder.

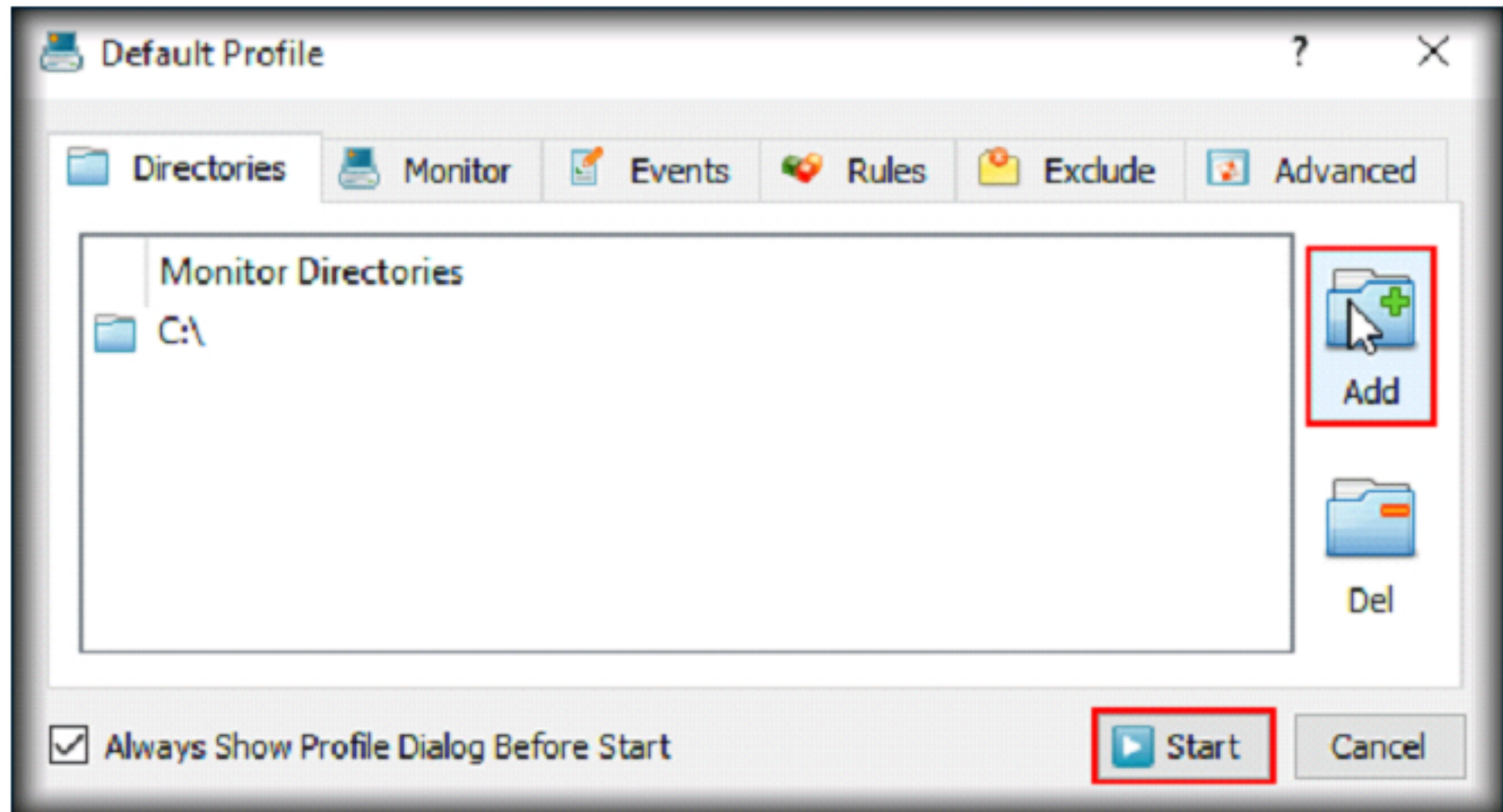


FIGURE 1.5: Starting monitoring of the selected folder

13. The investigator should observe the changes and application makes to the directories in the local system folder.
14. Navigate to **Z:\CHFIV9 Module 10 Cloud Forensics\Registry Changes Tracking Tools\Directory Monitor**, double-click **DirectoryMonitor2_21061_Setup.exe** and follow the wizard driven installation steps to install the application. It takes some time for the installation to complete. At the final step of installation, check **Launch Directory Monitor** option and click **Finish**.
15. Directory Monitor GUI appears, click the **Add** button to add the directory you need to monitor.

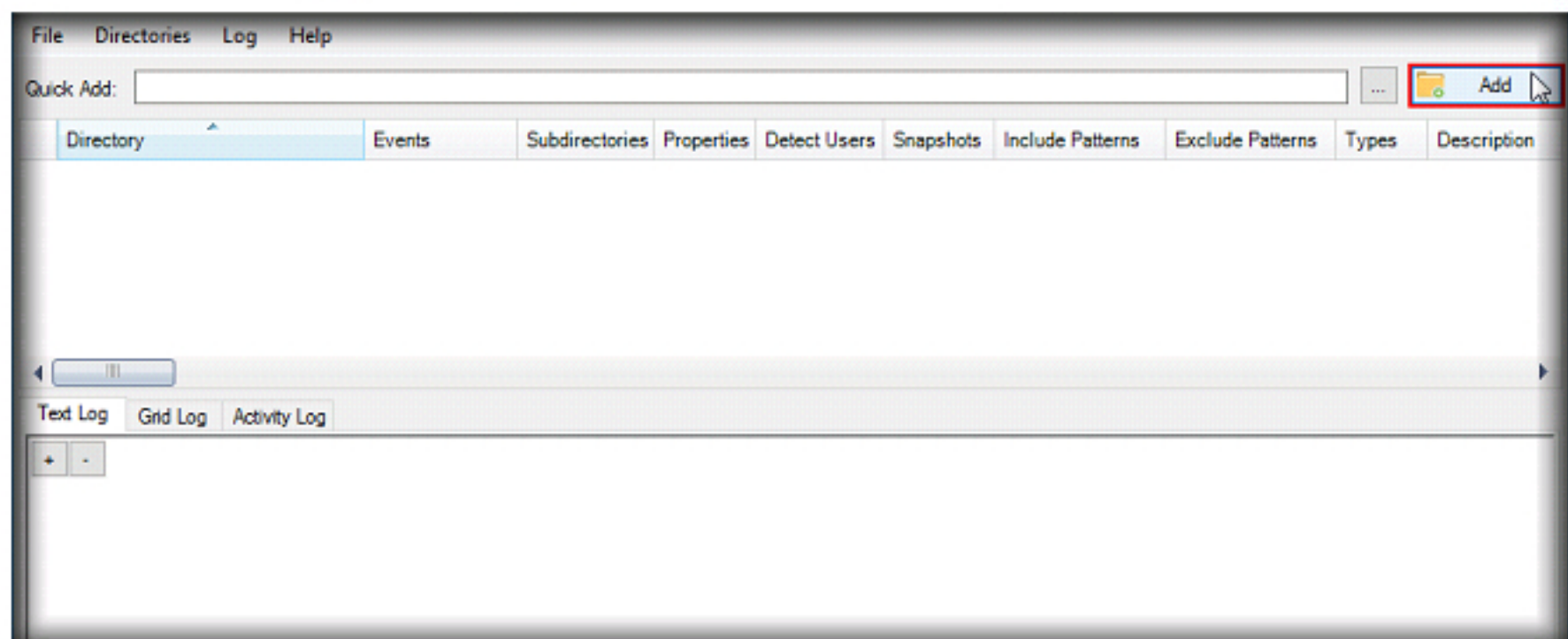


FIGURE 1.6: Directory Monitor main window with Add button highlighted

16. Click the **Ellipsis (...)** button to add the directories you need to monitor.

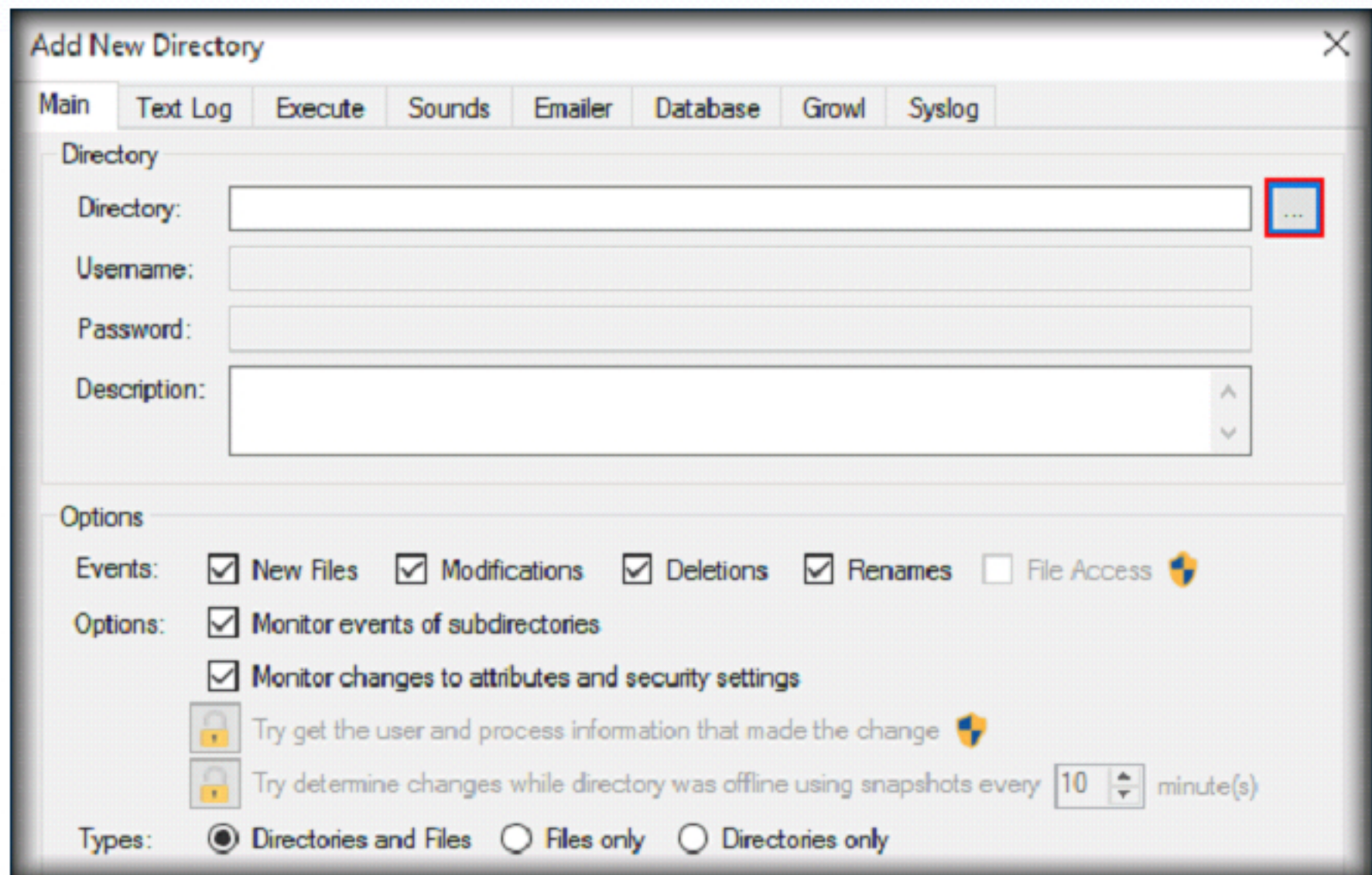


FIGURE 1.7: Adding directories to be monitored using ellipsis button

17. Navigate to location of the folder, select the folder, and click the **Select Folder** button.

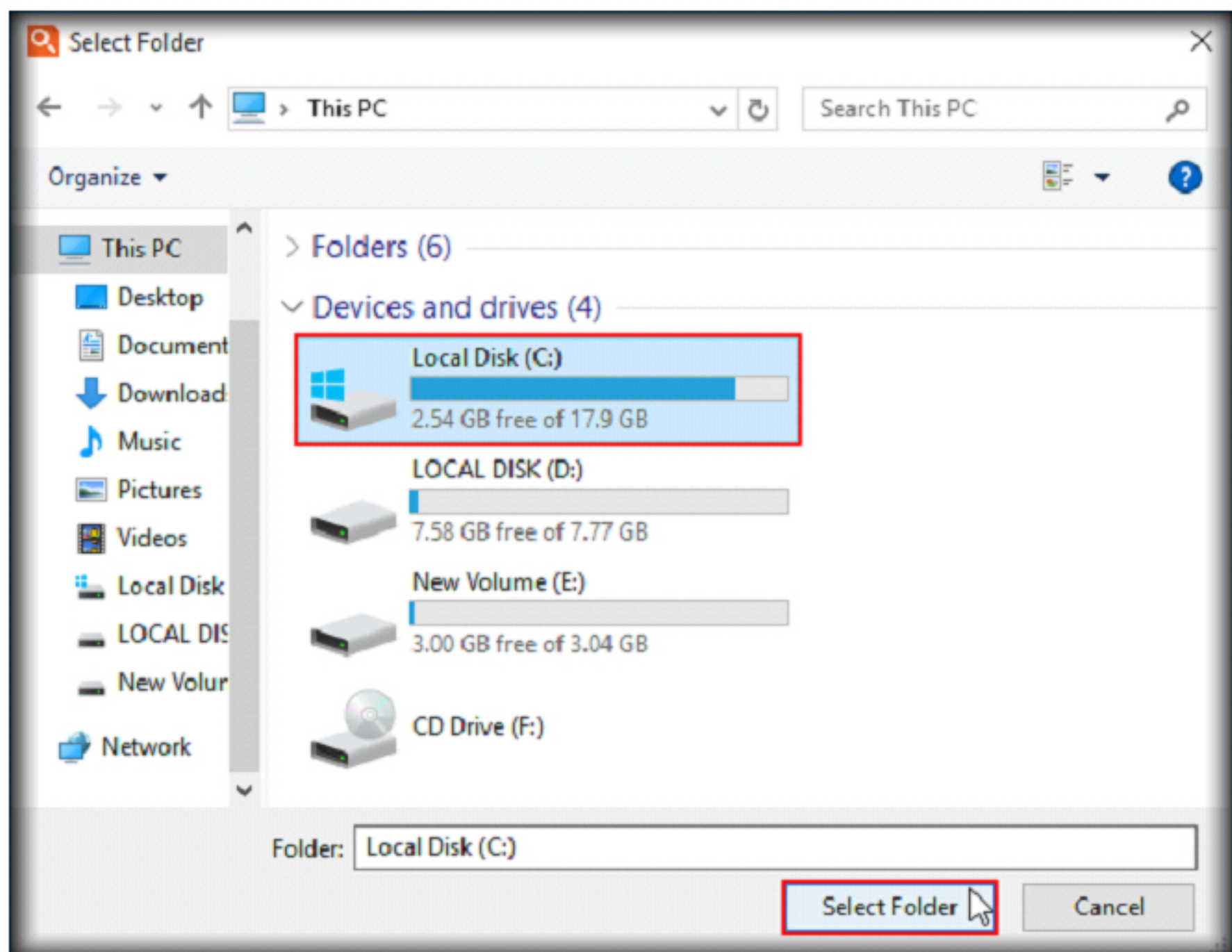


FIGURE 1.8: Navigating to the location and selecting the respective folder

18. Select the required **Events**, **Options**, and **Types** from the **Options** section, and click the **Save** button. The tool will start recording all the activities from the selected folder and present them in the log activity in the form of **Text Log**, **Grid Log**, and **Activity Log**.

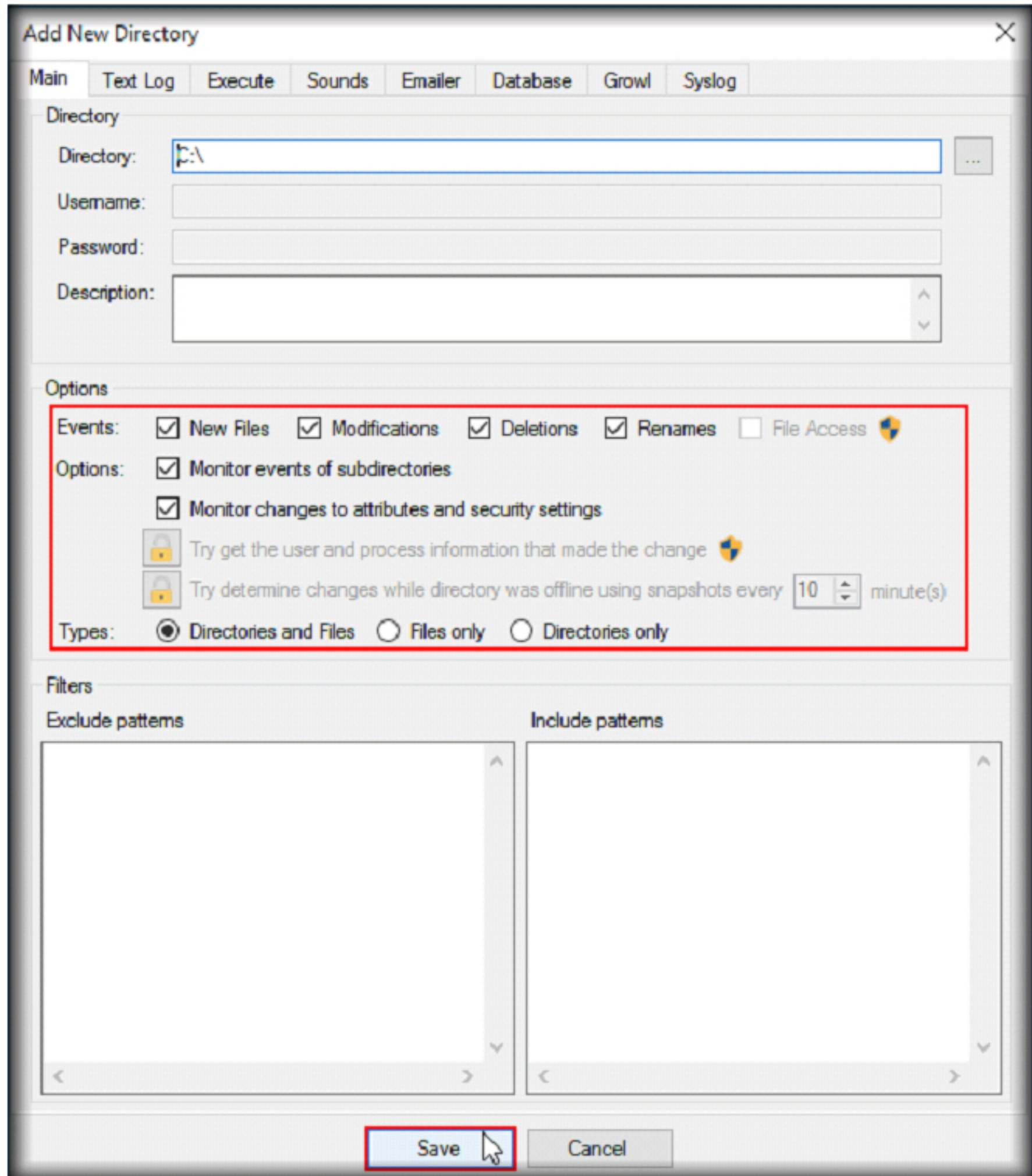


FIGURE 1.9: Saving all the required options and starting recording

19. To install the Dropbox client on the system, navigate to the location: **Z:\CHFIv9 Module 10 Cloud Forensics\Dropbox Investigation Tools\Dropbox Installer** double-click **DropboxInstaller.exe** and follow the wizard driven installation steps. Once you complete the installation process, sign in into the Dropbox account.

20. Now go to the already running **Disk Pulse** tool and pause the recording by clicking on the **Pause** button.

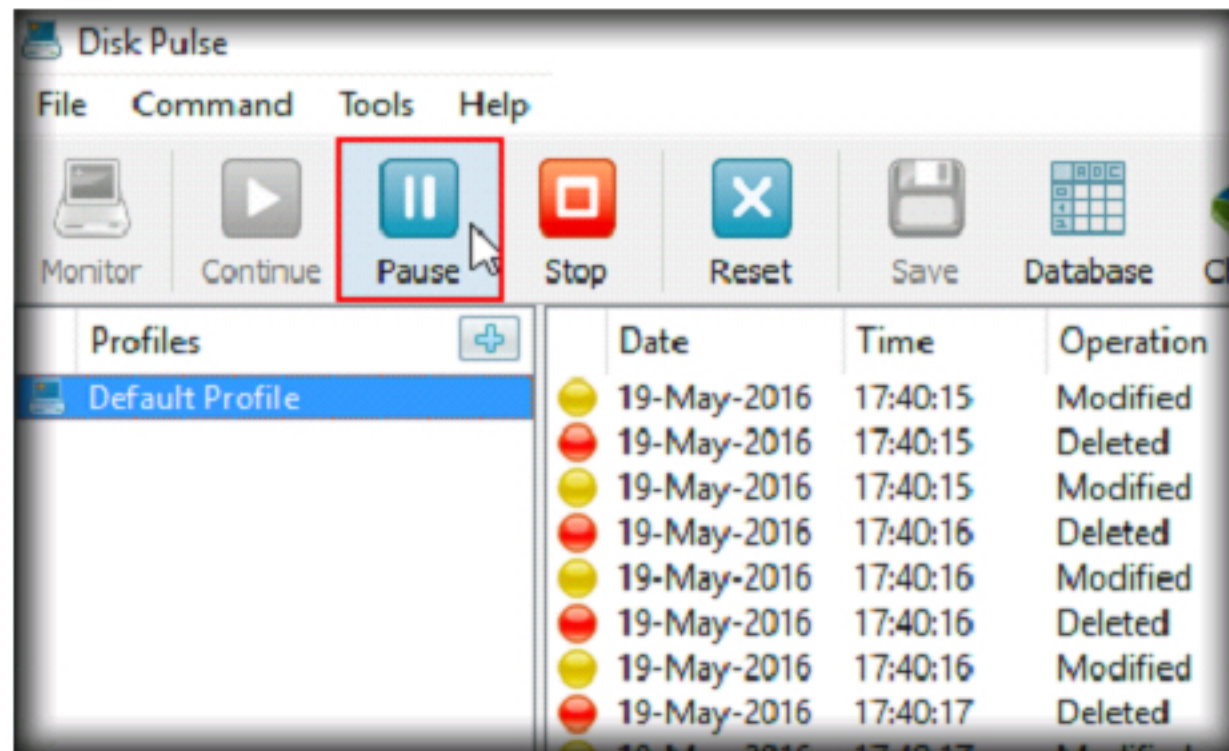


FIGURE 1.10: Pausing recording in the Disk Pulse tool

21. Select all the changes Disk Pulse has noted, right click the results, and click **Copy Changes To Clipboard** option.

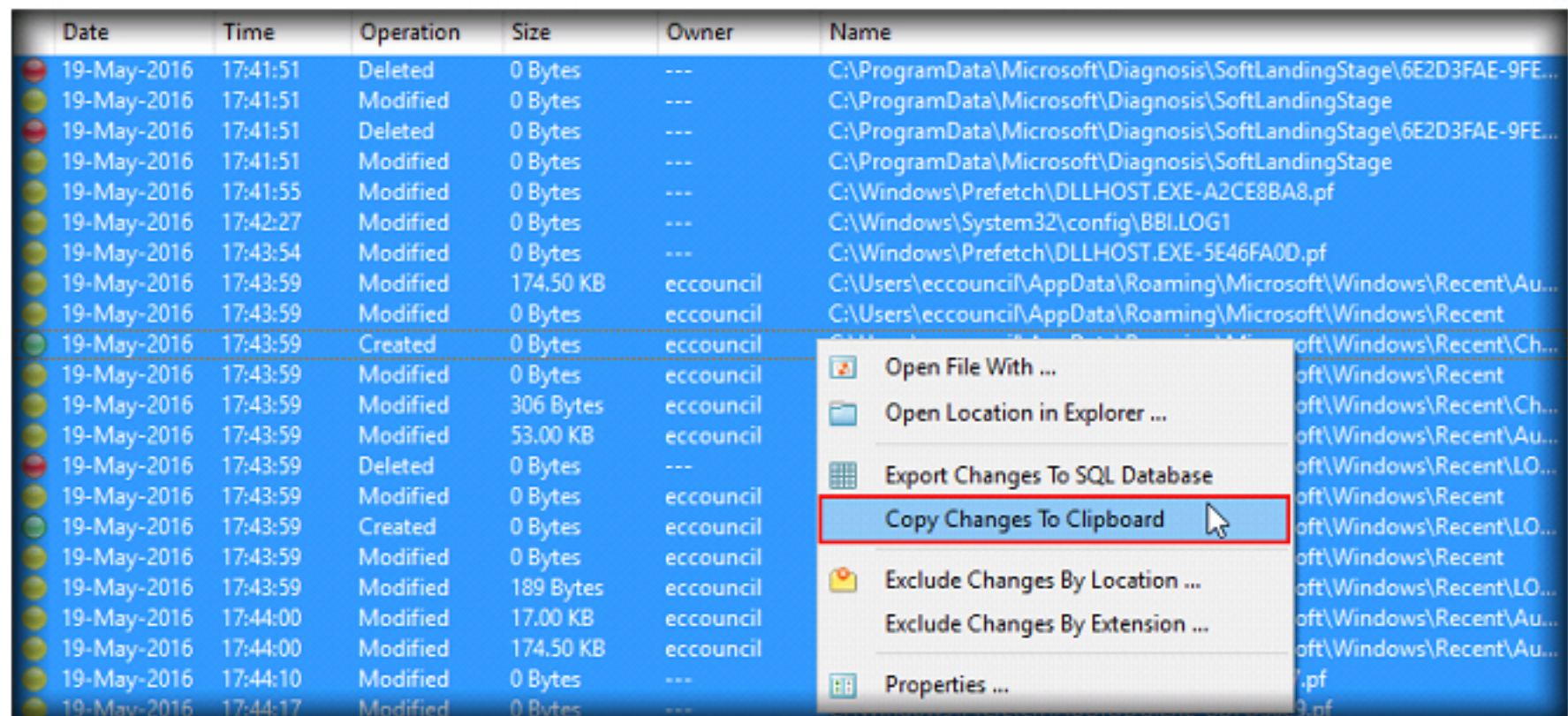


FIGURE 1.11: Copying the changes to the clipboard

22. Copy the changes to a text file for easy analysis. The tool provides details of all the folders modified during installation, thus giving a list of addresses to check for traces of Dropbox.

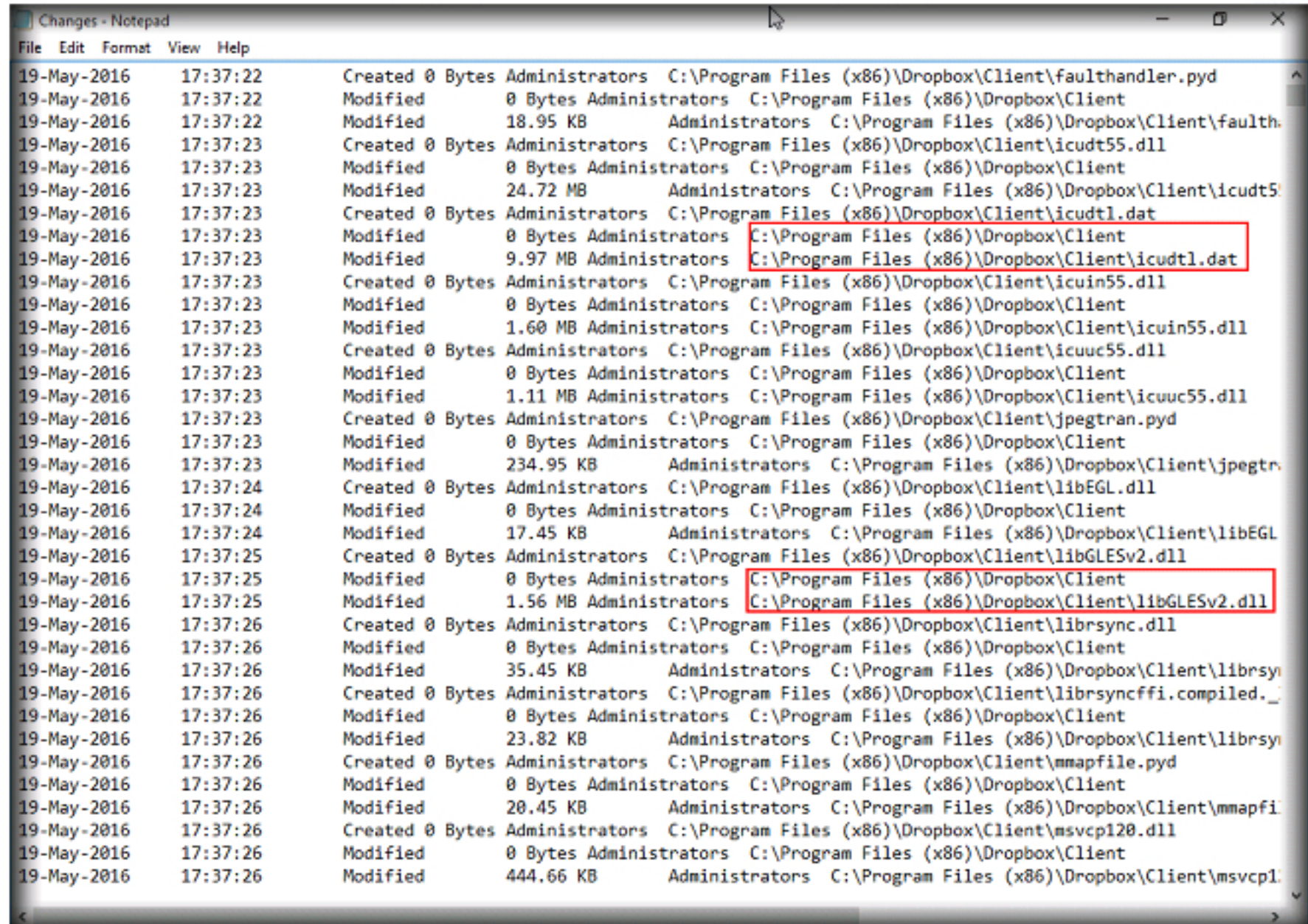
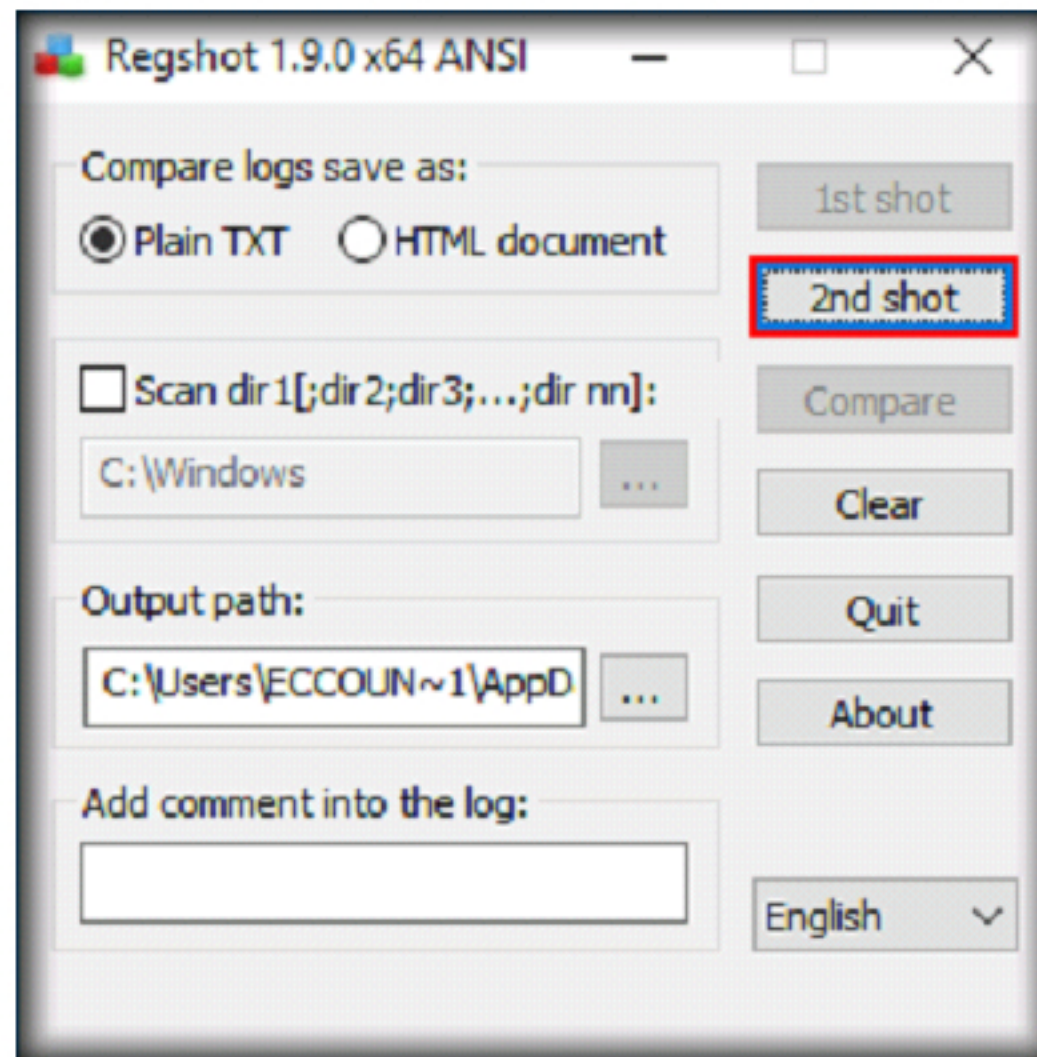


FIGURE 1.12: Viewing the changes in a text file

23. Run the **Regshot** tool. Click the **2nd shot** button to capture the second snapshot of the system.

FIGURE 1.13: Capturing the 2nd snapshot of the system

24. Now click the **Compare** button.

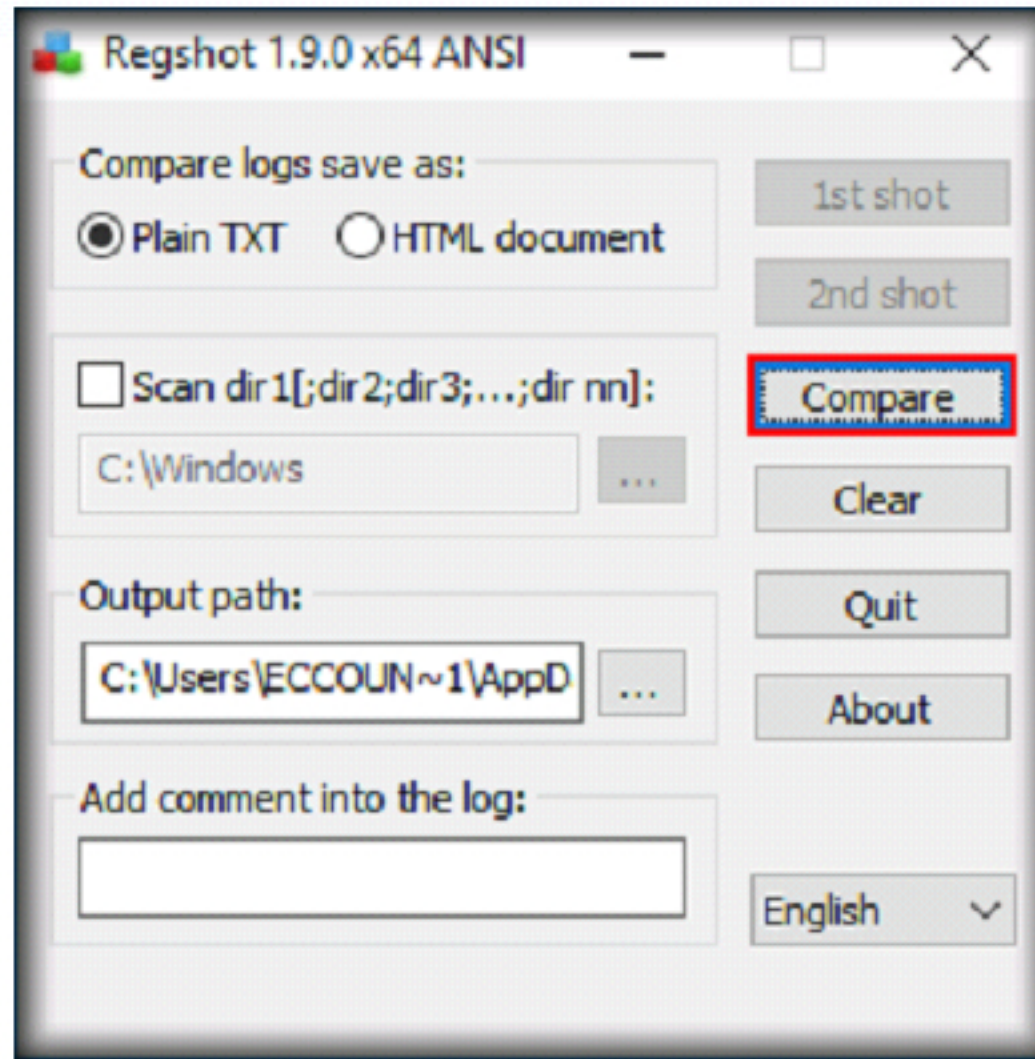


FIGURE 1.14: Comparing the snapshots in the Regshot tool

25. Regshot tool creates a result notepad file that consists of all the changes made to system files.

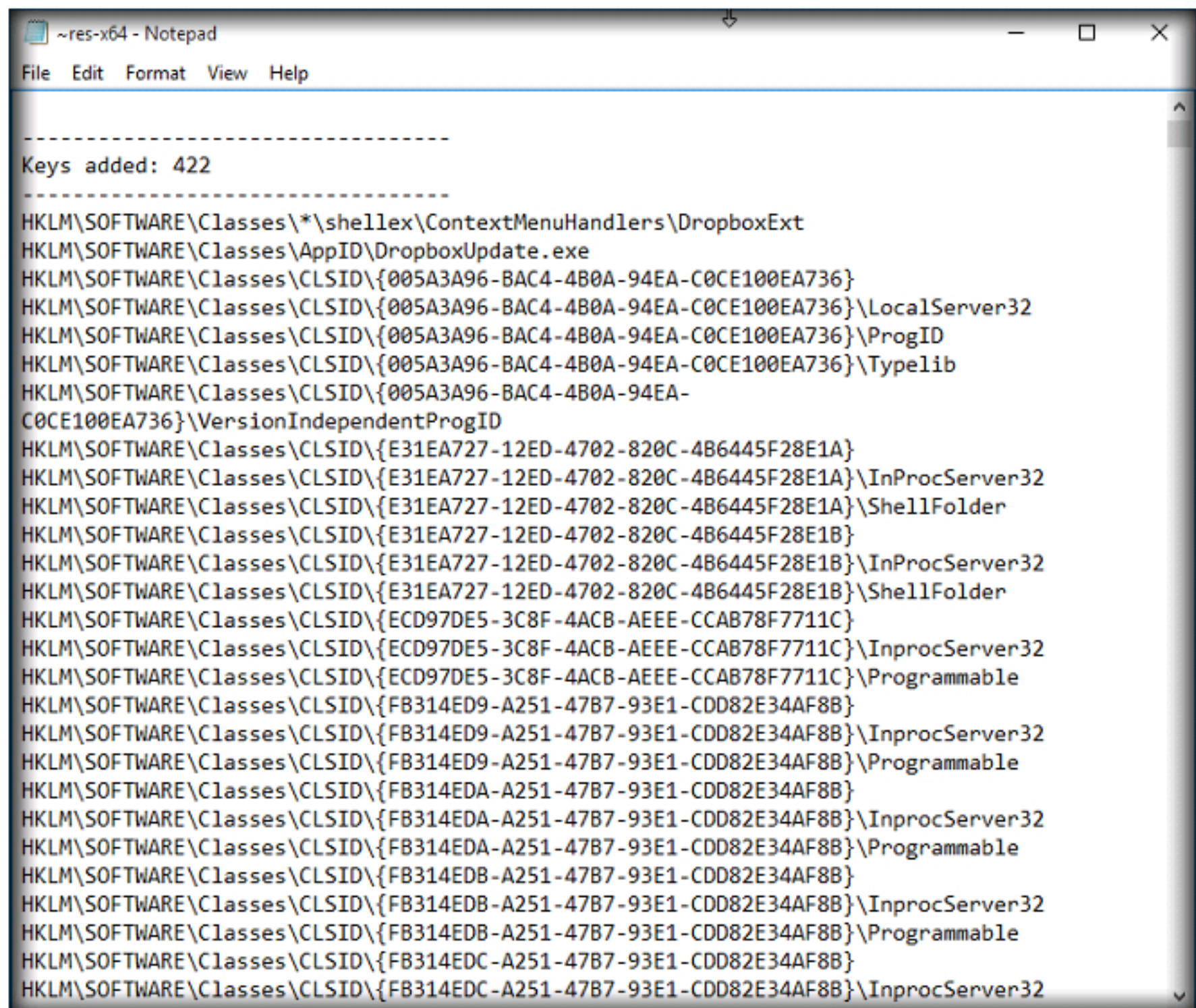


FIGURE 1.15: Viewing the Regshot output file

26. Go to the **WhatChanged** tool, click **Step #2: Find what changed since Step #1** button to take the snapshot of the system.

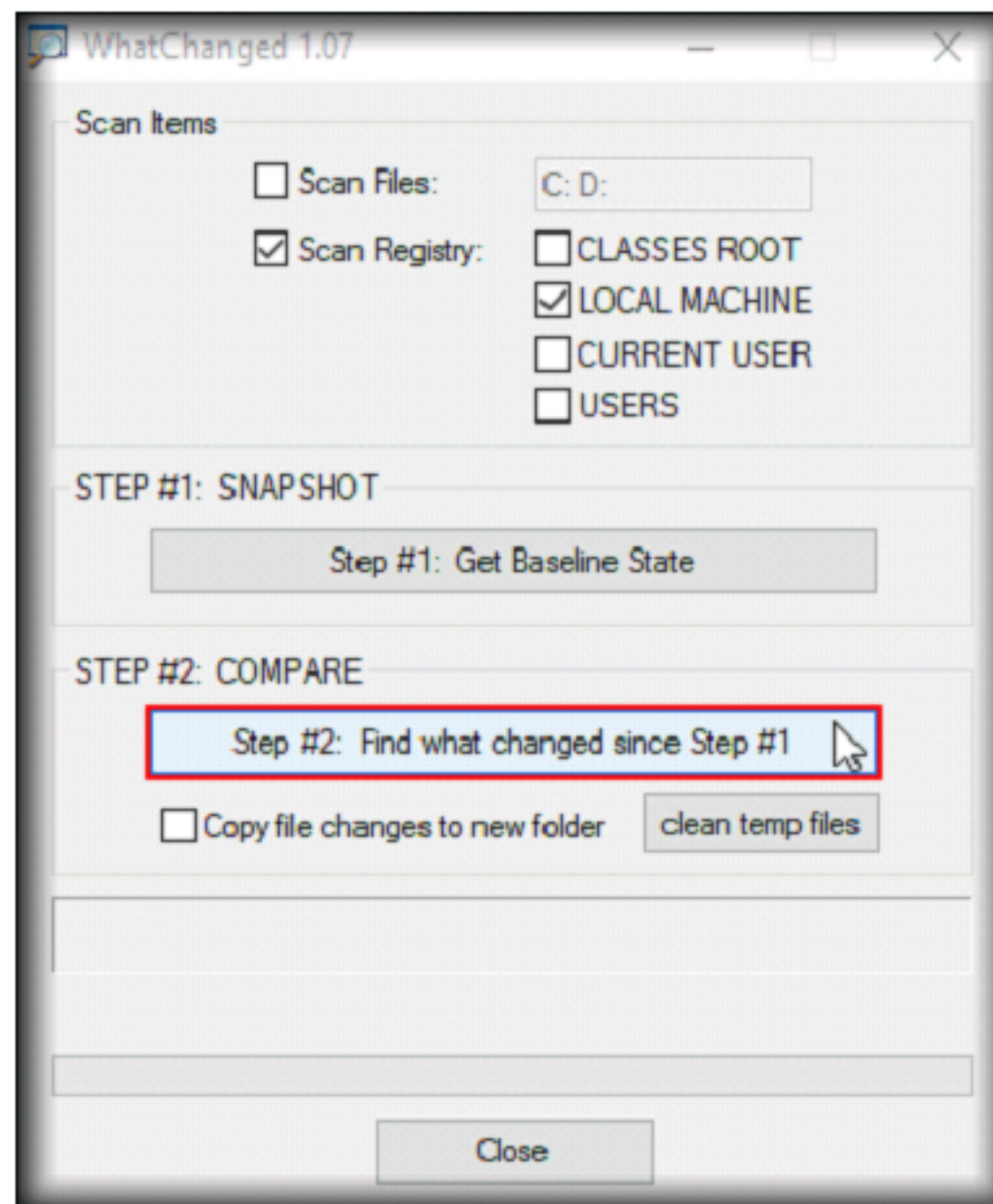


FIGURE 1.16: Executing the Step 2 of the WhatChanged tool

27. The WhatChanged tool will start taking another snapshot of the **LOCAL MACHINE**, while comparing it to the first snapshot. The tool also displays the number of changes made after the first snapshot.

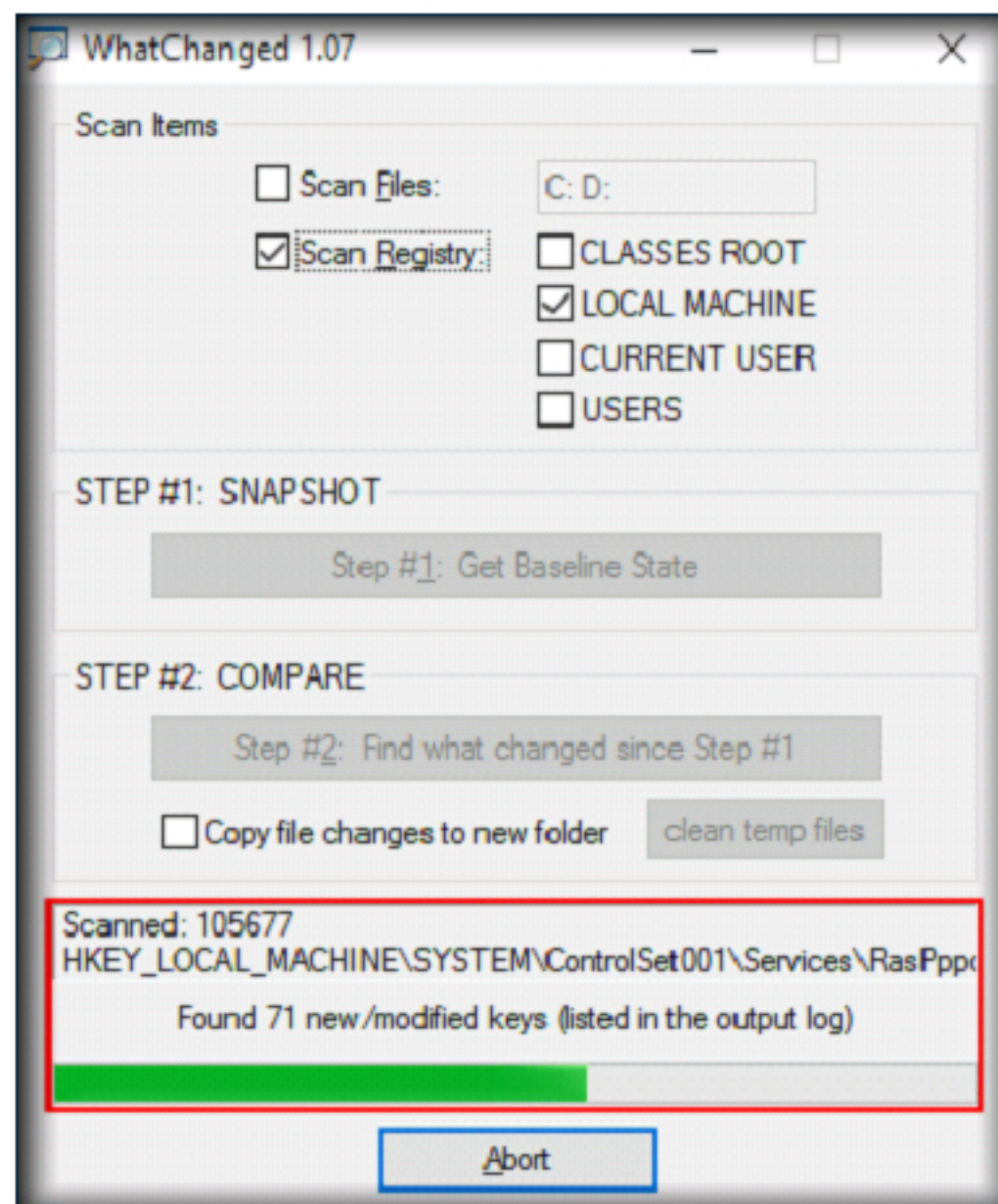


FIGURE 1.17: Comparison under process

28. After scanning the selected folder, the tool prompts a dialog box displaying the number of changes it observed across the selected system.
29. Click the **OK** button.

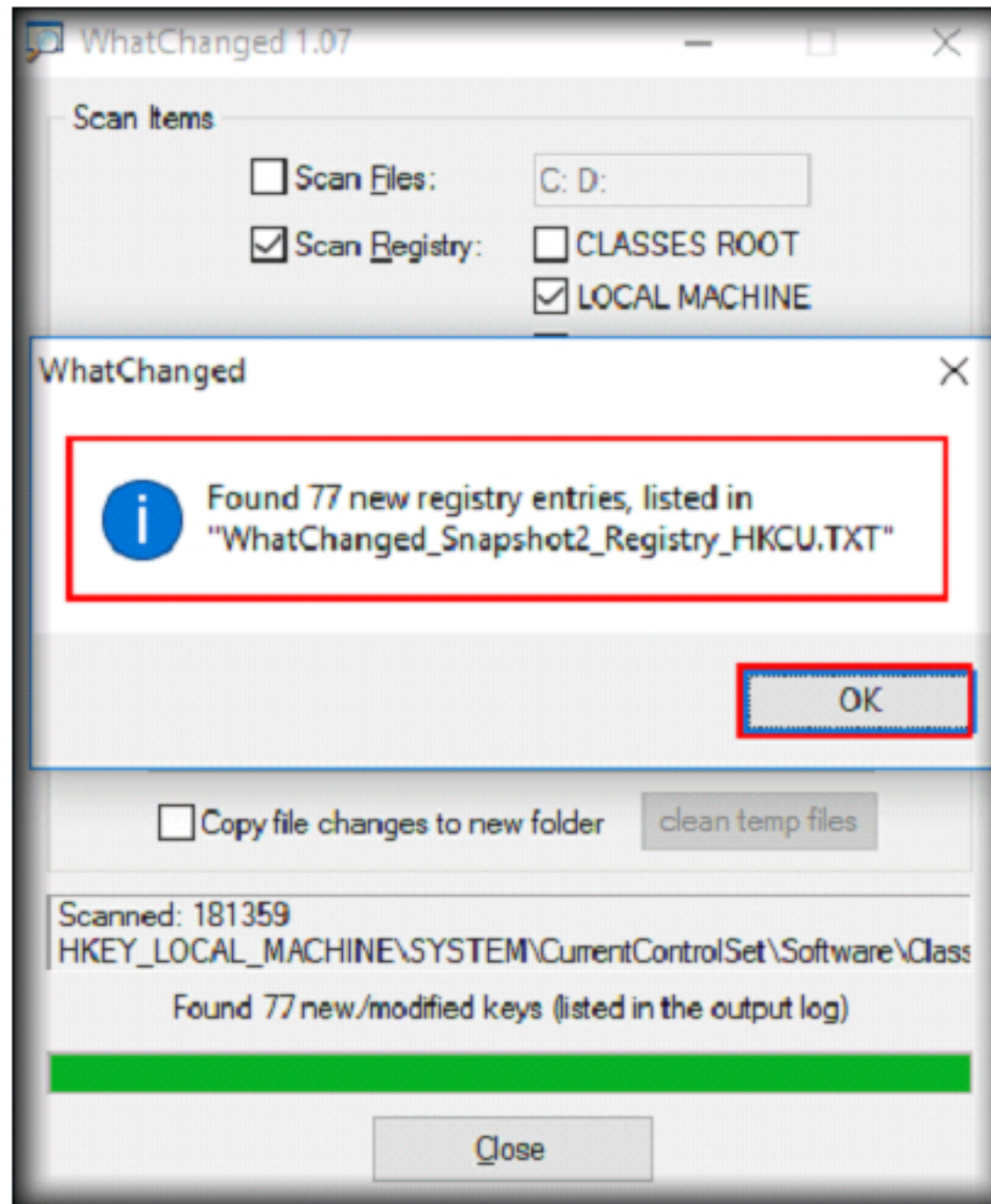


FIGURE 1.18: WhatChanged tool displaying the resultant changes after comparison

30. WhatChanged tool will also create a notepad file with details of the modified LOCAL MACHINE data and store it in the location of its executable, i.e., **Z:\CHFIv9 Module 10 Cloud Forensics\Registry Changes Tracking Tools\WhatChanged Portable**.
31. The notepad consists details of changes made to the **LOCAL MACHINE** along with address and the type of action involved.

32. Here, you can observe that most of the changes are as part of installation of Dropbox onto the system. The folders and addresses reflected in the notepad store traces of information that could help in the investigation of the case.

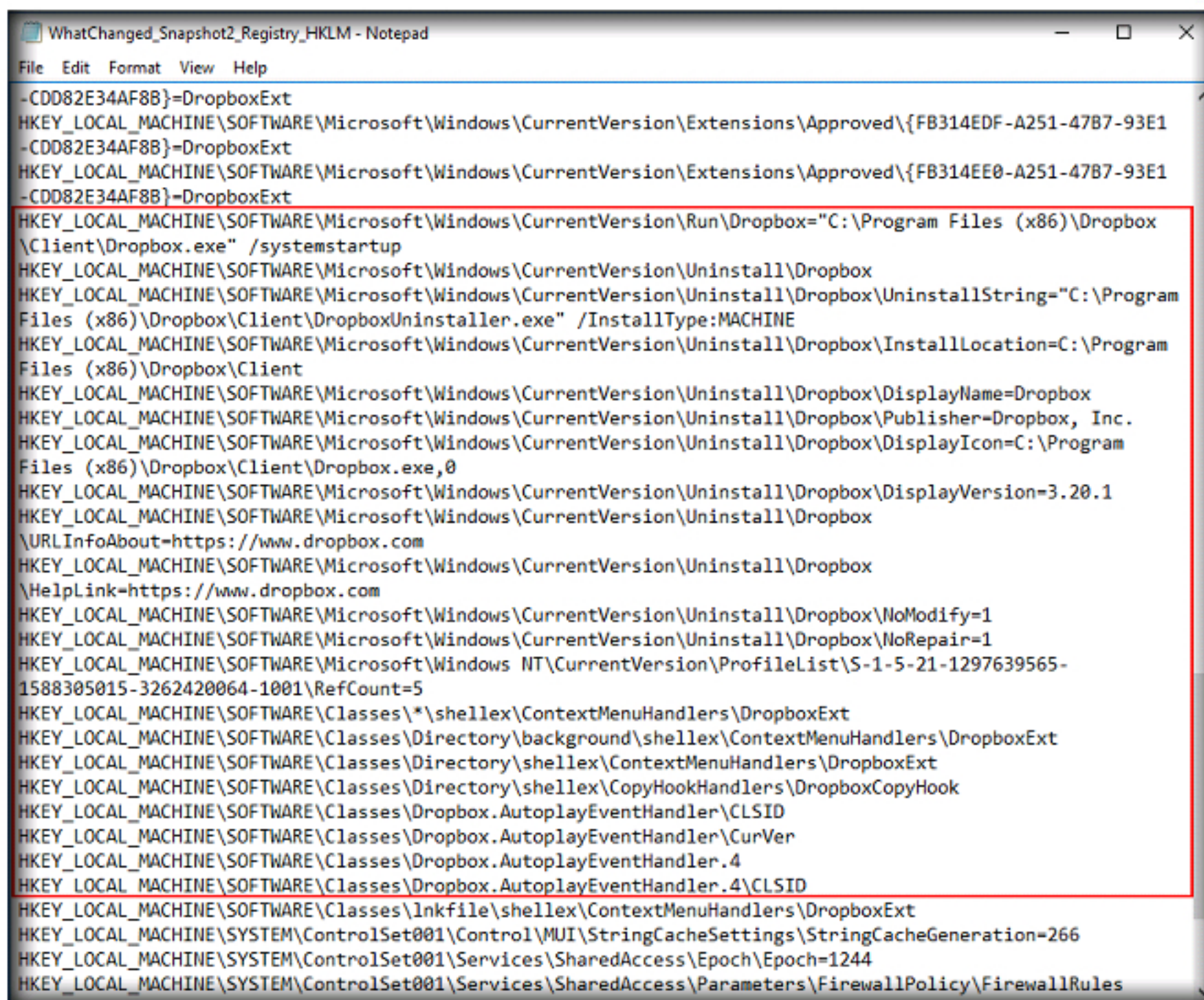


FIGURE 1.19: Notepad file showing the occurred changes

33. Open the already running Directory Monitor program and pause the scan. Right click a process and select **Pause** option from the list.

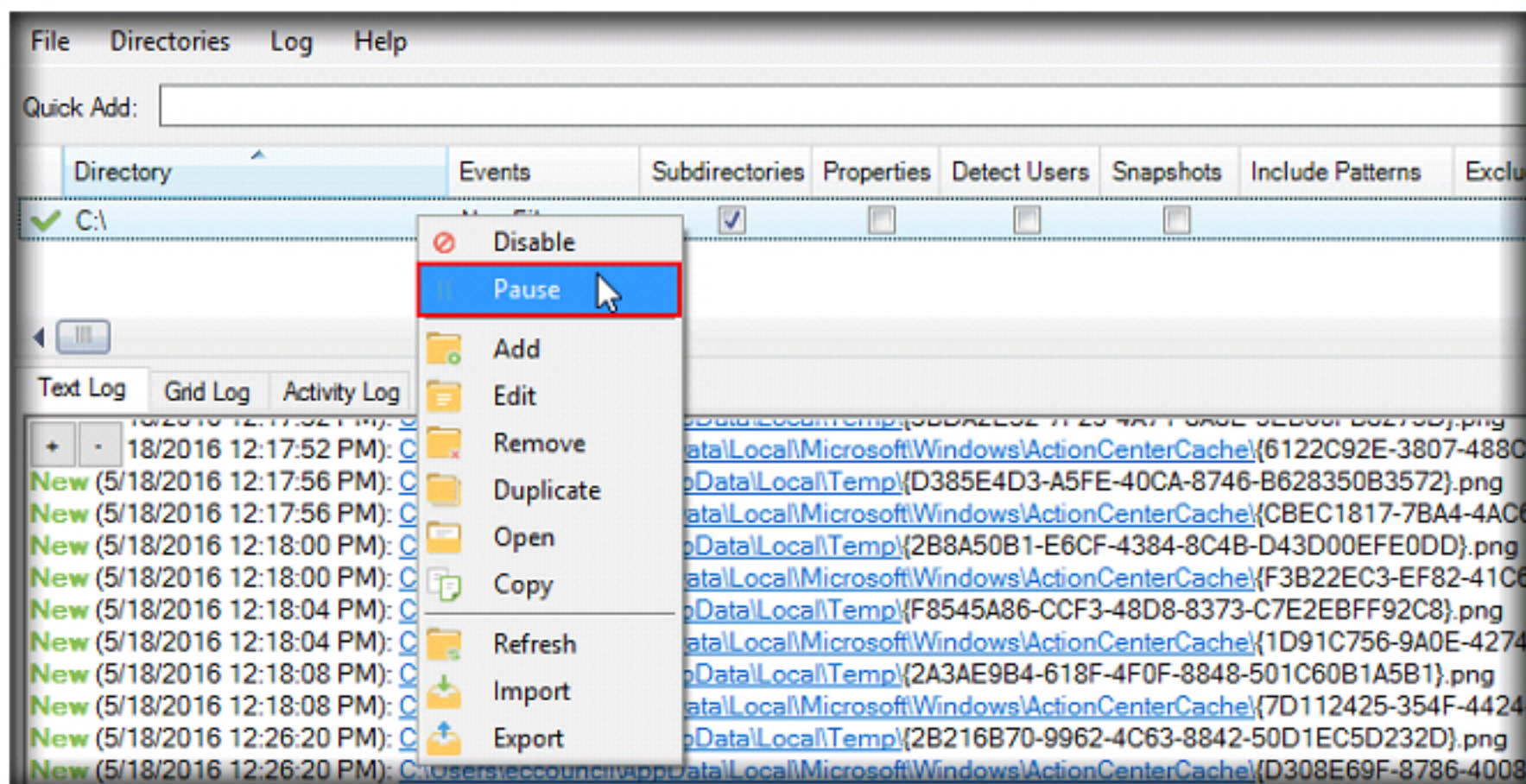


FIGURE 1.20: Pausing the scan of the running Directory monitor program

34. The tool will display all the actions that have contributed to changes in the system. On observing closely, you can see that the Dropbox installation process has added various new directories and folders to various system files.

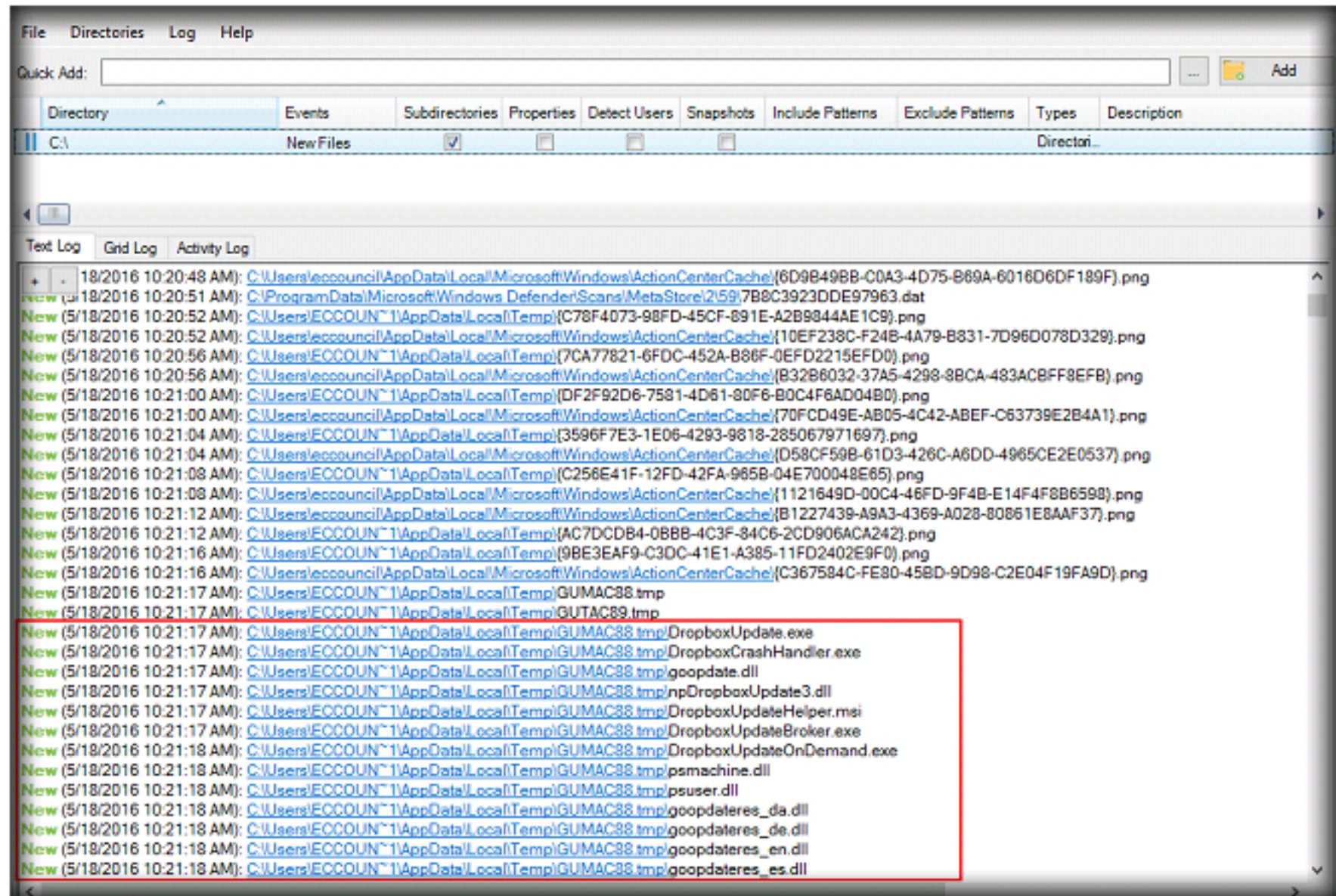


FIGURE 1.21: Screenshot showing the actions involved in Dropbox installation process

35. Open the already running **Disk Pulse** tool. Click the **DBX-JOURNAL Files** in the **Categorize By Extension** section of the tool to view all the changes the Dropbox files make to the system during configuration. All the Dropbox files hold the **.dbx** extension.

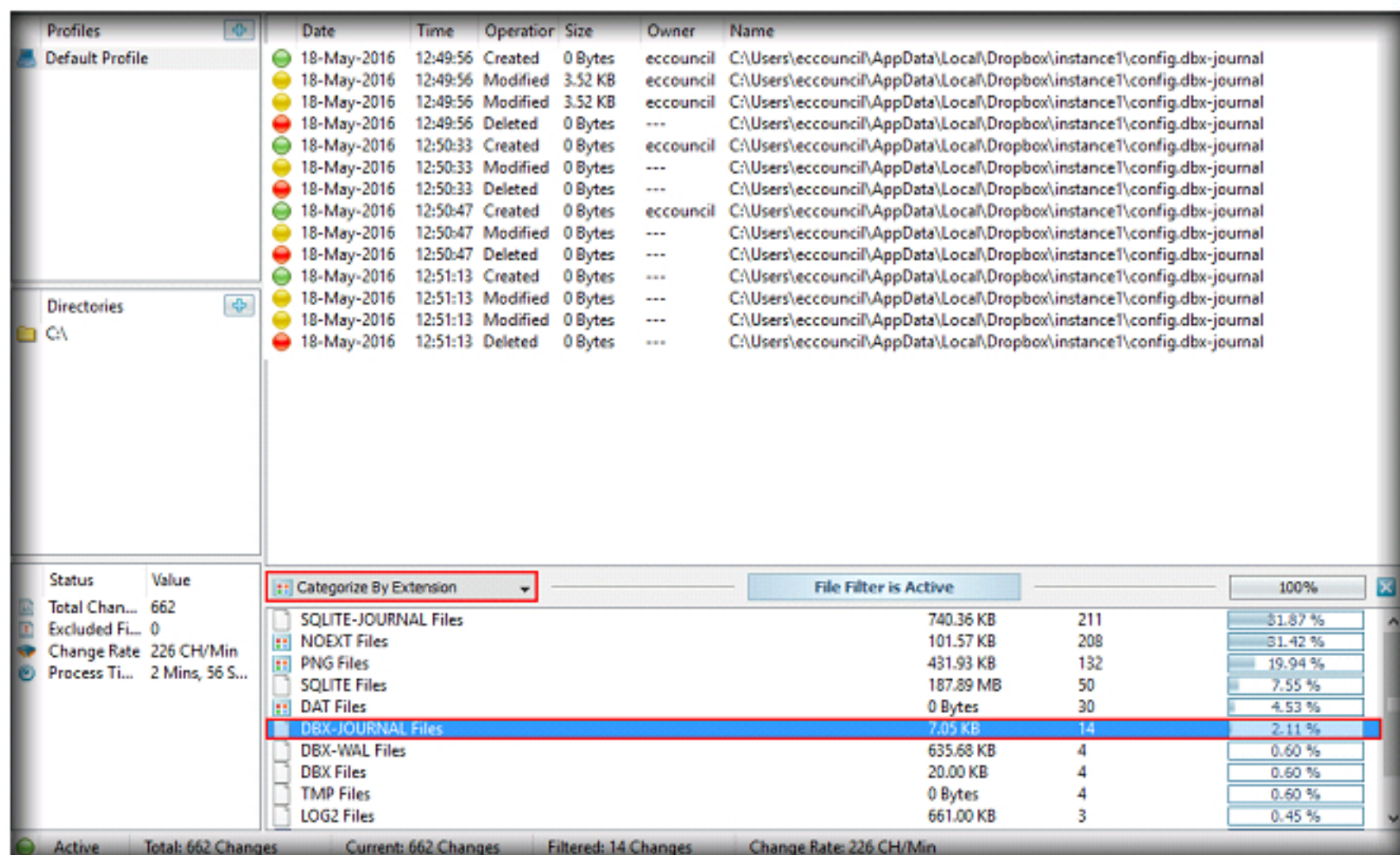


FIGURE 1.22: Viewing the changes the Dropbox files make to the system during configuration

36. Launch the **RAM Capturer** tool from the location **Z:\CHFIV9 Module 10 Cloud Forensics\RamCapturer**.
37. Specify the **Output folder path** where you want to store the captured data and click the **Capture!** Button.

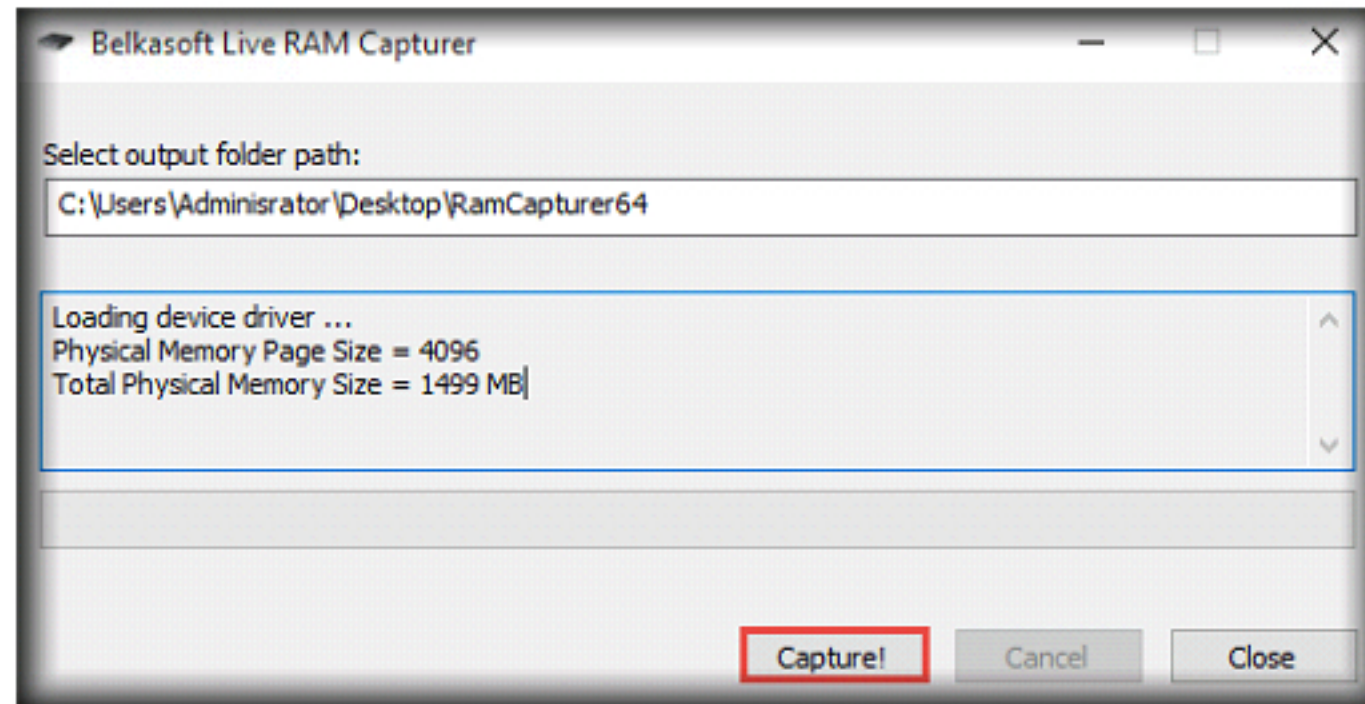


FIGURE 1.23: Storing the captured RAM data using the RAM Capture tool

38. Click **Close** button after the tool completes capturing the RAM data.

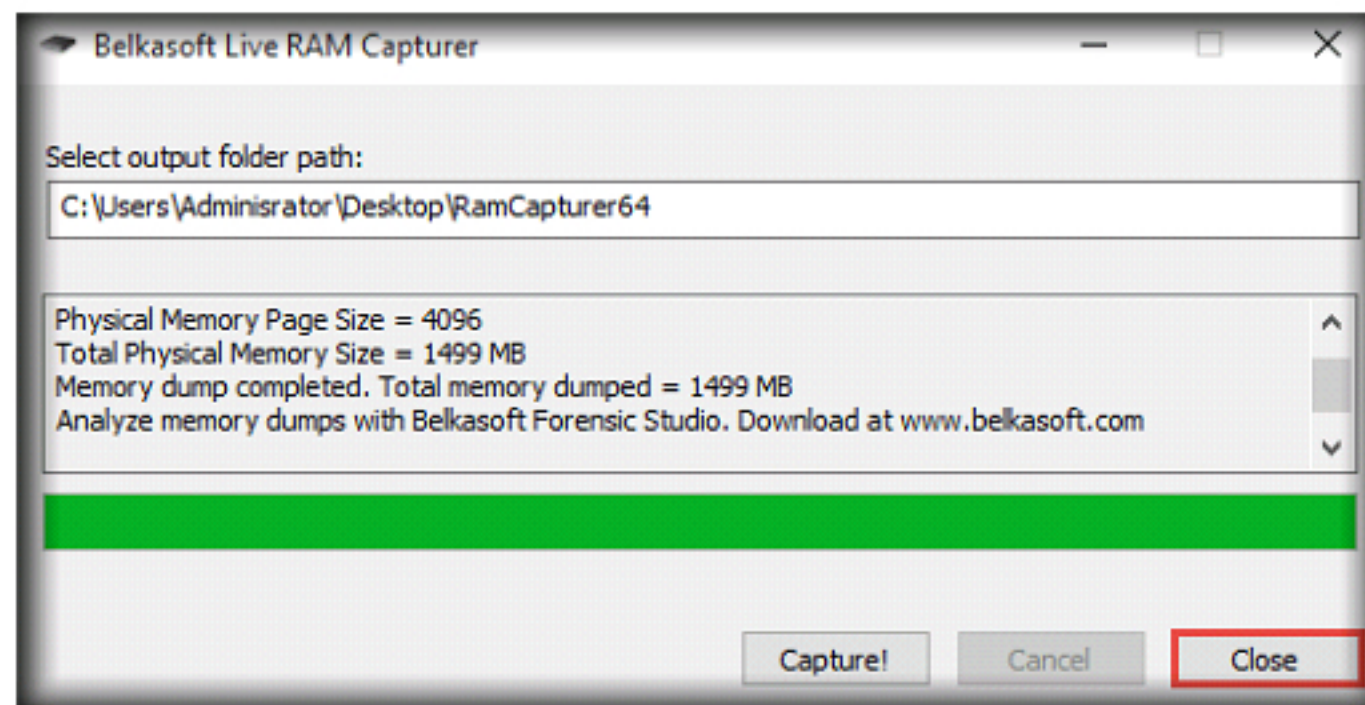


FIGURE 1.24: Figure showing the completion status of the RAM Capturer tool

39. Navigate to the **Z:\CHFIV9 Module 10 Cloud Forensics\Hex Editor Tools\HxD** and double click the **setup.exe** file to run the **HxD** tool. Click the **Open** icon from the top right side of the menu bar.

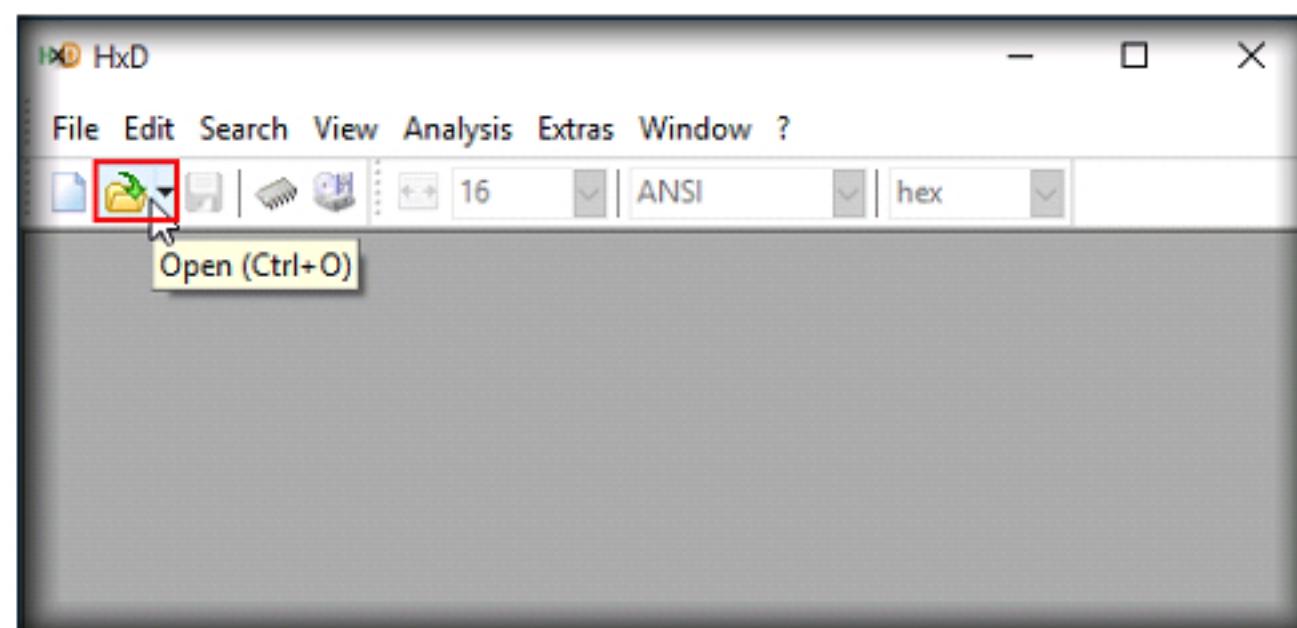


FIGURE 1.25: HxD tool main window with Open icon highlighted

40. Navigate to the location that stores captured RAM data, **C:\Users\Administrator\Desktop\RamCapturer64**, select the file, and click the **Open** button.

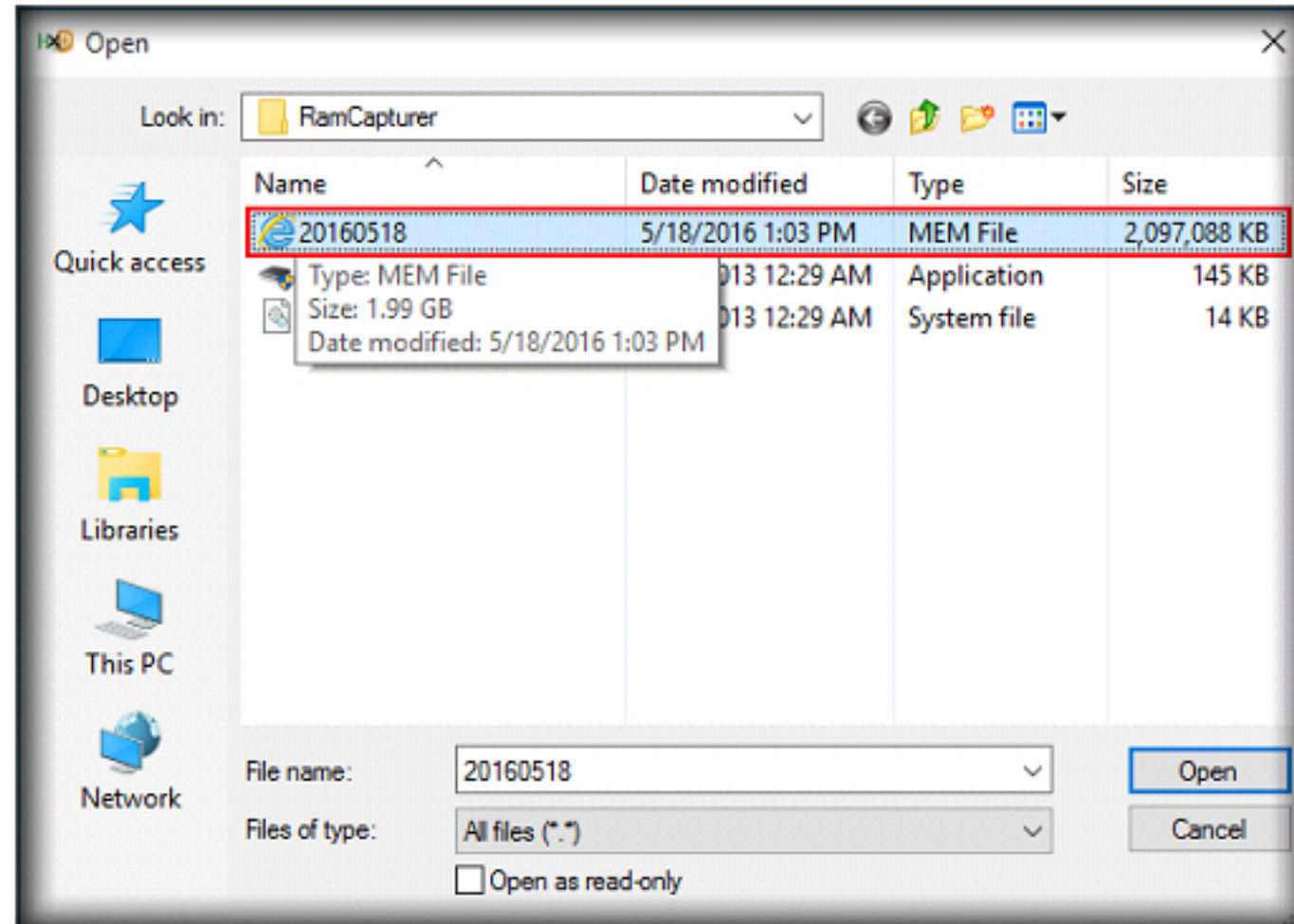


FIGURE 1.26: Window representing the required file in the destination folder

41. The tool will display the hex value of the captured RAM data. Go through the ANSI data it displays to find suspicious strings.

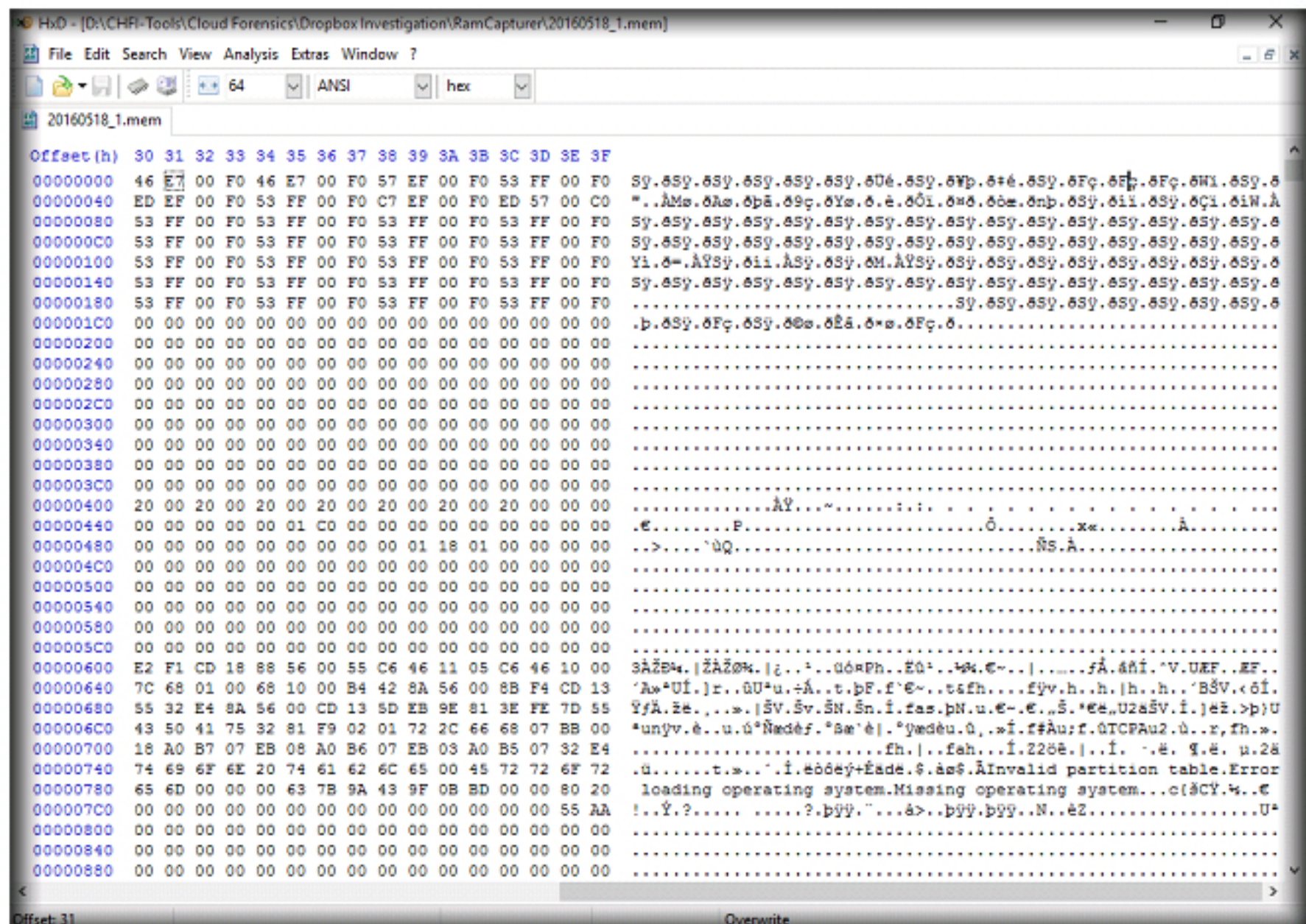


FIGURE 1.27: Examining the ANSI data

42. Use the search function to search for strings such as email ID, display name, filecache.dbx path, Server_time, file list, deleted, etc.

43. Press **Ctrl+F** to initiate search option. Enter keyword, such as Dropbox, in the **Search for** drop-down field and click **OK** button.

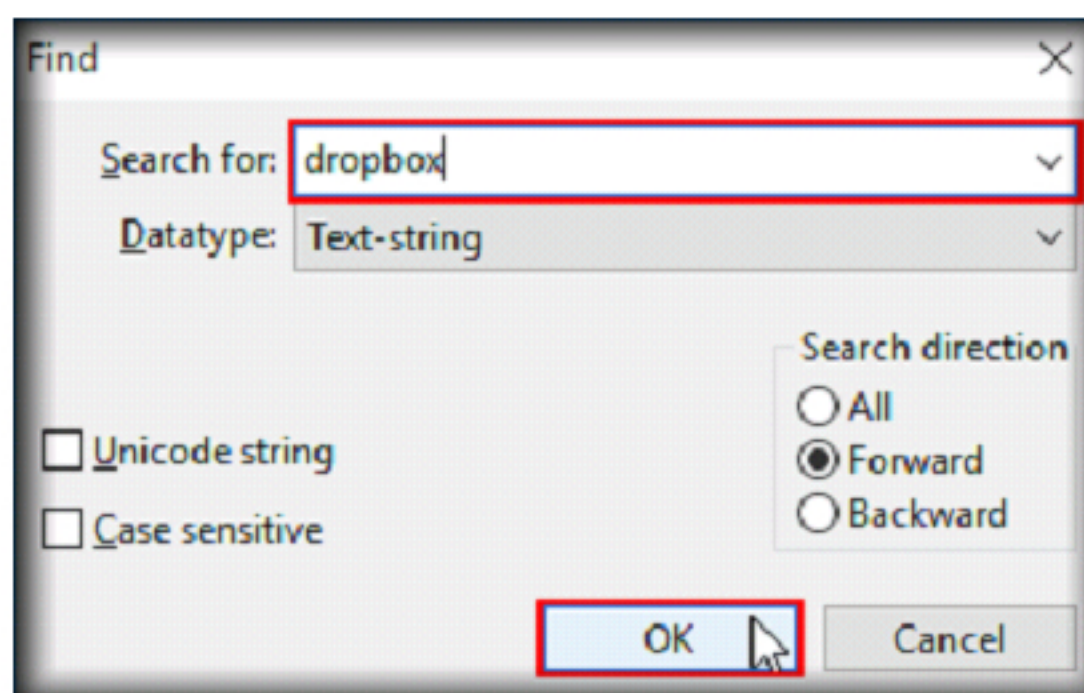


FIGURE 1.28: Search window

44. The tool will go to a line having keyword in it. Press **F3** to move forward and search for more such strings.

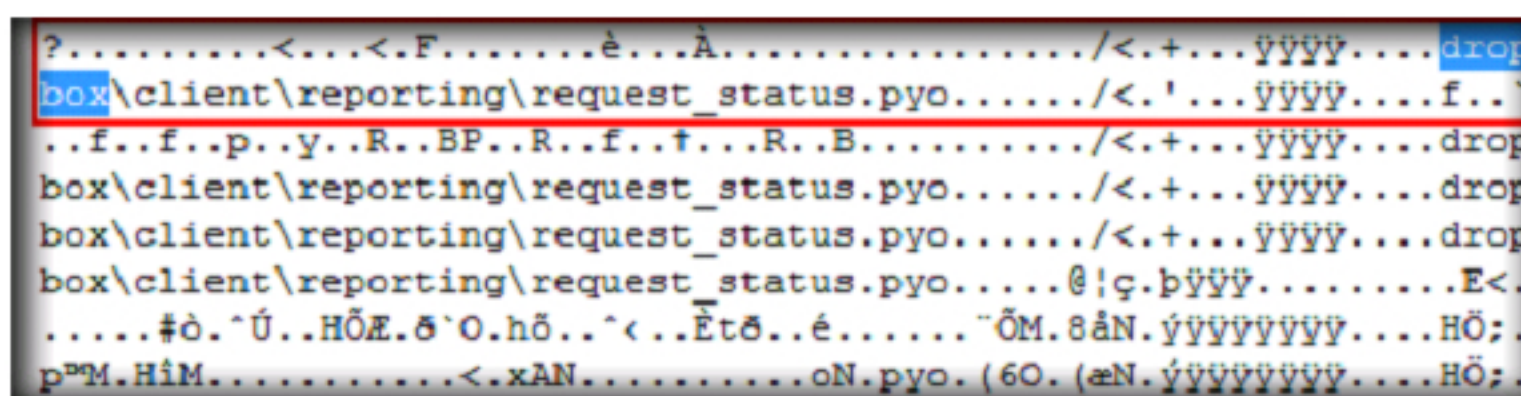


FIGURE 1.29: Screenshot showing the queried search keyword

45. The process will reveal locations of Dropbox files in the system, account credentials such as username, and type of platform used to access the account.

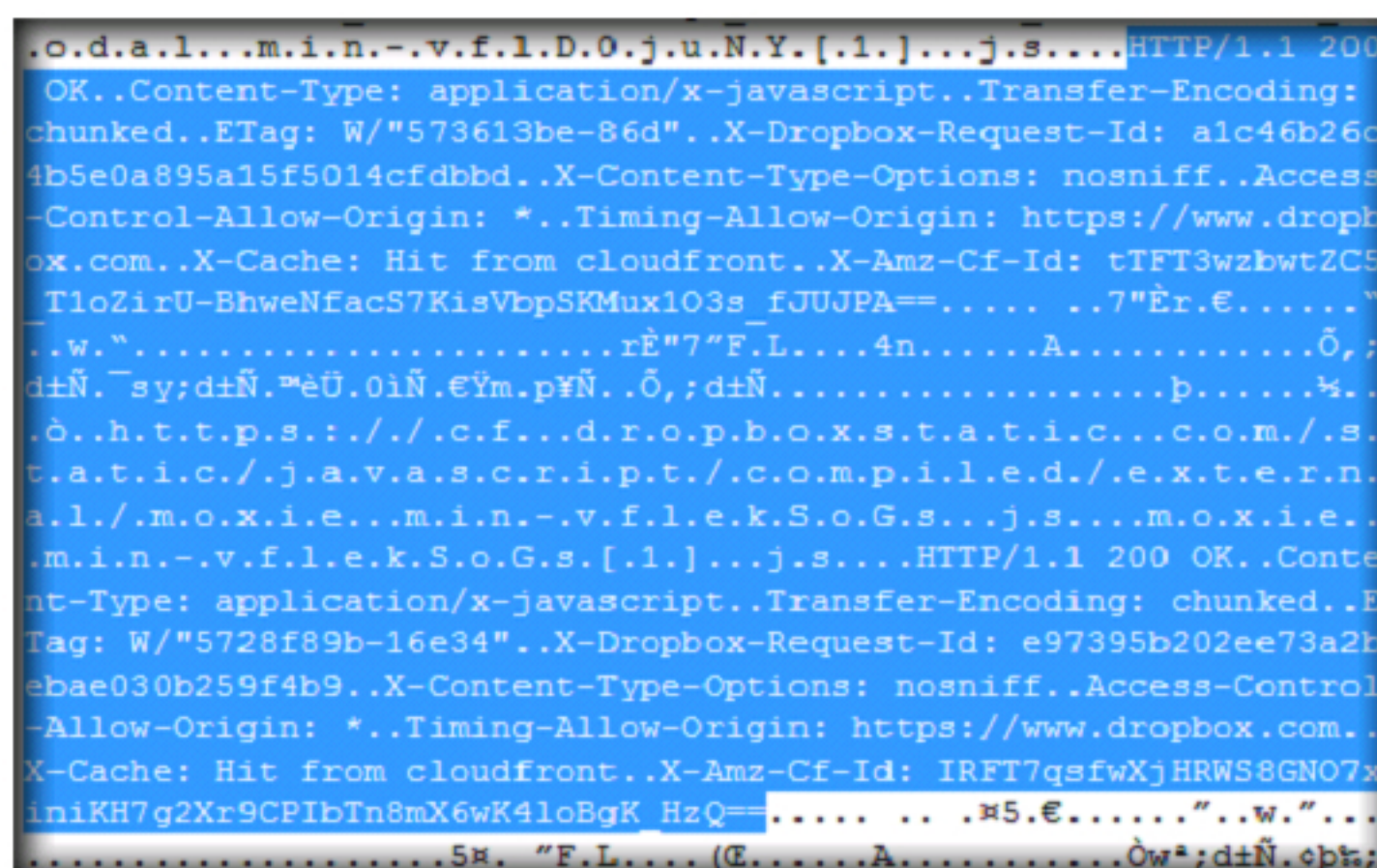


FIGURE 1.30: Screenshot showing the revealed information

46. The tool displays the location of the Dropbox filecache.

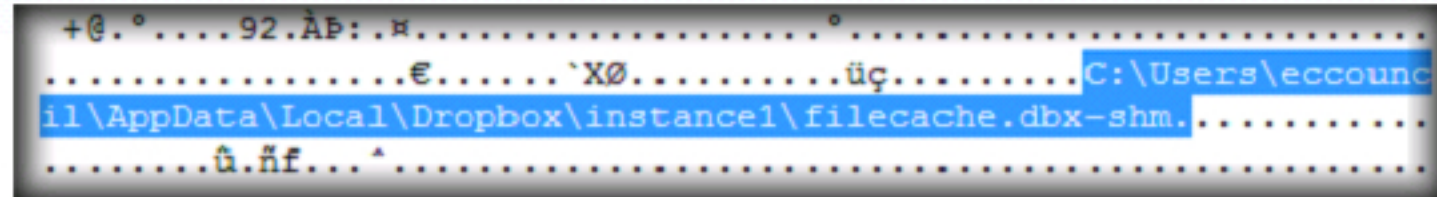


FIGURE 1.31: Screenshot showing the Dropbox filecache location

47. The hex tool will also display the passwords stored by the web browsers in their cache. To view the password, search for relevant strings such as password, login_password, paswd, etc.
48. Here, you can see that the user has allowed Mozilla Firefox web browser to store the password, which is available in the hex value of the RAM capturer data.

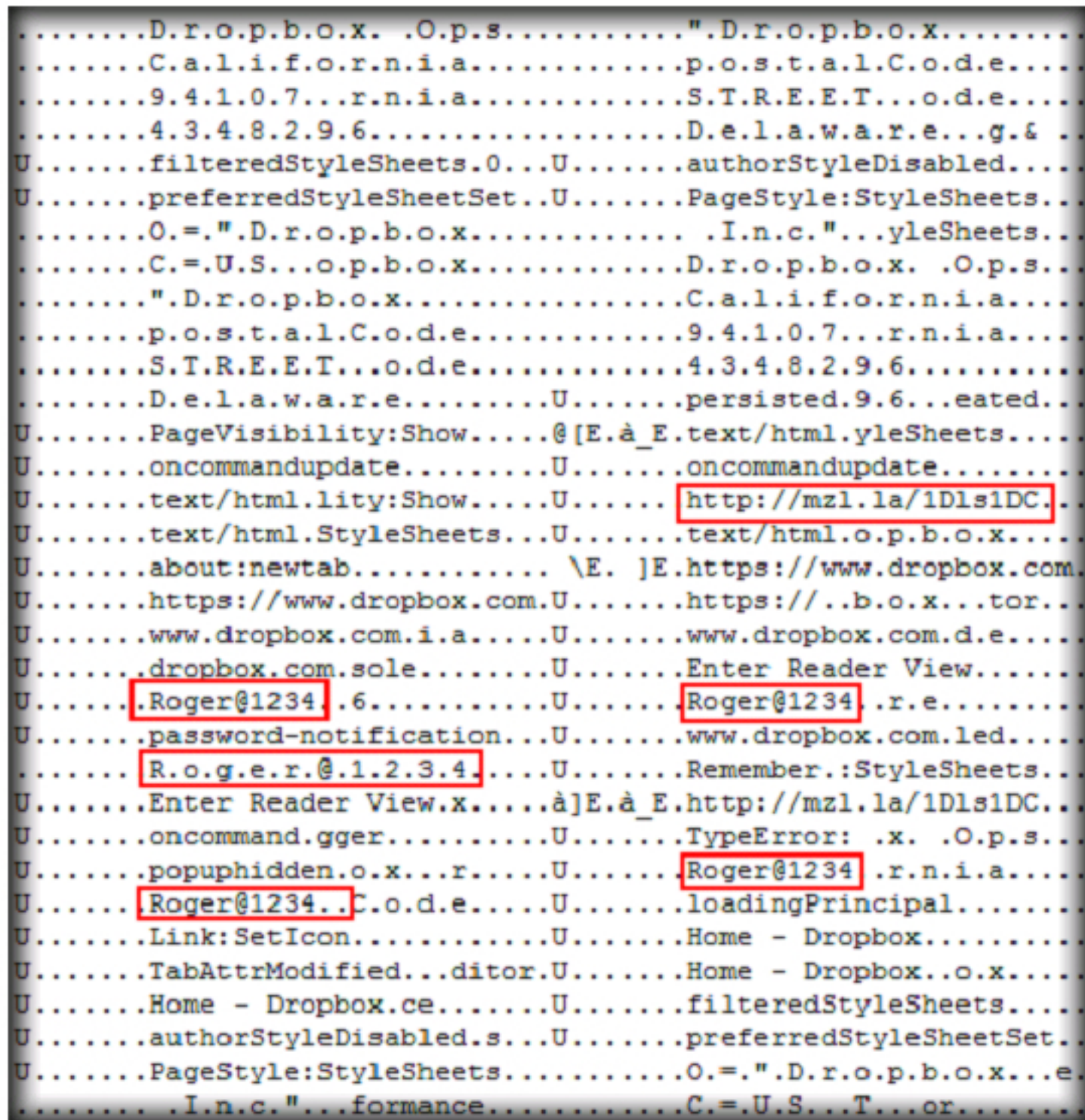


FIGURE 1.32: Analyzing the captured RAM data of Mozilla Firefox

49. Google's Chrome browser also stores the password in the RAM that can be traced in the RAM captured data.

```
U.....www.dropbox.com....€....U.....https://www.dropbox.com.
U.....https://.r....%>f..Q..U.....www.dropbox.com....€....
U.....https://www.dropbox.com.U.....https://.%.x.%>f.Đ...
U.....www.dropbox.com....€....U.....https://www.dropbox.com.
U.....formOrigin..Đ.%>f.à8..U.....https://www.dropbox.com.
U.....www.dropbox.com.Đ.%..%.U.....www.dropbox.com.>f.À...
U.....password.>f.P...&...€....U.....checkbox...€....P.%€.%
U.....getAppByLocalId( 0..0...U.....getAppByLocalId( 0 )...
U.....keypress.r.€....°.%à.%U.....text/html.%.Đ.%>f.`...
U.....keypress.>f.à<....€....U.....keypress...€....%.@.%
U.....keypress..%.X.%>f.P¥..U.....hostname.>f.e..2..€....
U.....https://www.dropbox.com.U.....formSubmitURL.%>f.ñ..
U.....https://www.dropbox.com.U.....usernameField...Đ.%...%.
U.....login_email...%>f.pÅ..U.....newPasswordField...€....
U.....login_password..0.%.`.%U.....Roger@1234..x.%>f.pÉ..
U.....oldPasswordField...€....U.....nsILoginInfo....%.À.%
...%.%.nsILoginInfo..%>f.@`..U.....nsILoginInfo.ù..B..€....
U.....nsILoginMetaInfo..%.%.%.nsILoginMetaInfo.>f.°...
U.....nsILoginMetaInfo...€....U.....nsIFactory.€....P.%€.%
À.%à.%nsIFactory..~.%>f.ĐD..U.....nsIFactory..Đ8..J..€....
U.....nsIPromptFactory..%.à.%..%.@.%nsIPromptFactory.>f.Đ<..
U.....nsIPromptFactory...€....U.....nsIObserver.h....%.@.%
€.%..%.nsIObserver.y.%>f..M..U.....nsIObserver..Q..R..€....
U.....nsIAuthPrompt...p.%..%.à.%...%.nsIAuthPrompt.%>f..}..
U.....nsIAuthPrompt...V..€....U.....nsIAuthPrompt2..Đ.%...%.
@.%.`.%nsIAuthPrompt2...>f.e..U.....nsIAuthPrompt2..Z..€....
U.....nsILoginManagerPromter..%.À.%nsILoginManagerPromter.
```

FIGURE 1.33: Analyzing the captured RAM data of Google Chrome

50. In case the passwords are not available in the hex data of the captured RAM data, run the **WebBrowserPassView** tool to find the usernames and password of the email accounts logged in through browsers as well as the accounts using clients to connect to the server.
51. The tool reveal details such as URL, browser, username, password, and password strength.

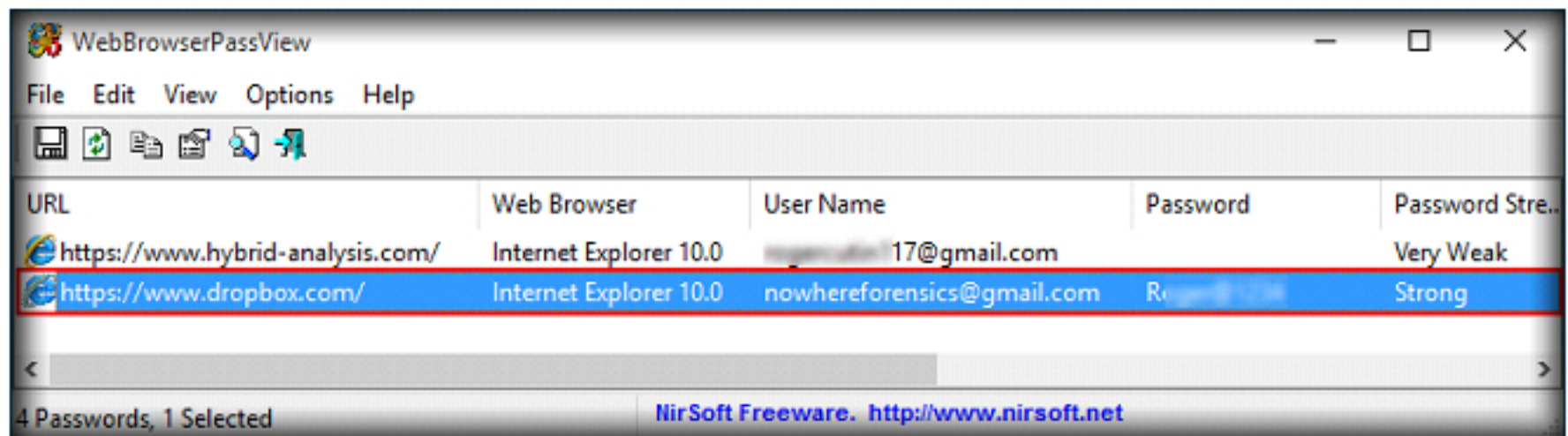


FIGURE 1.34: WebBrowserPassView tool revealing details of email accounts

52. Use the username and password credentials of the Dropbox account to logon into it. Find the traces of files the perpetrator has deleted.
53. In the homepage of the Dropbox, click the **Delete Files** option from the left pane.

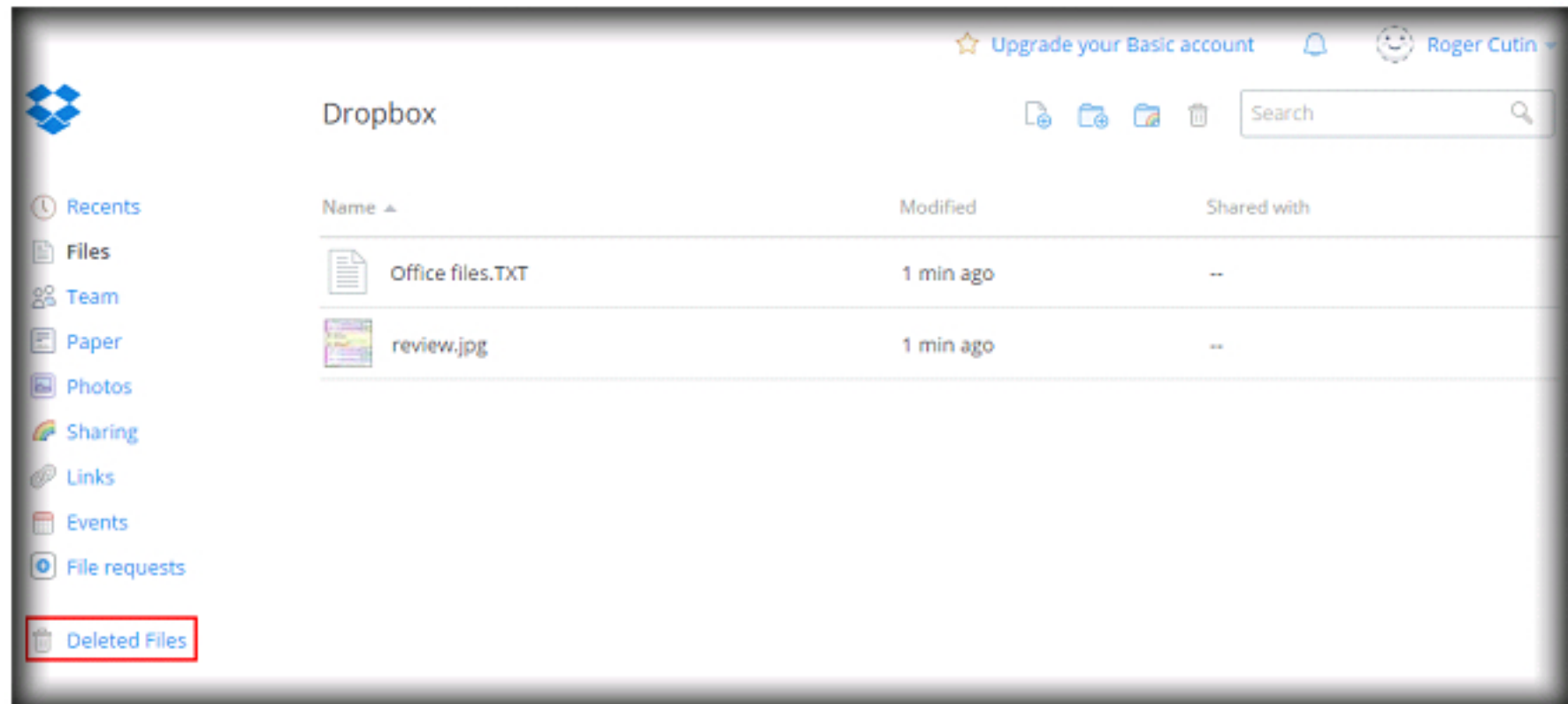


FIGURE 1.35: Homepage of Dropbox with Delete Files option highlighted

54. The website will navigate to the **Deleted Files** page. You can see all the deleted files here. To restore a deleted file, hover the mouse over the file you want to recover and click **Restore** button.
55. Restoration will help you in getting the original file and help to check its impact on the system.

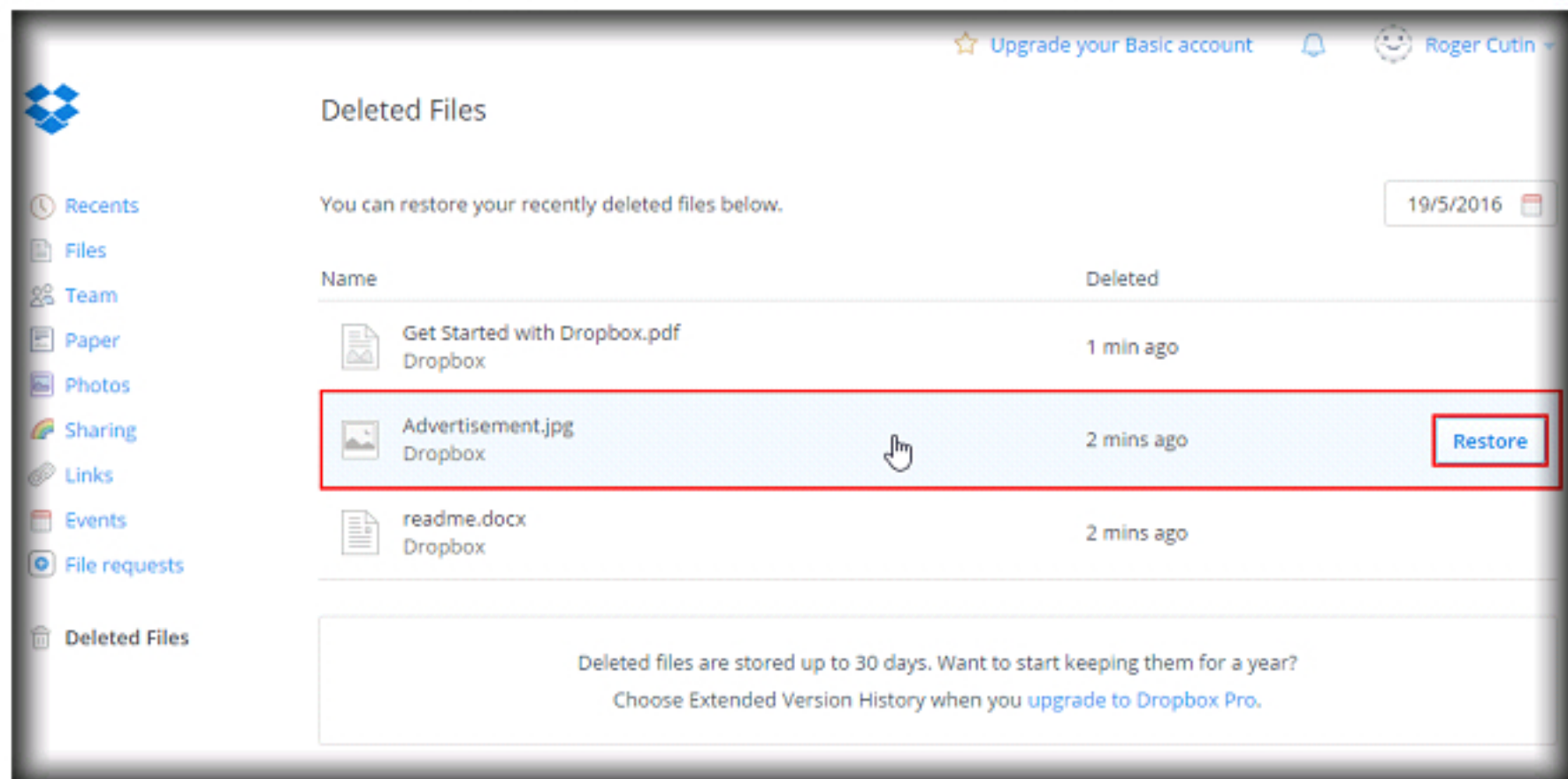


FIGURE 1.36: Restoring a deleted file from Dropbox

56. As part of the investigation, you should always try to find if someone had accessed the account from a different source along with details such as time and location.

57. To find out previous sessions or logs of the account, go to the sessions section of Dropbox website. In the account homepage, click the **Username** on the top right corner and select **Settings** from the dropdown list.

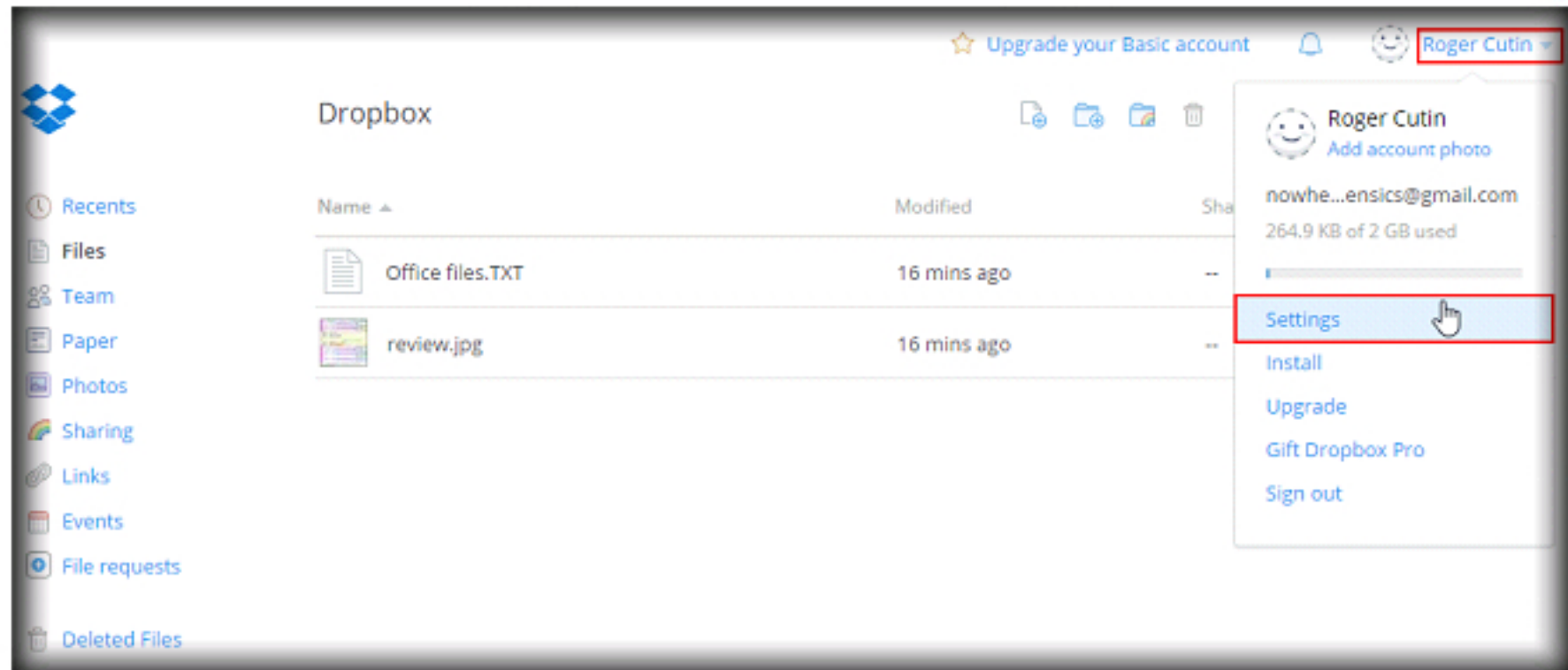


FIGURE 1.37: Finding previous sessions or logs of an account

58. In the settings page, click the **Security** tab.

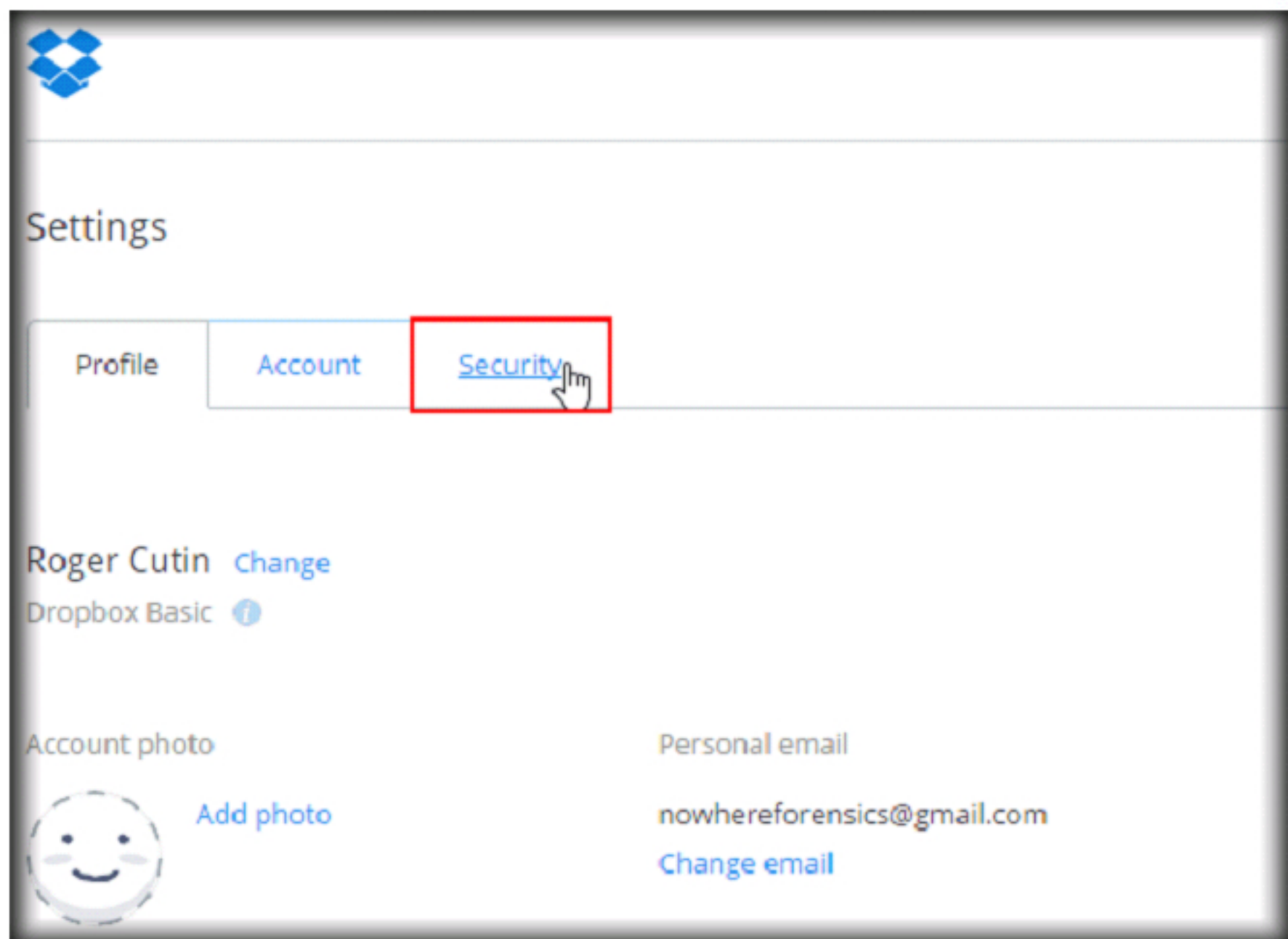


FIGURE 1.38: Screenshot showing the Security tab

59. The security tab contains **Password**, **Session**, **Devices**, and **APPs** sections. Scroll down to **Sessions** section to view previous logins and browsers used to login.

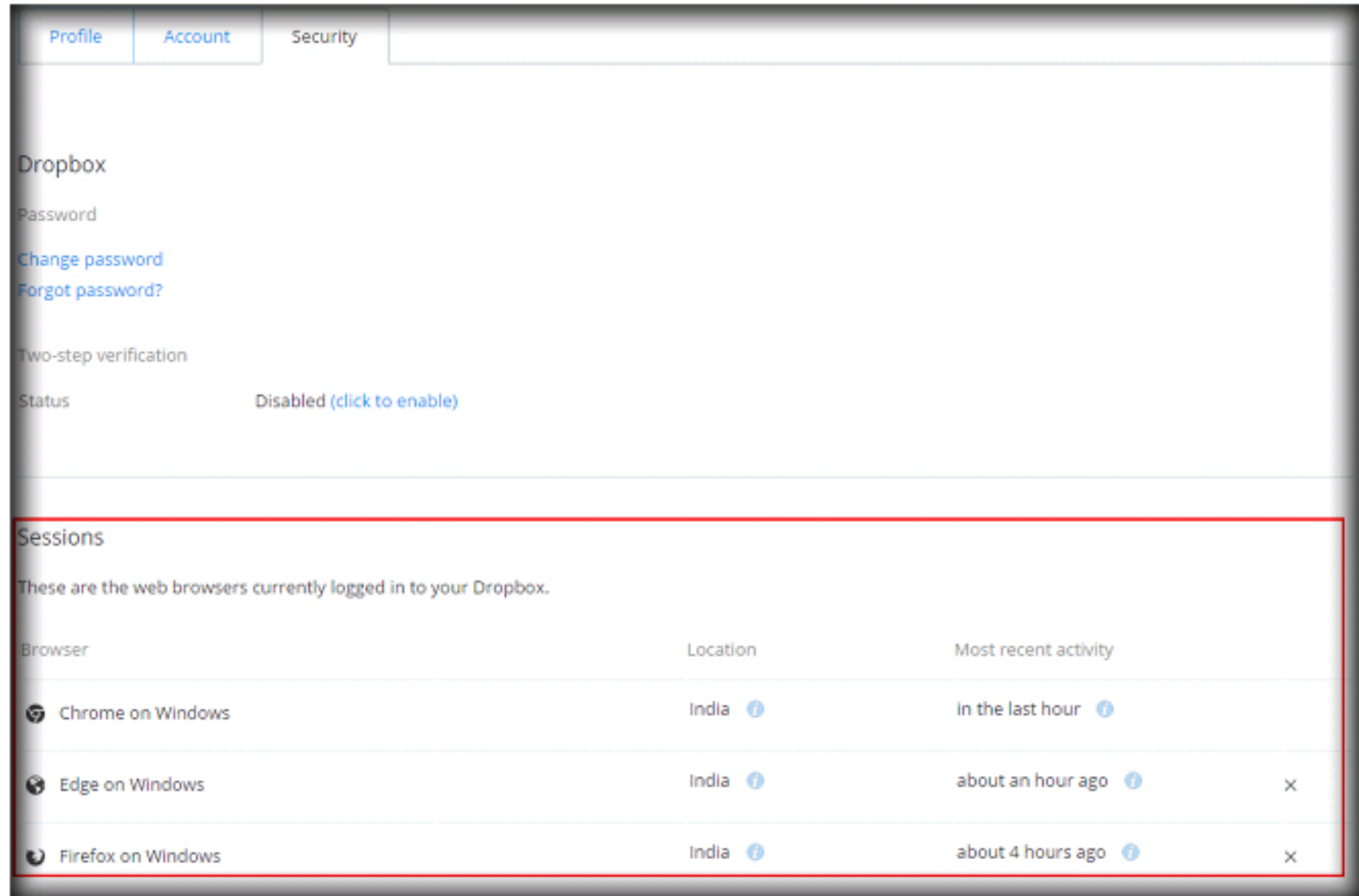


FIGURE 1.39: Viewing previous logins and browsers used to login

60. Scroll further to view the **Devices** section, which contains a list of devices that have accessed the Dropbox account through a client.
61. In addition, it displays the applications accessing the account.



FIGURE 1.40: Viewing Devices section

62. Dropbox also stores the details about each file uploaded in the form of versions and also allows you to recover any of the previous versions of a modified file.

63. In the home page, select the **Files** option from left side menu list, right click the file and select **Previous versions...** option from the provided list to view previous versions of the file.

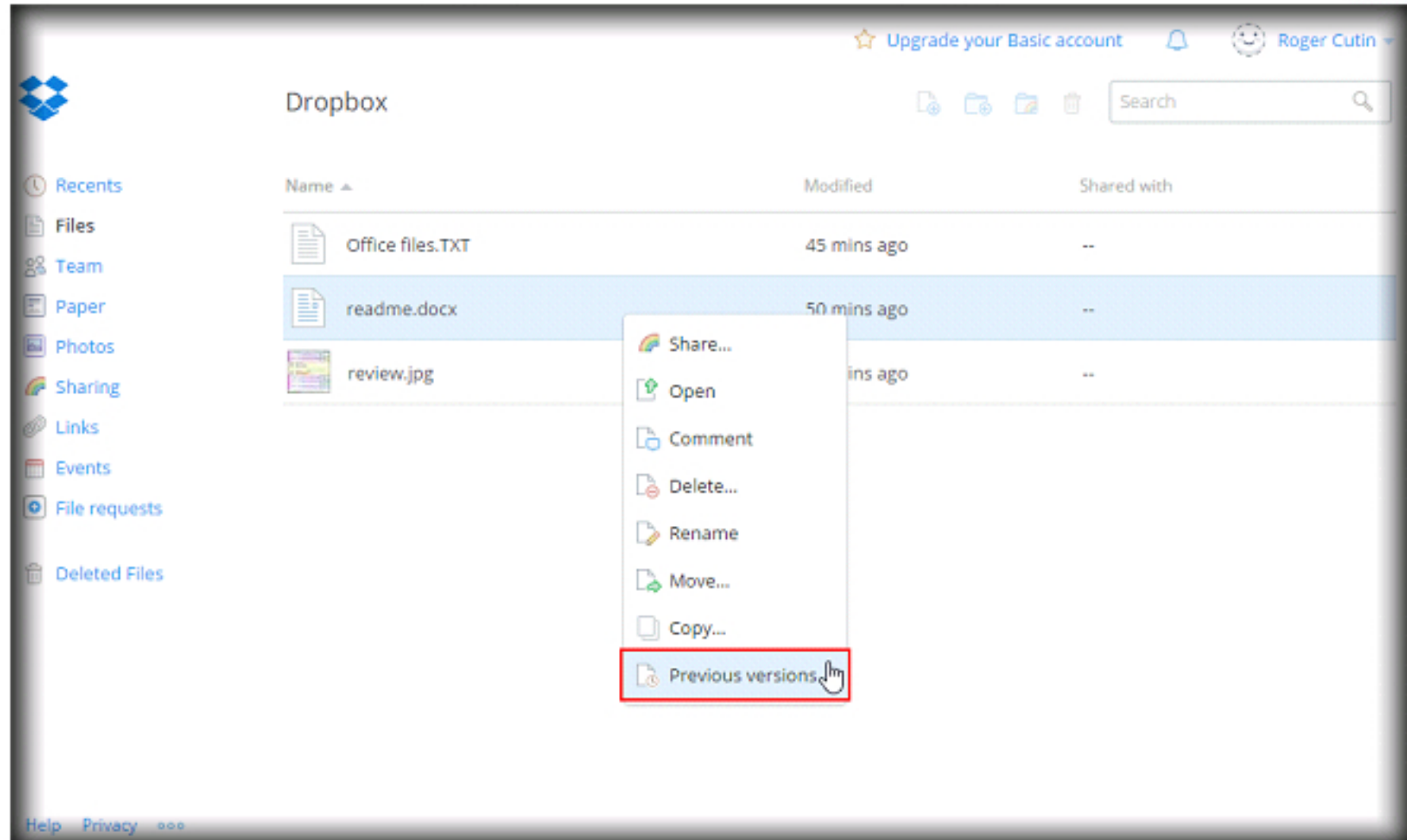


FIGURE 1.41: Viewing previous versions of a file

64. The tool will prompt you to the **Version History of <filename>** page, wherein you can select the version of the file you want to recover and click the **Restore** button.

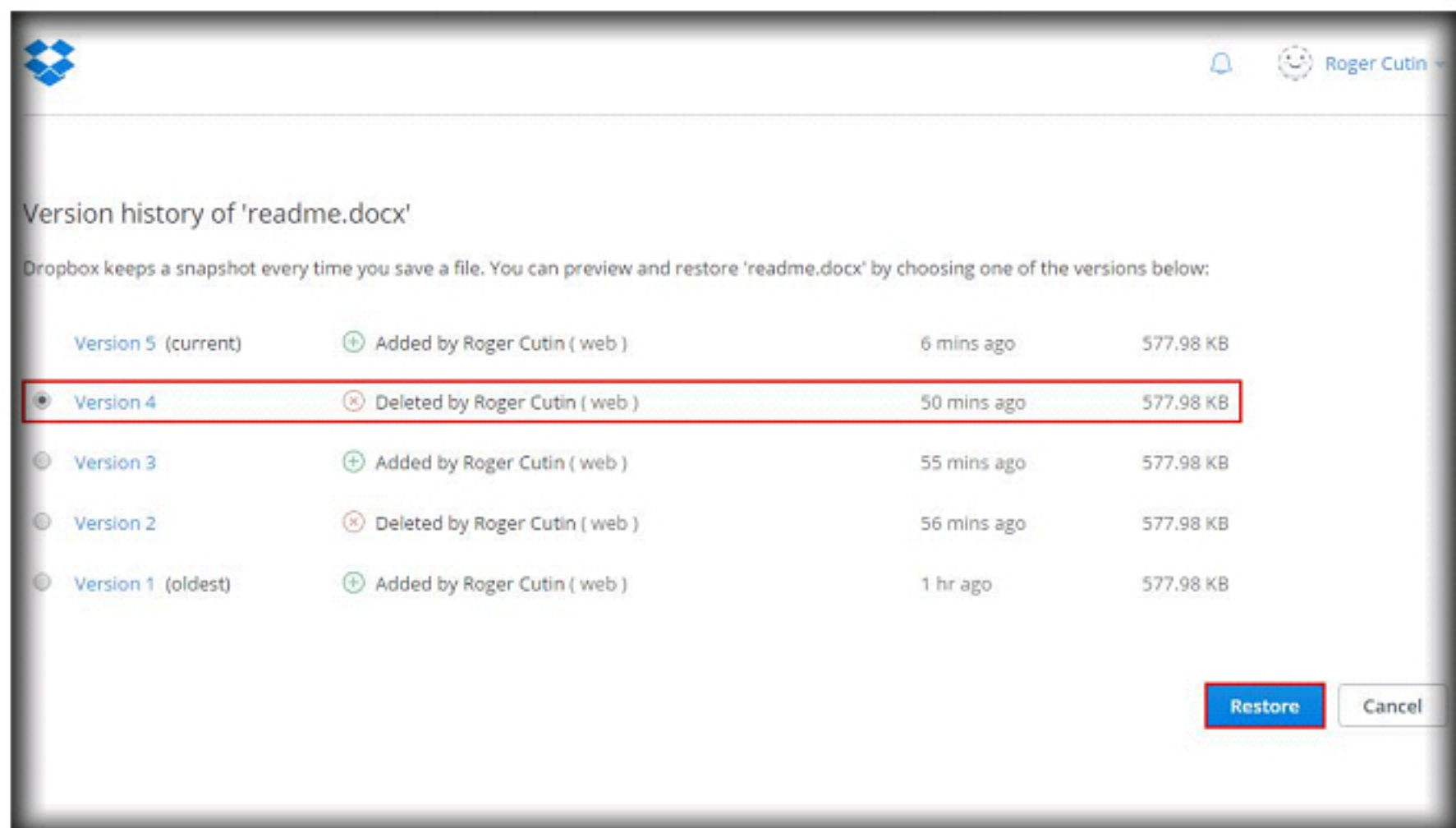


FIGURE 1.42: Screenshot showing how to recover and restore a particular version of a file

65. Other artifacts of Dropbox include events occurring over time. Dropbox stores record of all the events in the Events menu.

66. In the **Dropbox** account homepage, click the **Events** option from the left menu pane to view the events list.

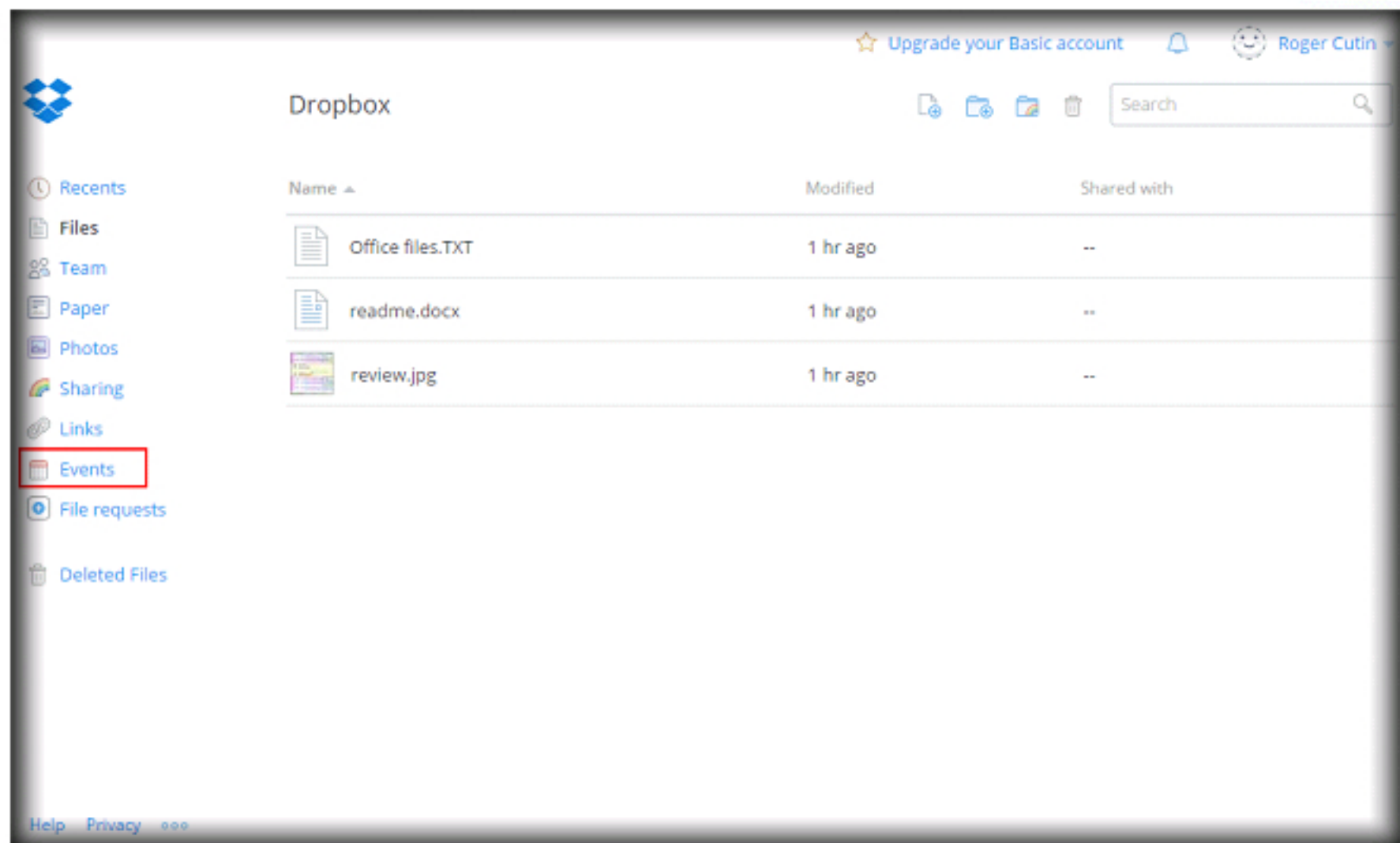


FIGURE 1.43: Viewing the events list

67. The events section stores all events, including adding and deleting of files, linking accounts to systems and applications, etc.

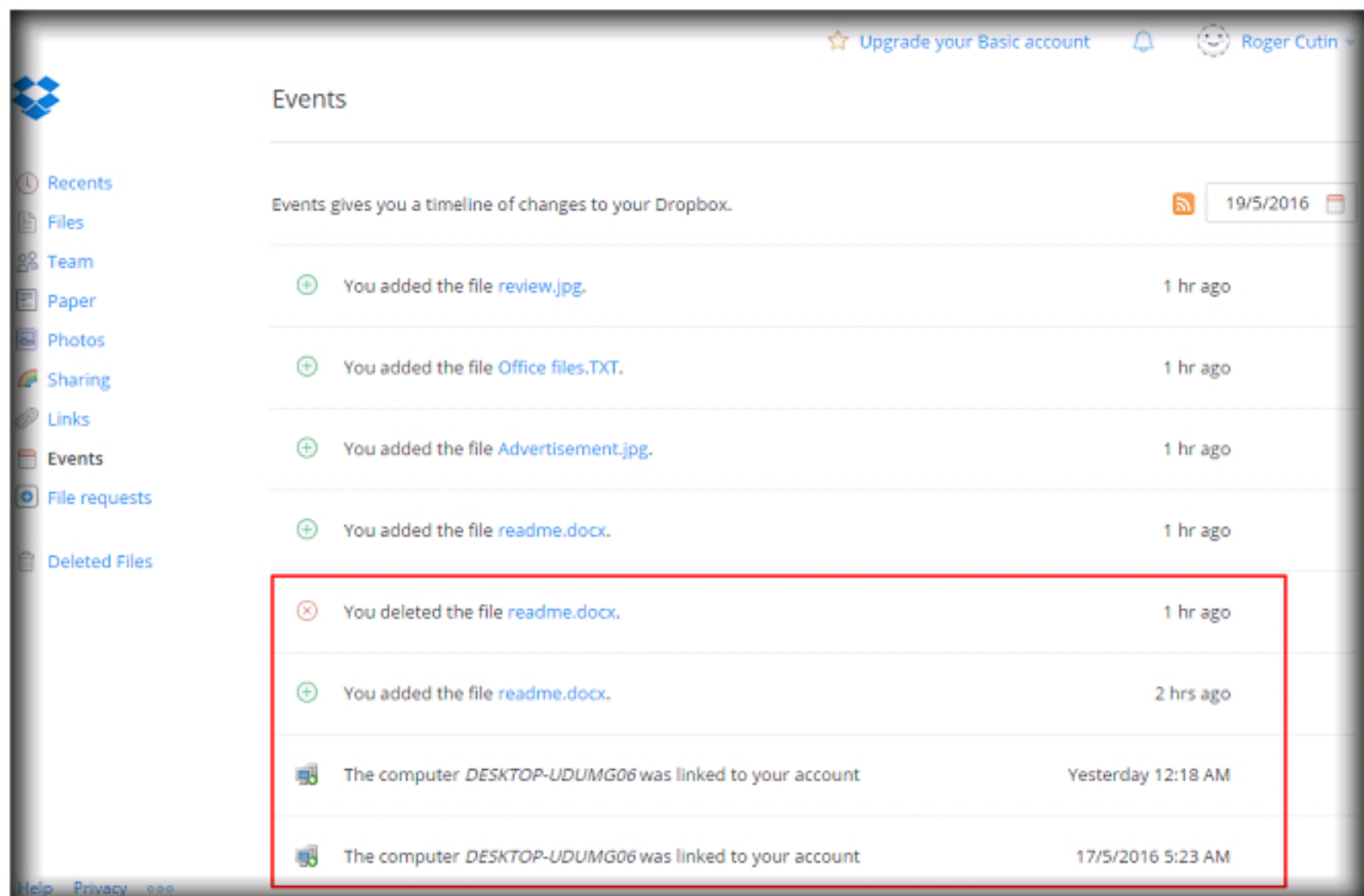


FIGURE 1.44: Viewing the information in the Events section

68. Now you need to know about the files a system retains when a user uninstalls Dropbox. Investigators can analyze these files to gather any available evidence.

69. Run the already installed **Regshot** and **Disk Pulse** tools and follow the steps 2, 6, 7 and 8 in order to capture the system information before installing an application.
70. Right click the **Windows** icon at the lower left corner of the screen and select **Control Panel** option.

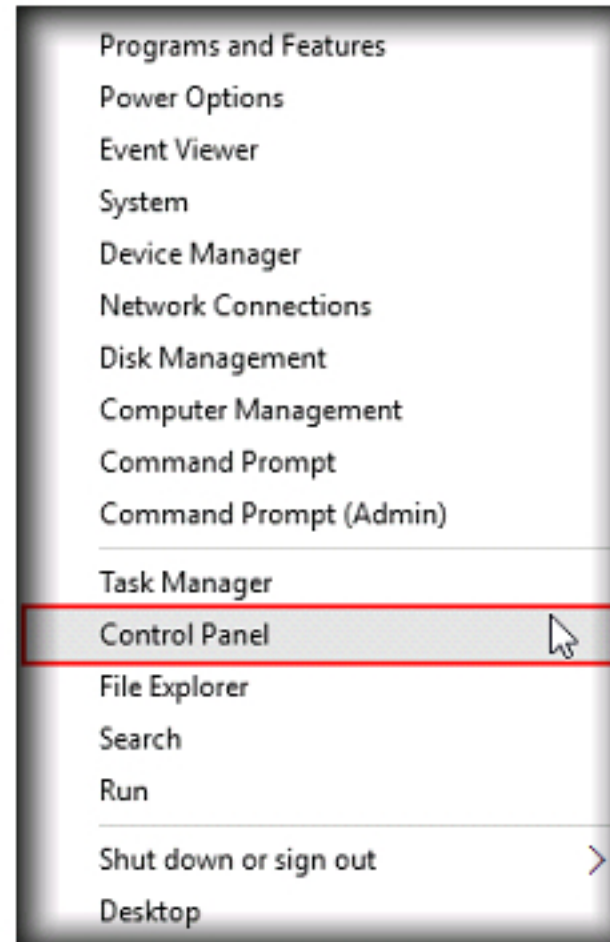


FIGURE 1.45: Screenshot showing Control Panel option

71. In the **Control Panel** window, click the **Uninstall a Program** link under the Programs section.

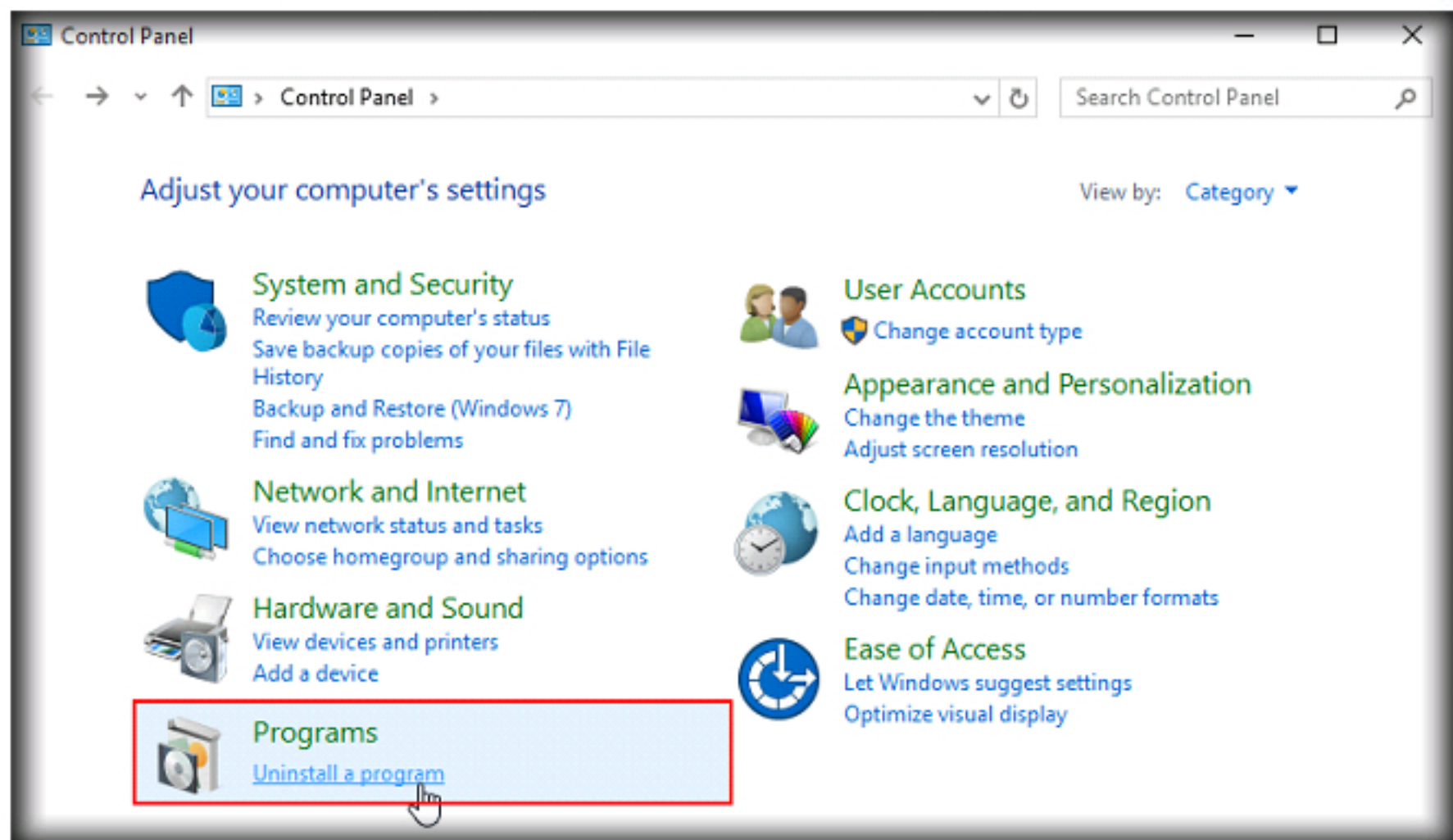


FIGURE 1.46: Screenshot showing Uninstall a Program link in the Control Panel window

72. In the Uninstall or change a program section double click the **Dropbox** option to uninstall it.

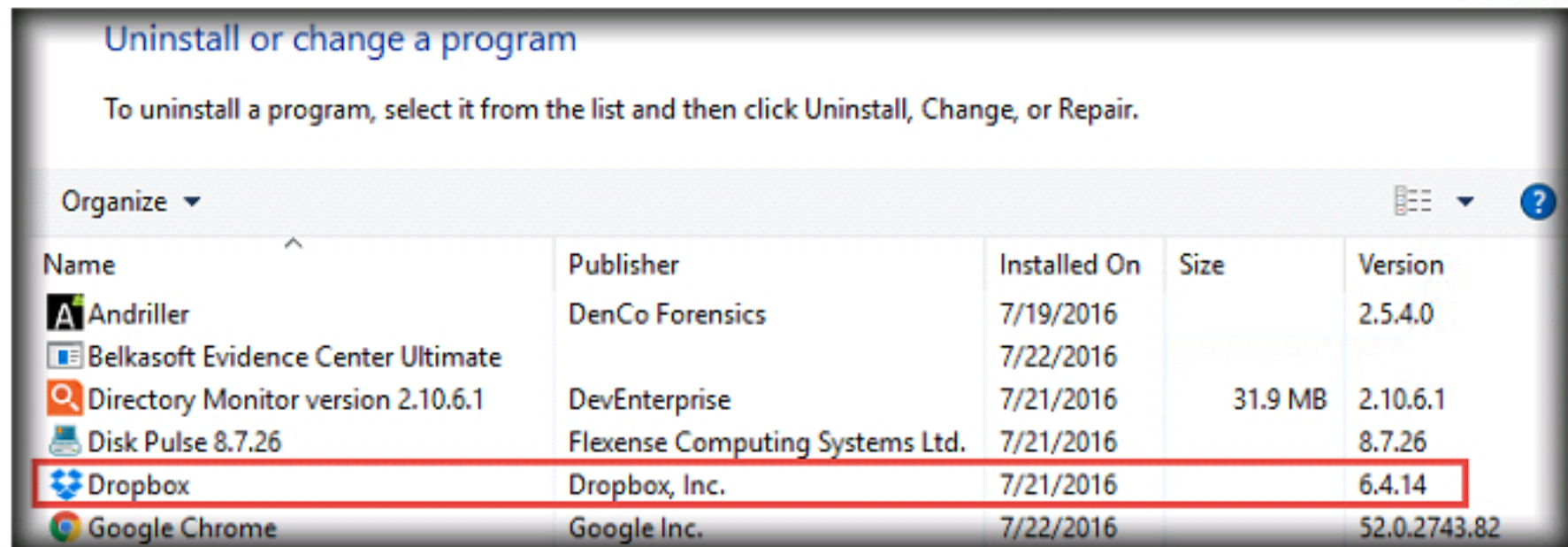


FIGURE 1.47: Uninstalling Dropbox application

73. Click the **Close** button after completion of the uninstallation process.

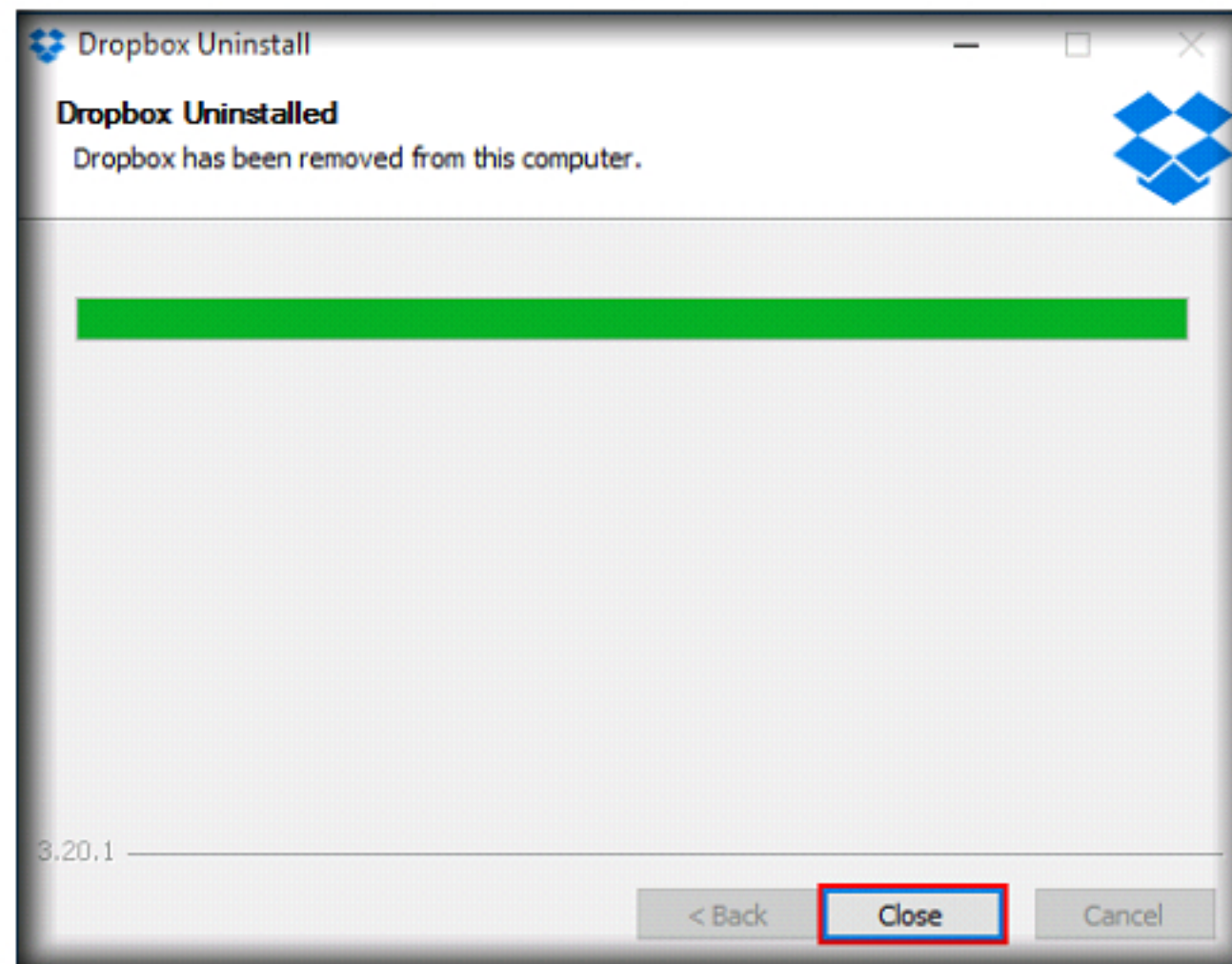


FIGURE 1.48: Uninstalling Dropbox application

74. Go to the **Disk Pulse** tool and click the **Stop** button from the tool bar to stop recording the processes.

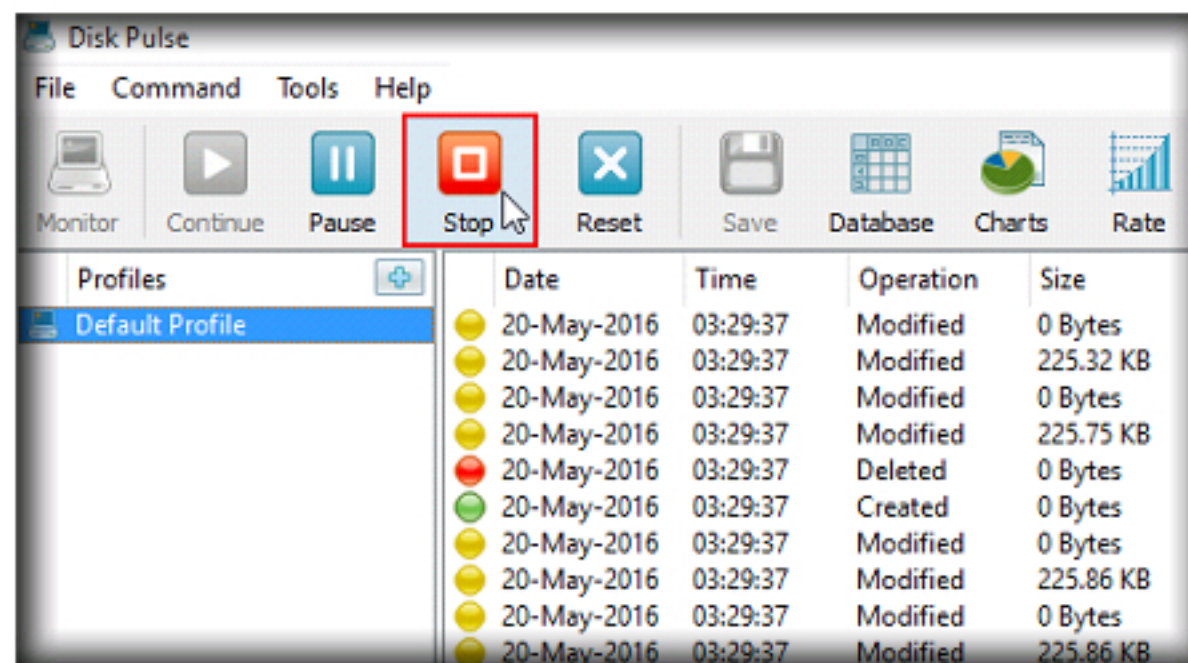


FIGURE 1.49: Stopping recording in the Disk Pulse tool

75. Select all the changes, right click, and select the option **Copy Changes To Clipboard**. This will help you to create a text or notepad file with all the modified addresses.

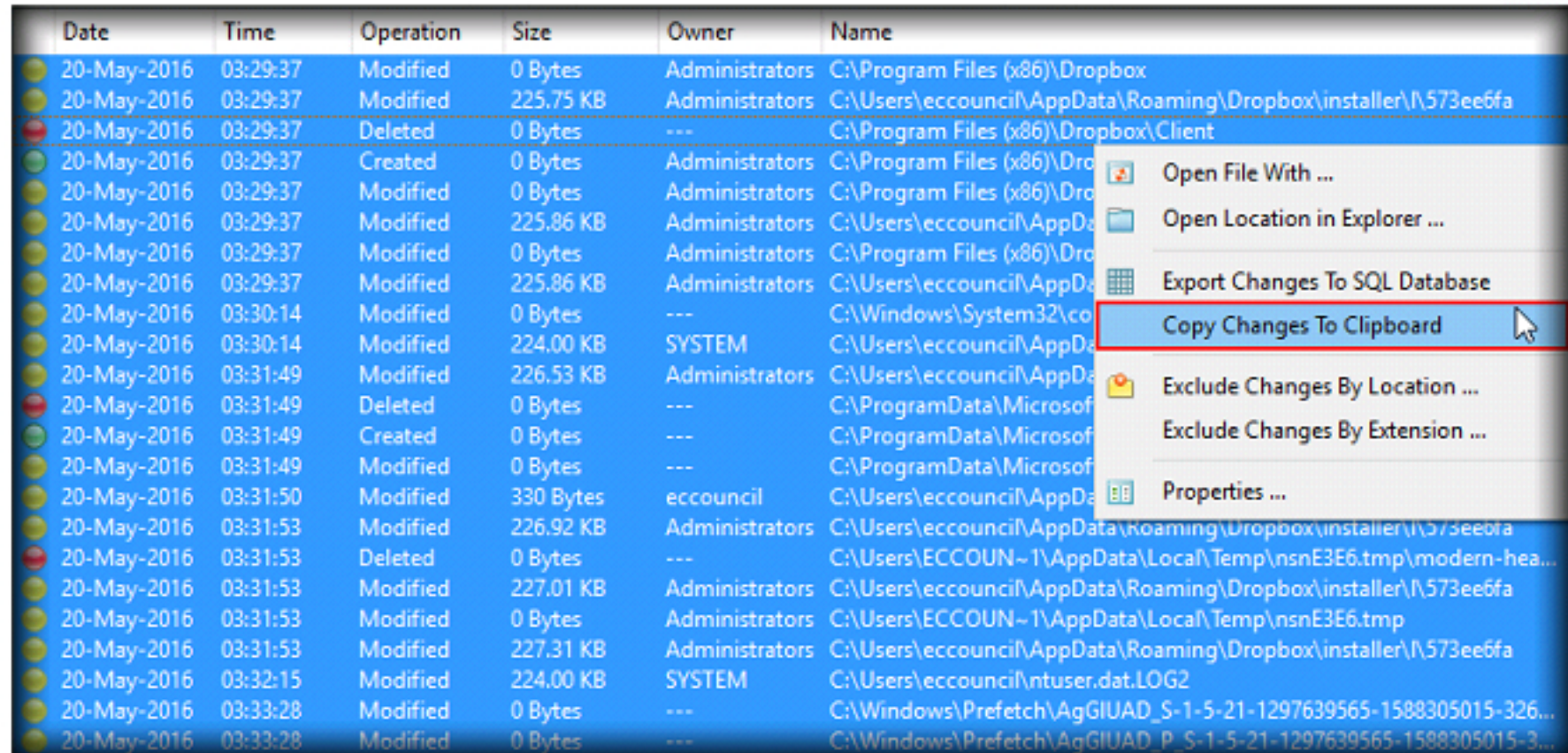


FIGURE 1.50: Copying the changes recorded in Disk Pulse tool to clipboard

76. Now create a text file and paste the contents onto it. These modified files represent all the changes made while uninstalling the Dropbox client from the system.
77. Launch the **Regshot** tool and click the **2nd Shot** button to capture the second snapshot of the system. This action will record the changes in registry of the system.

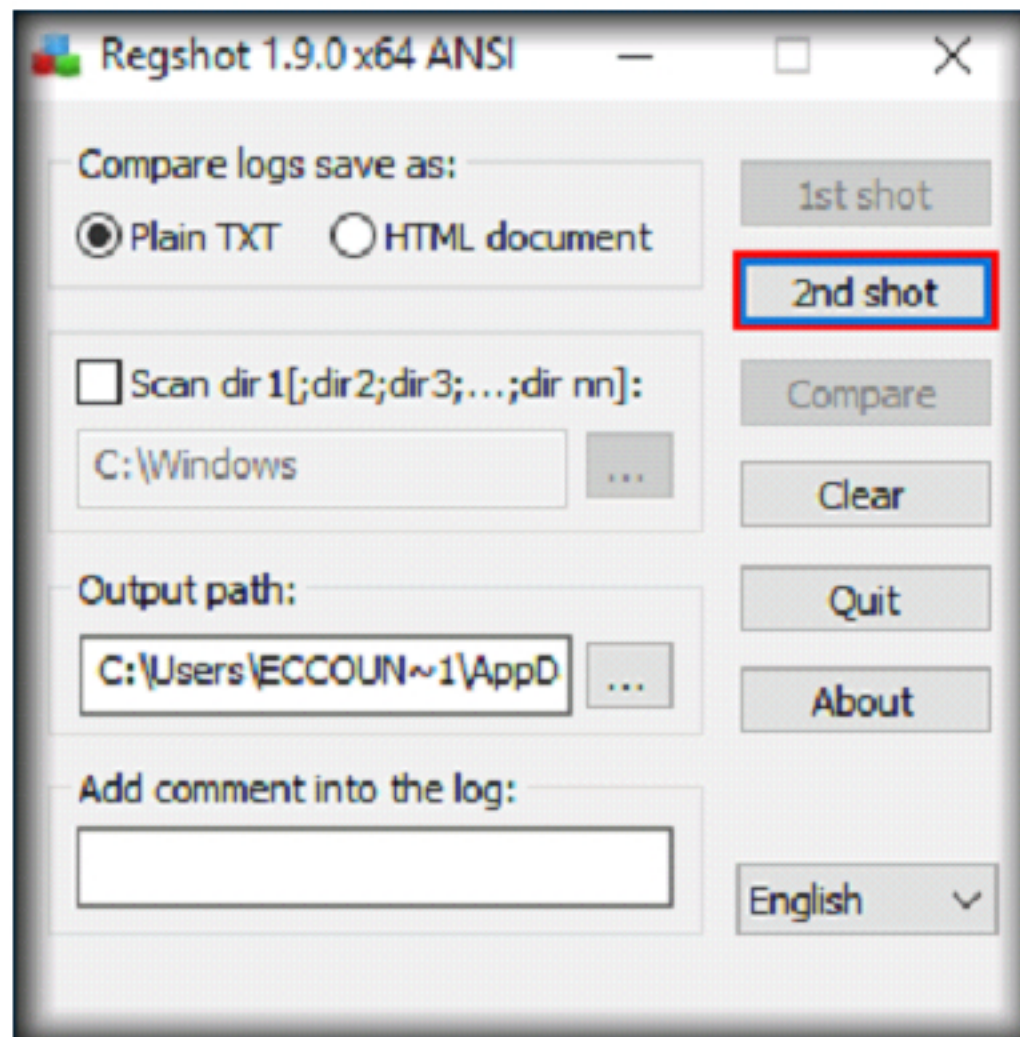


FIGURE 1.51: Capturing the 2nd snapshot of the system

78. After capturing the snapshot, click the **Compare** button to initiate the process of comparing both the snapshots and displaying the list of changed or modified registry locations.

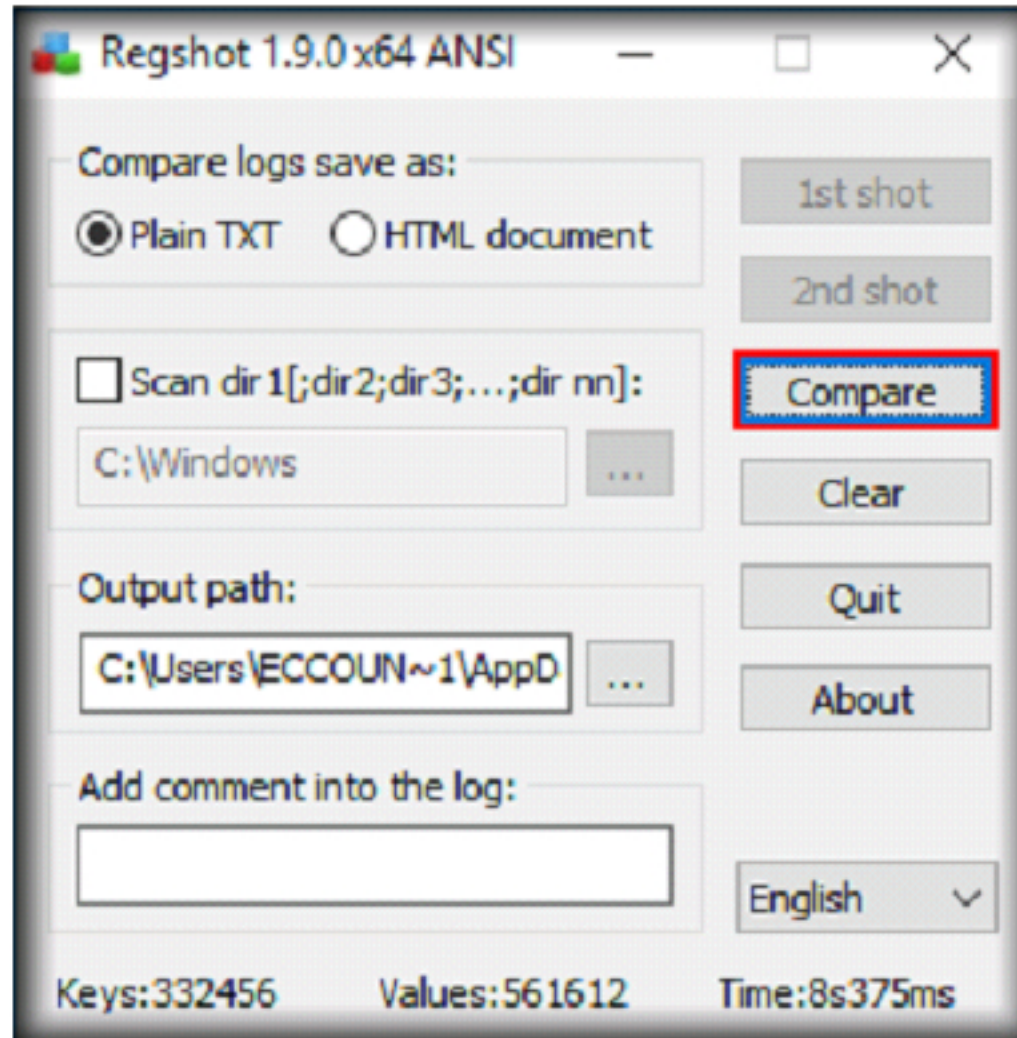


FIGURE 1.52: Comparing the snapshots in the Regshot tool

79. The tool will prompt a result notepad file after comparing the first and second snapshots. The file contains address links of all the modified files and folders. The File also mentions total number of changes made in the system while uninstalling the Dropbox client.

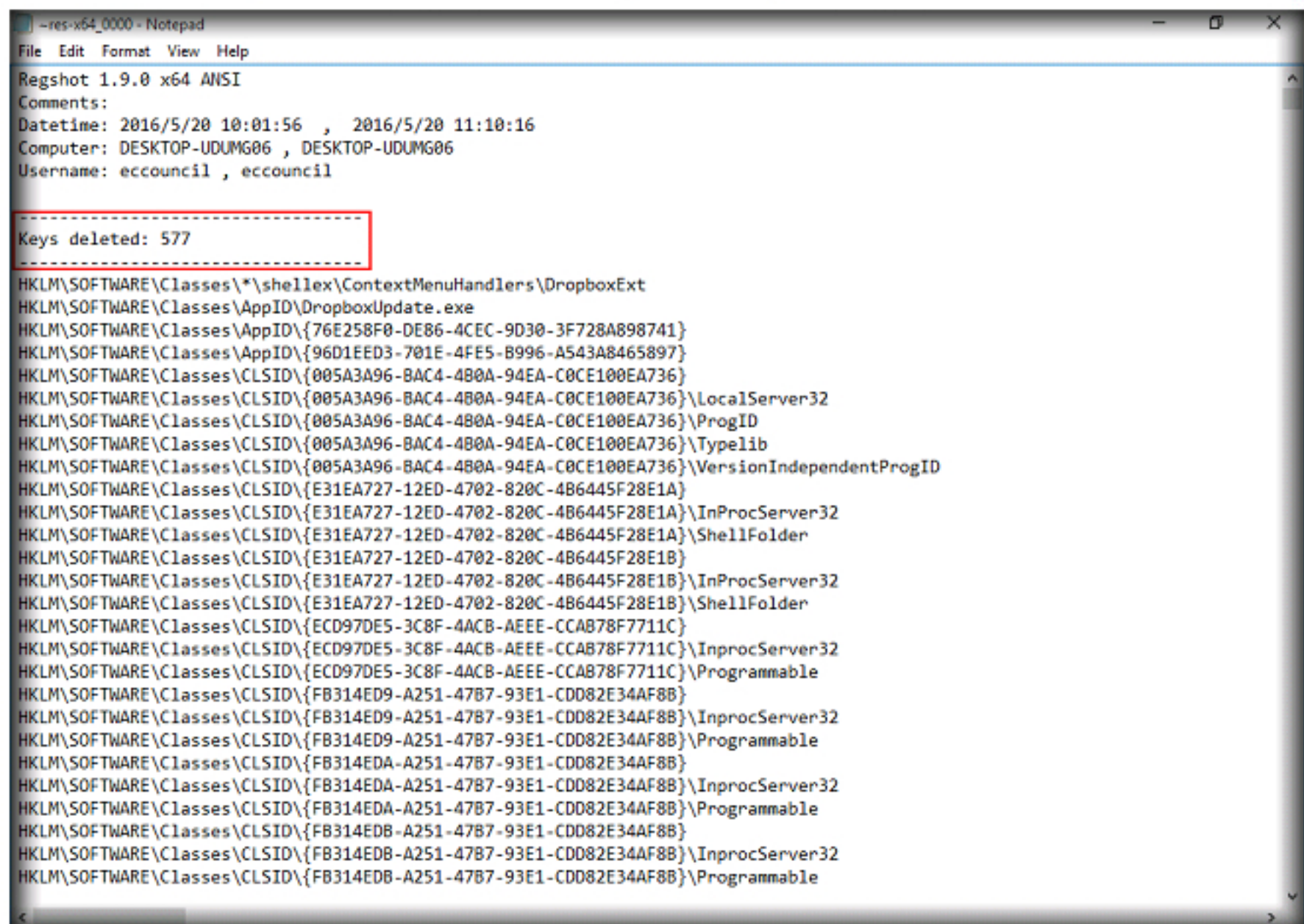


FIGURE 1.53: Viewing the Regshot output file

80. Comparing the addresses changed after uninstallation with the ones modified after installation will give you the files and folders that still store Dropbox data. Analyze these folders to find evidences.
81. Other files that store Dropbox data are registry keys, recent files, LNK files, browser history and cache, Thumbnails Registry Point, Volume Shadow Copies, Pagefile.sys, and Hiberfil.sys.

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.

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

Investigation of Google Drive

Google Drive is a cloud storage service that allows users to access it from various sources such as desktop client, browser and mobile application. Investigators need to understand the process through which it saves the files and allows access to collect evidences in case of attacks.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

An expert forensics investigator needs to have knowledge of how Google Drive can impact a system's files and folders, along with other changes it makes. This lab will help you learn about files, folders, registry, local machine keys, etc., a Google Drive client uses on a system. It will also help you to learn the process of extracting the data from these files for investigation.

You will learn to gather evidences of attack on a Google Drive account when accessed through client browser and also when the user has uninstalled the client.

Lab Objectives

The objective of this lab is to find the files, folders, registry keys, and other Google Drive Data from a system.

Lab Environment

In this lab, you need:

- A computer running on Windows 10.
- Internet connection.
- Google Drive account.
- Tools such as Disk Pulse, What Changed, HxD Editor, RAM Capturer, WebBrowserView and DB Browser located at **Z:\CHFIV9 Module 10 Cloud Forensics**.

 **Tools demonstrated in this lab are available in Z:\CHFIV9 Module 10 Cloud Forensics**

Lab Duration

Time: 35 Minutes

Lab Tasks

TASK 1

Google Drive Installation

1. Navigate to **Z:\CHFIv9 Module 10 Cloud Forensics** and install the tools Disk Pulse, WhatChanged, HxD Editor, RAM Capturer, WebBrowserView and DB Browser
 - a. WhatChanged: **Z:\CHFIv9 Module 10 Cloud Forensics\Registry Changes Tracking Tools\WhatChanged Portable**
 - b. Disk Pulse: **Z:\CHFIv9 Module 10 Cloud Forensics\Registry Changes Tracking Tools\Disk Pulse**
 - c. Directory Monitor: **Z:\CHFIv9 Module 10 Cloud Forensics\Registry Changes Tracking Tools\Directory Monitor**
 - d. RAM Capturer: **Z:\CHFIv9 Module 10 Cloud Forensics\RAM Capturer**
 - e. HxD: **Z:\CHFIv9 Module 10 Cloud Forensics\Hex Editor Tools\HxD**
 - f. WebBrowserPassView: **Z:\CHFIv9 Module 10 Cloud Forensics\Password Recovery Tools\WebBrowserPassView**
2. Run the **WhatChanged** tool to create a baseline state of the system. Select the **Scan Registry** option and also check the **LOCAL MACHINE** option.
3. Click the **Step #1: Get Baseline State button** to capture first snapshot or create baseline of the system.

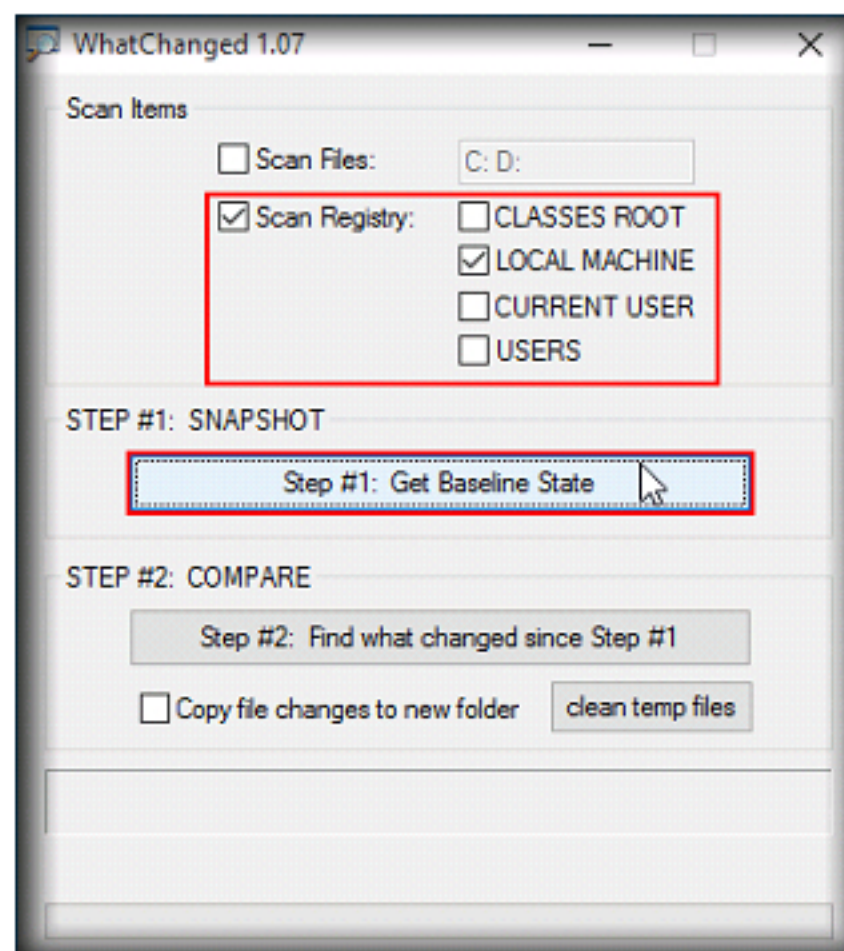


FIGURE 2.1: Performing step 1 in WhatChanged tool

4. The tool will prompt a **WhatChanged** dialog box displaying the total number of entries it recorded. Click the **OK** button.

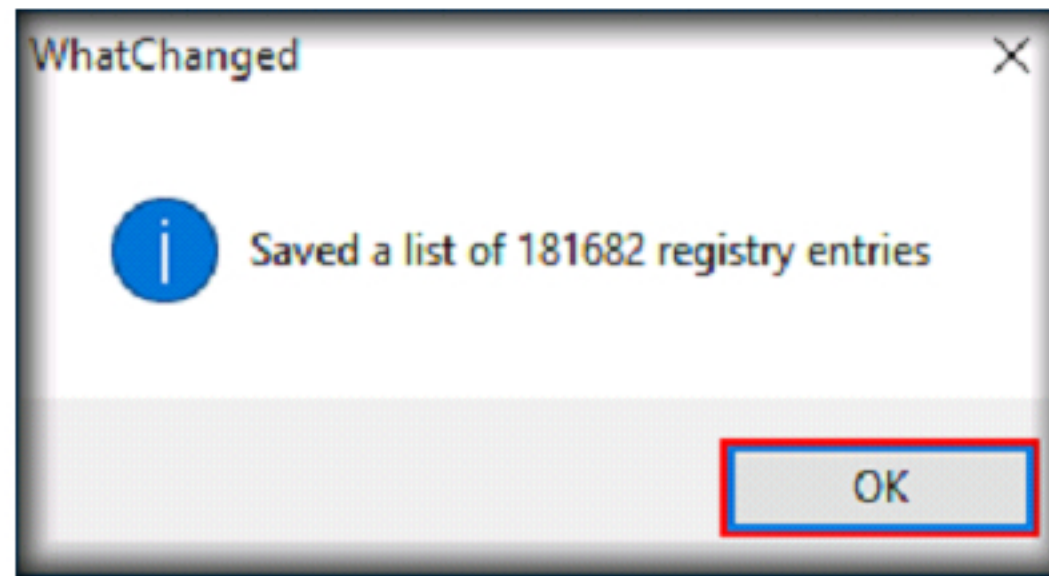


FIGURE 2.2: WhatChanged dialog box

5. Run the **Disk Pulse** tool and click the **Monitor** button to start monitoring changes made to a particular folder.

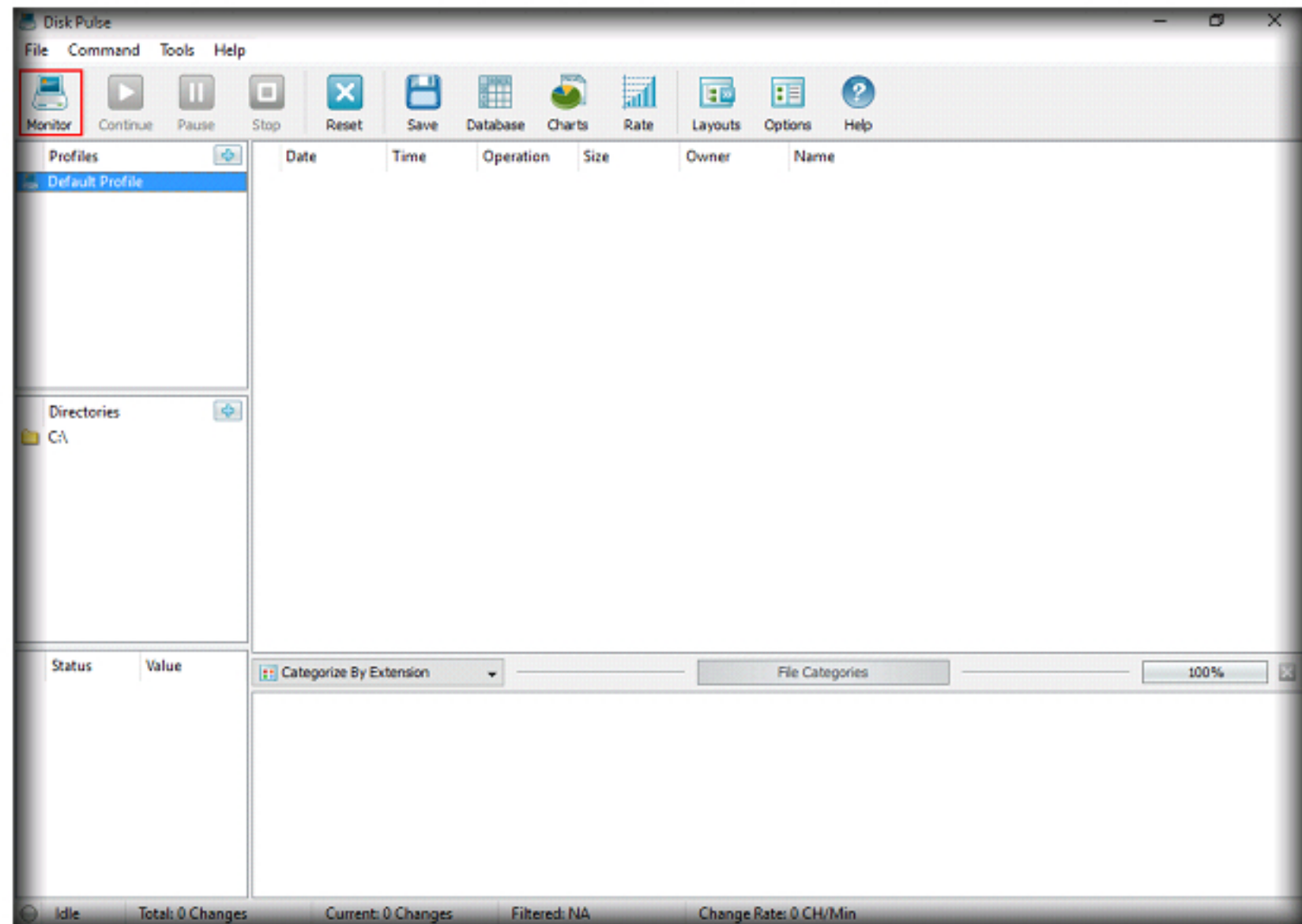


FIGURE 2.3: Clicking on Monitor option in Disk Pulse tool

6. The tool will display a **Default Profile** dialog box which will allow the user to add directories you want to monitor. The tool adds **C:** directory to this profile by default.

7. Click **Add** to add more directories, else click the **Start** button.

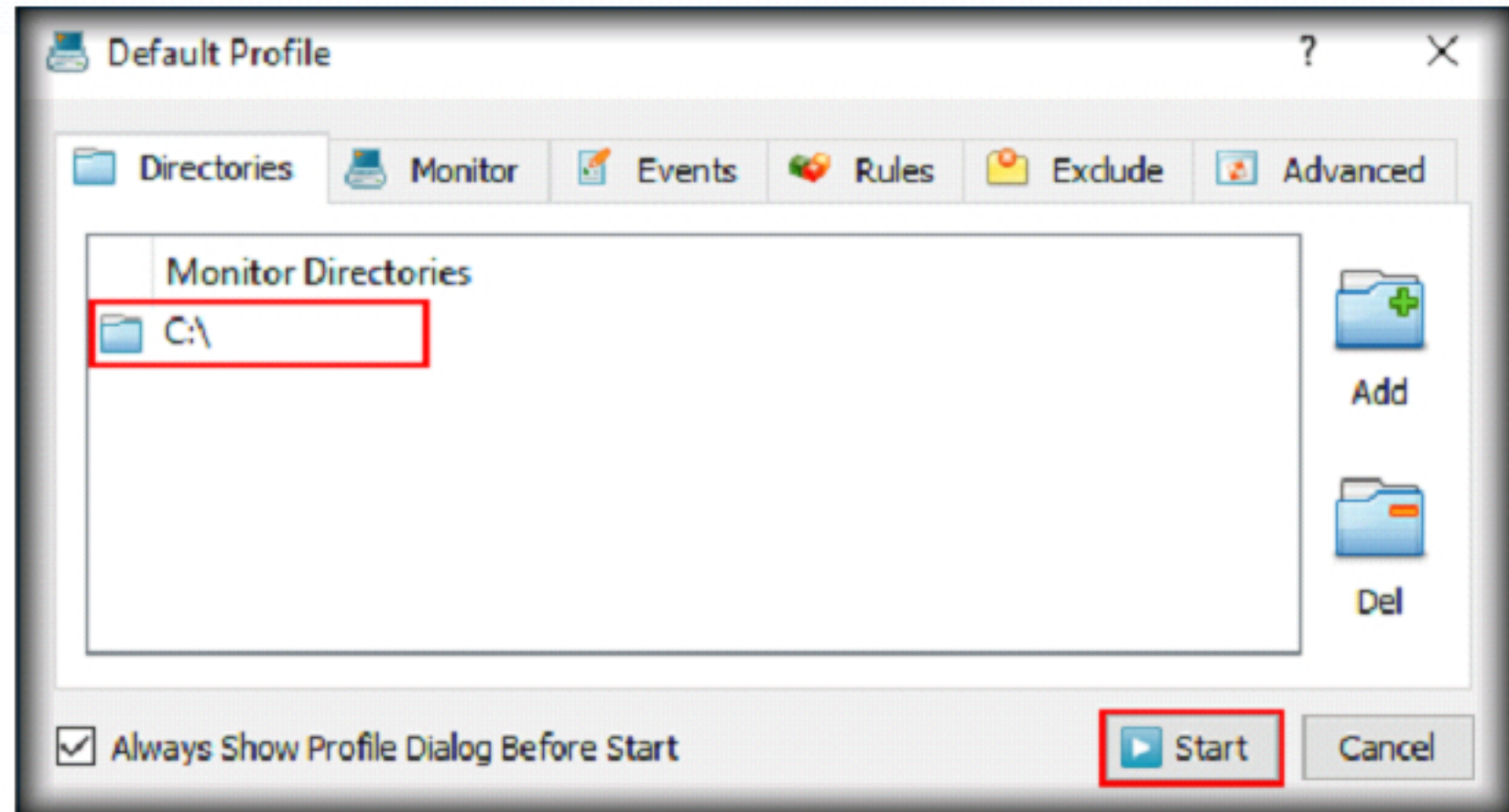


FIGURE 2.4: Starting monitoring of the selected folder

8. Navigate to **Z:\CHFIv9 Module 10 Cloud Forensics\Google Drive Investigation Tools\Google Drive Client**, double-click **googledrivesync.exe** and follow the wizard driven installation steps to install the application. On completing the installation, click **Close** in the **Installation Complete** window.
9. Click **Google Drive** icon in the **Apps** screen to run the Google Drive client, and click on **Get Started** to start using the client.

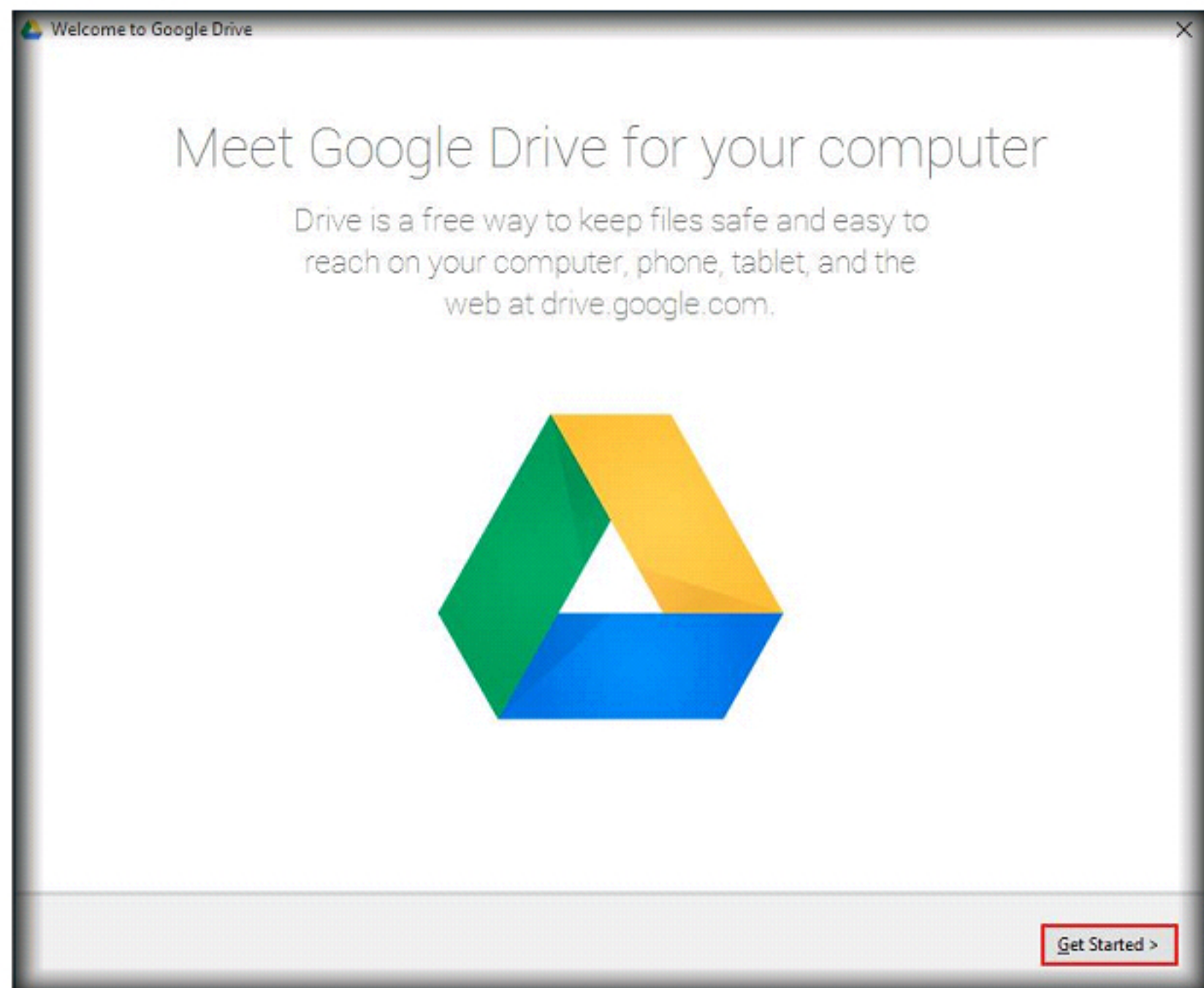


FIGURE 2.5: Google Drive installation

You can download Google Drive installer from <https://www.google.com/drive/>

10. Enter the email address of the Google Drive Account and click the **Next** button.

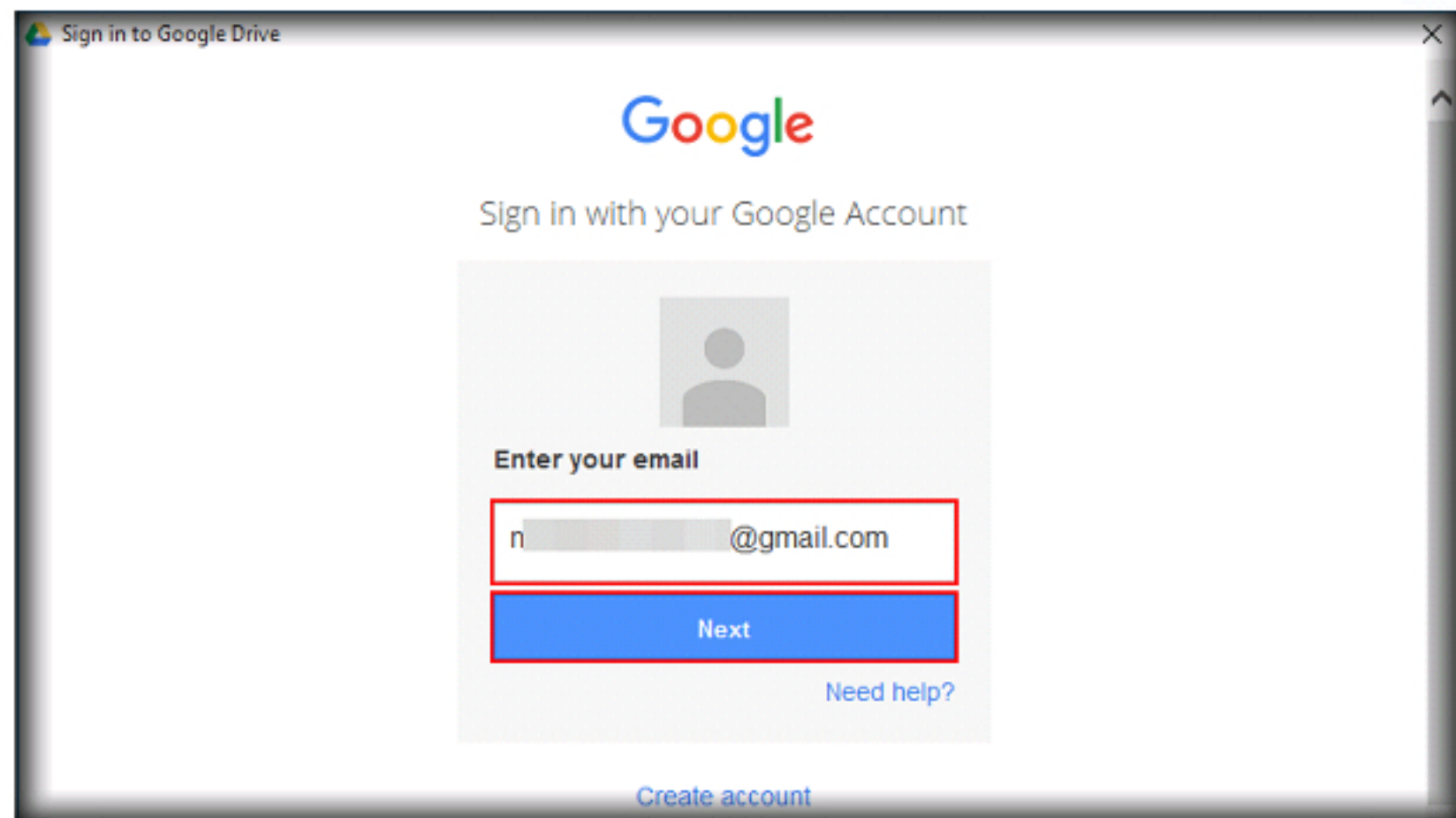


FIGURE 2.6: Entering email address of the Google Drive Account

11. Enter the password of the account and click the **Sign In** button.

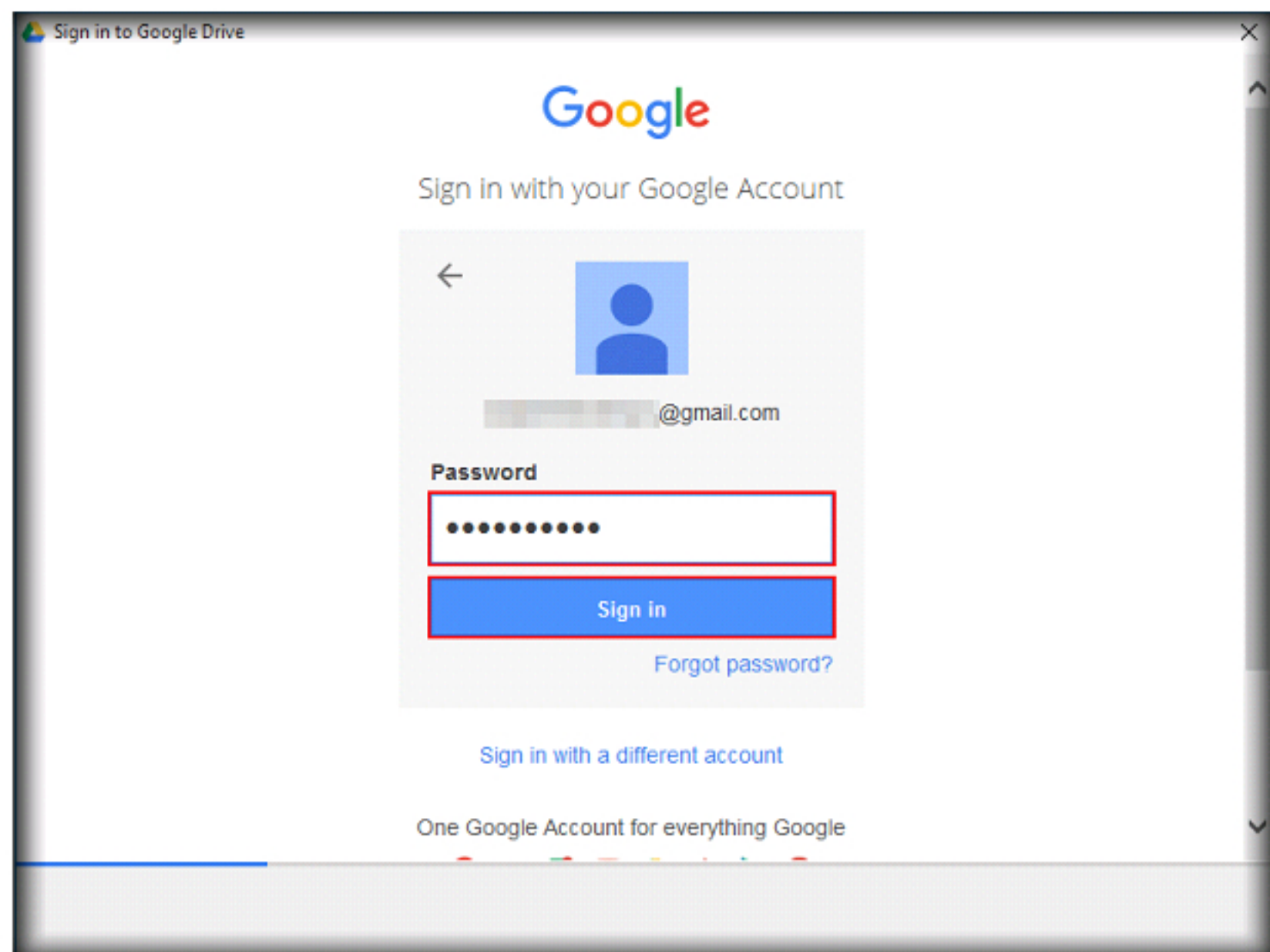


FIGURE 2.7: Entering password of the respective Google Drive Account

12. The Drive client will take you through the installation information. Note this information because it will help you know about the places where the client stores information on the system. Click the **Next** button.

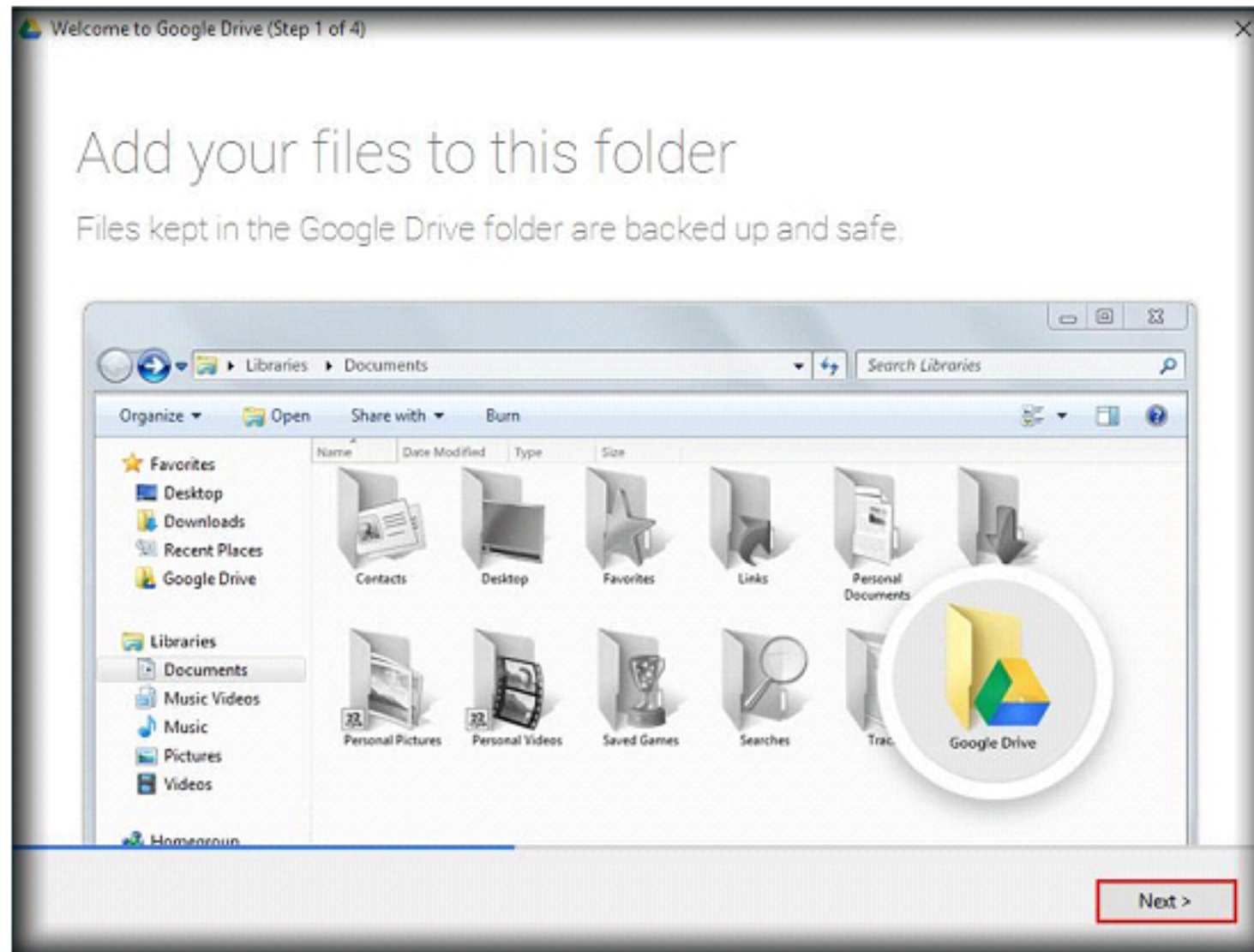


FIGURE 2.8: Google Drive installation

13. Click **Next** button till you go to **Step 4**. Step 4 describes the location which syncs the files on the drive and gives location of a folder that stores the files on the system. In this case, the Google Drive will save a folder at **C:\Users\Administrator\Google Drive** and will sync all the contents saved to cloud to this folder. Click the **Next** button.

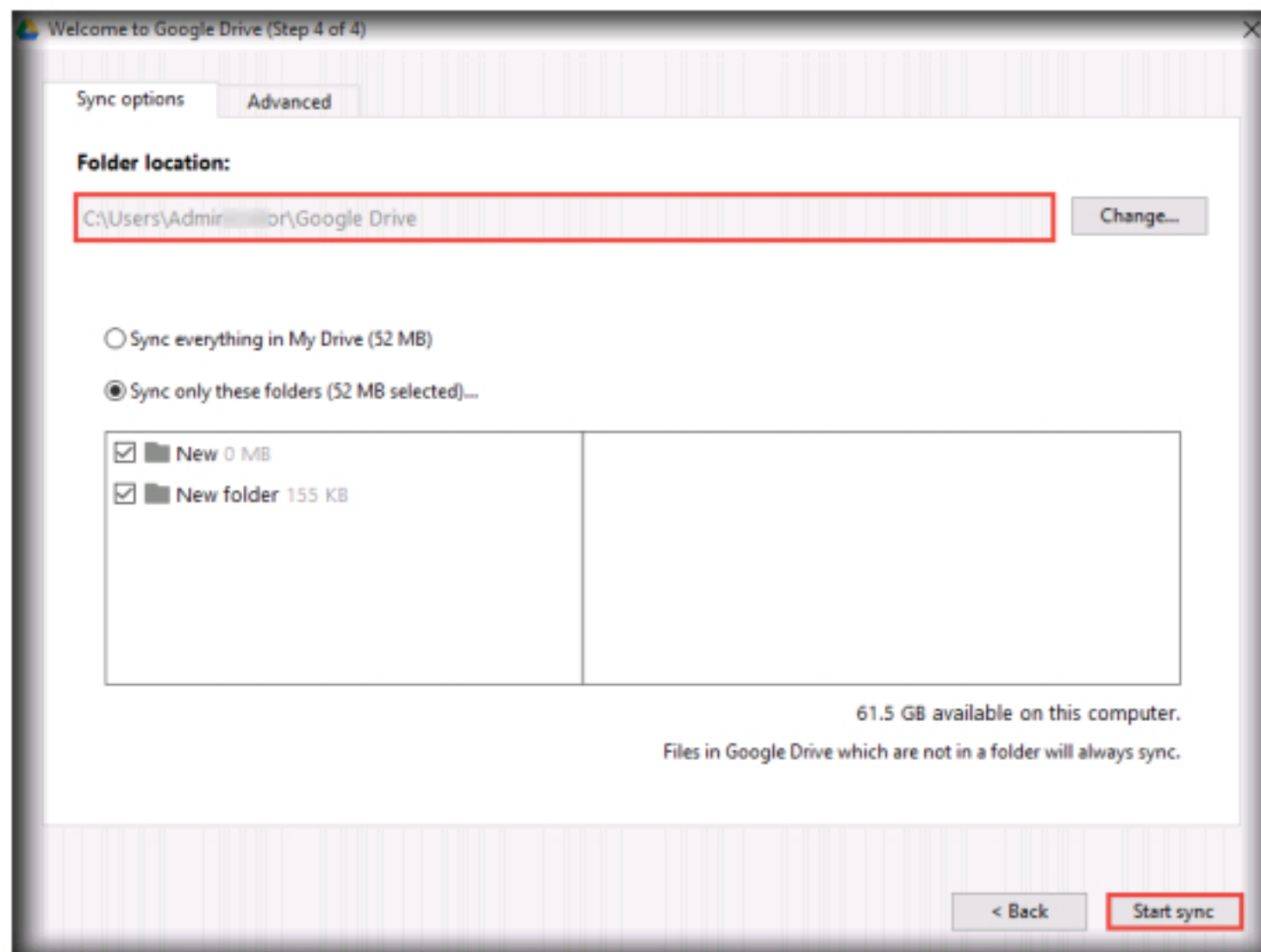


FIGURE 2.9: Screenshot showing the location on the system which syncs the files on the drive

14. Click the **Done** button.

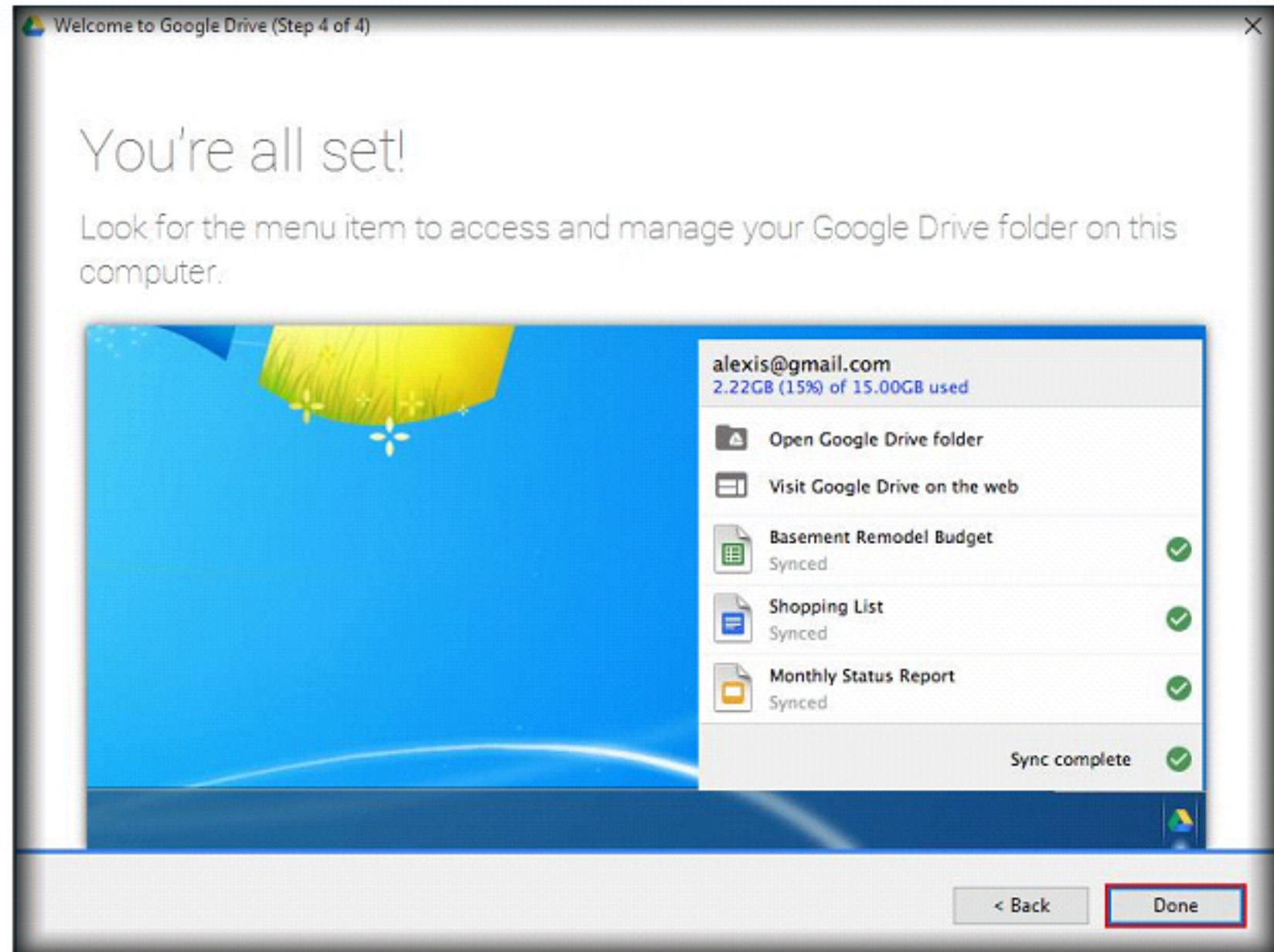


FIGURE 2.10: Final step of installation

15. After installation is completed, go to the **Disk Pulse** tool and click the **Stop** button to stop monitoring process.

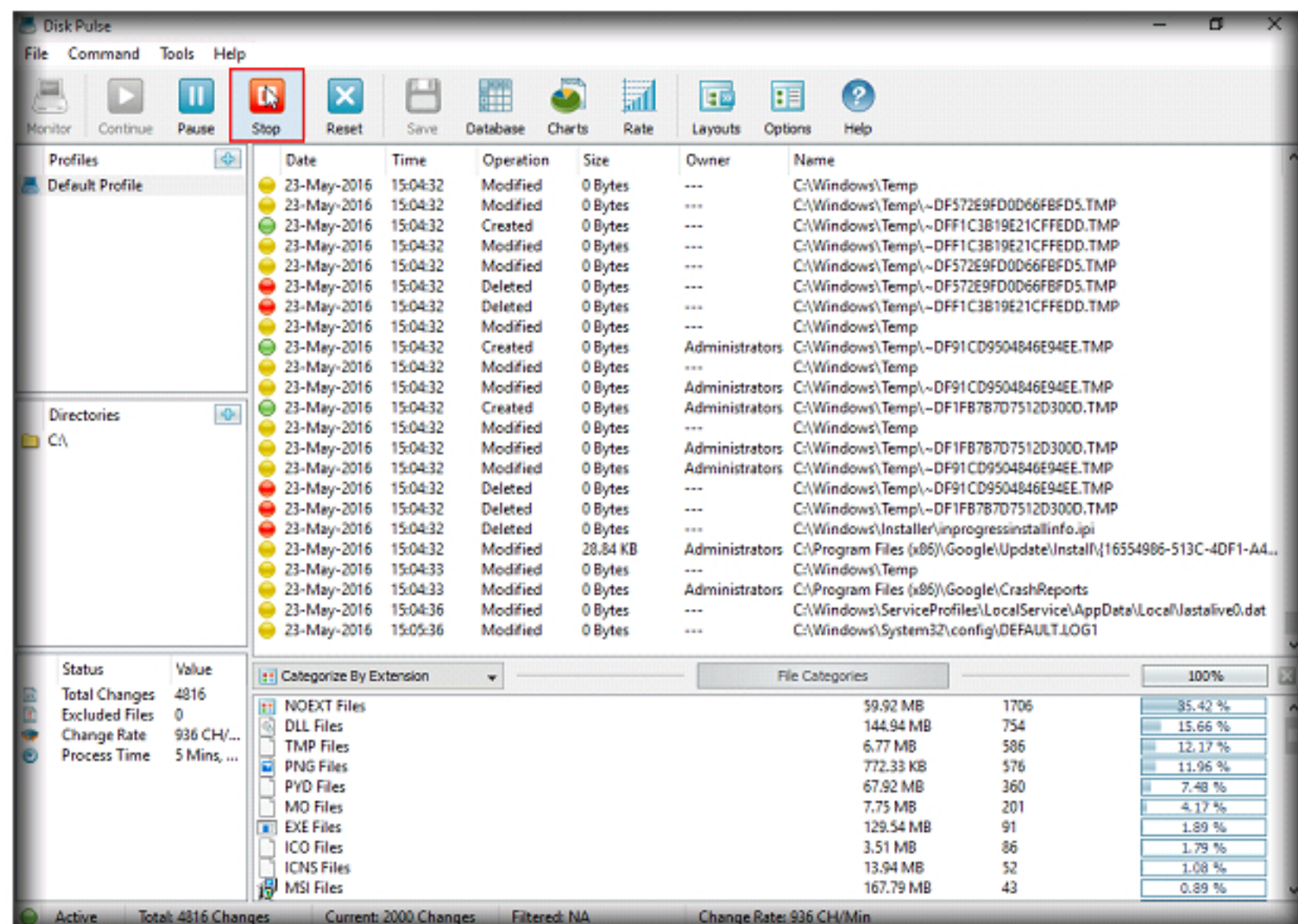


FIGURE 2.11: Stopping the monitoring process in the Disk Pulse tool

16. The tool will display a **Warning** dialog box, click the **Yes** button to stop the monitoring process.

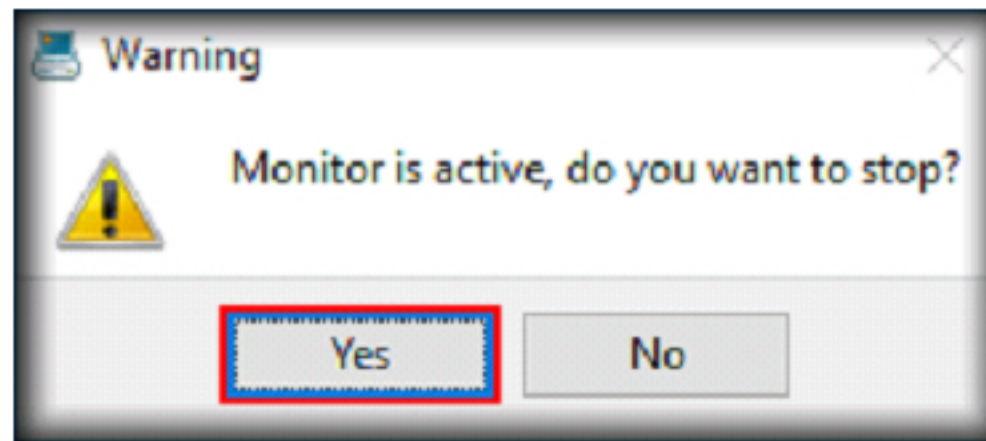


FIGURE 2.12: Disk Pulse tool Warning dialog box

17. Click the Save Record or Save Icon in the tool to save all the entries in the required format.

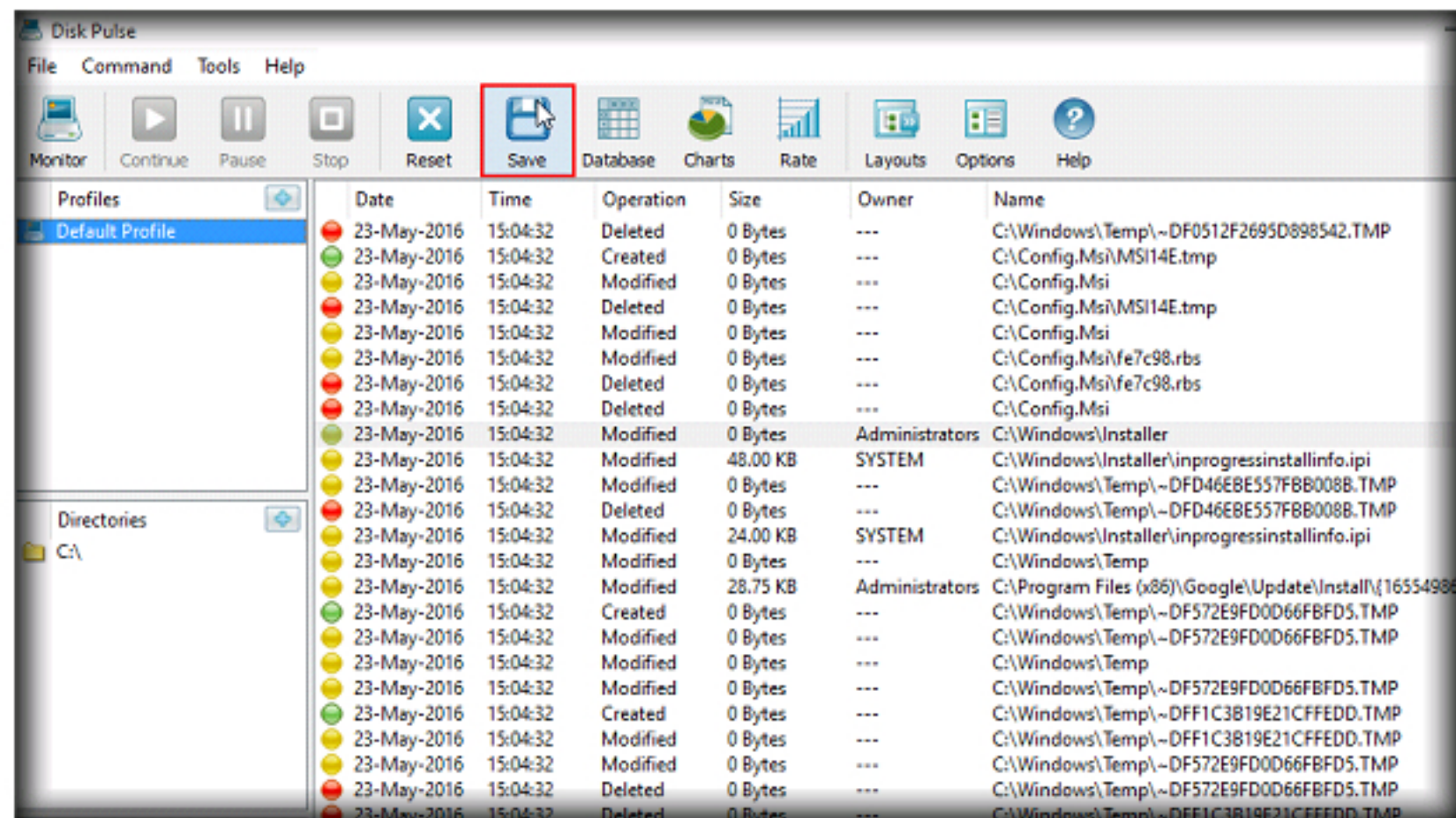


FIGURE 2.13: Saving the Disk Pulse entries in required format

18. The tool will prompt a **Save Disk Change Monitor Report** dialog-box. Click the **Format** option from dropdown list bar and select the required format. Here, you can select **Text format**. Click the **Save** Button.

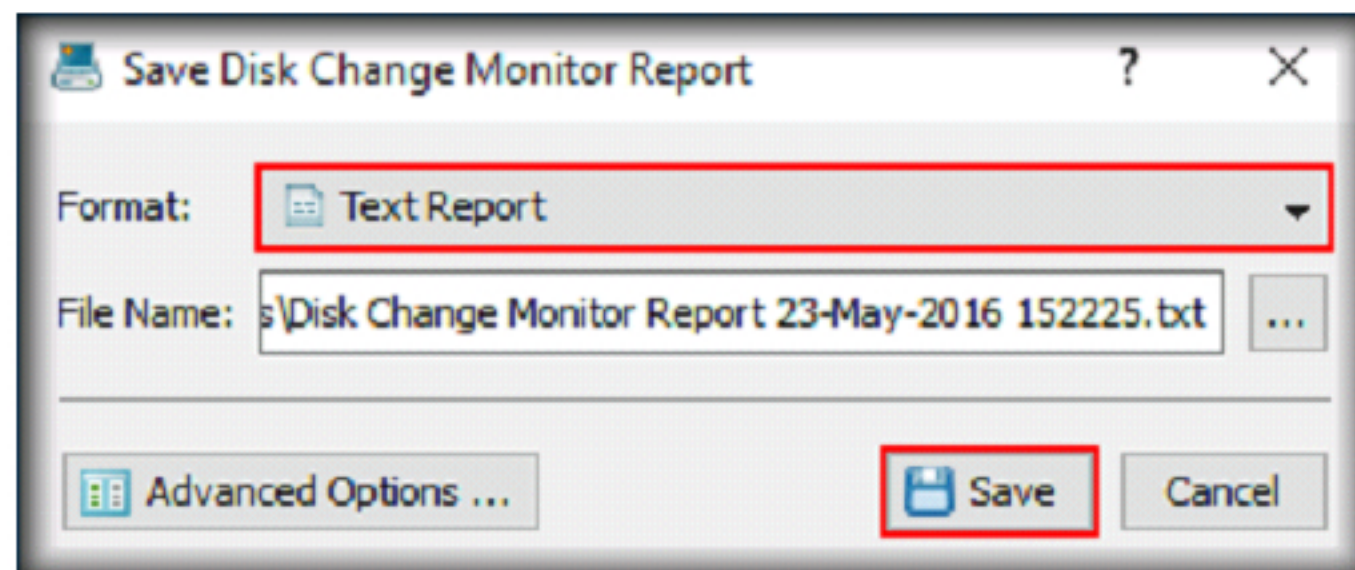


FIGURE 2.14: Selecting the required format to save the Disk Pulse entries

19. The tool will save a Text file with all the changes listed in it.

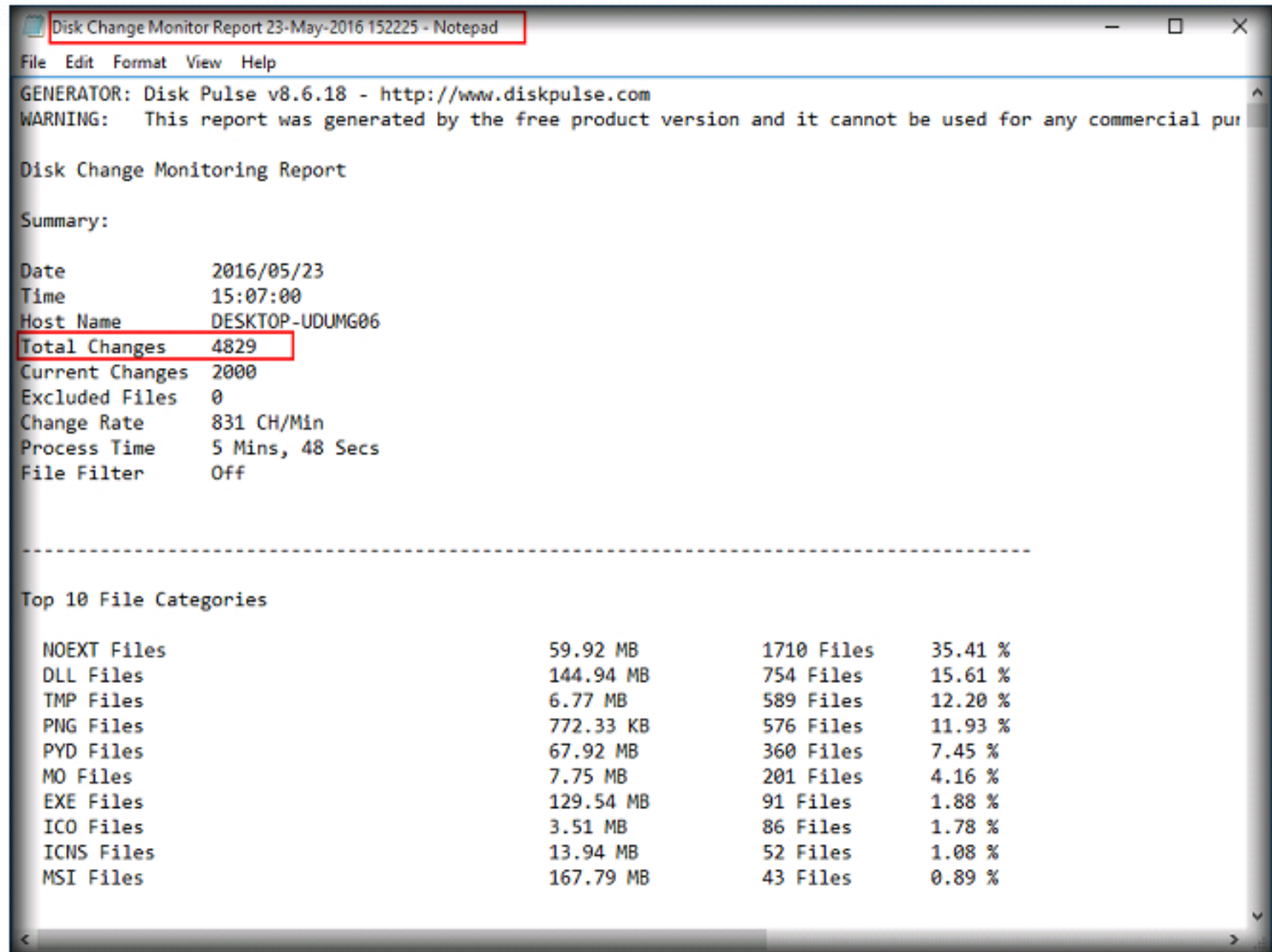


FIGURE 2.15: Viewing the saved Text file with all the changes listed

20. Go to the WhatChanged tool and take the second snapshot of the system. Click the **Step #2: Find what changed since Step #1.**

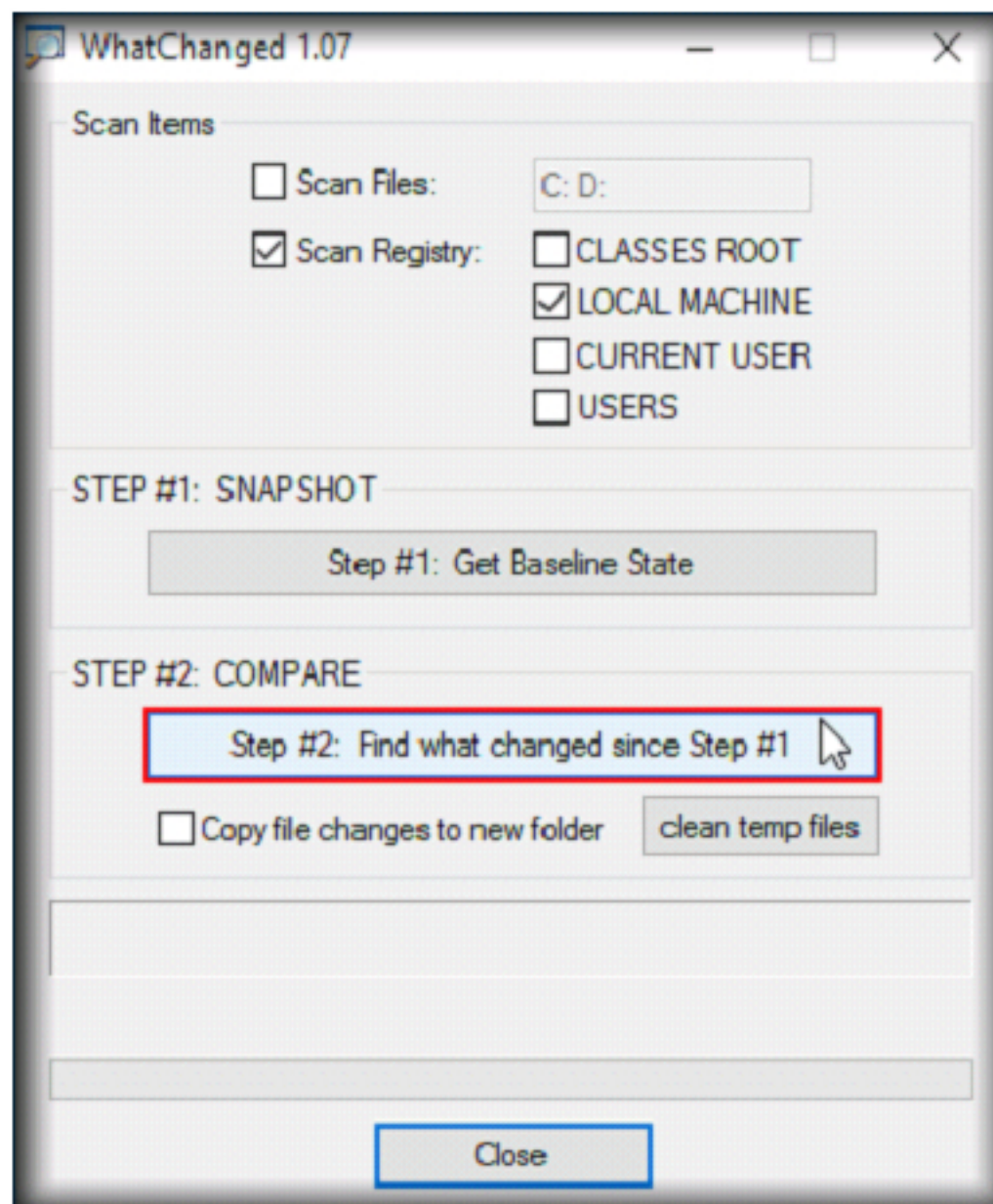


FIGURE 2.16: Executing the Step 2 of the WhatChanged tool

21. The tool will check for the changed entries and re-record all the modified ones. The tool will display the number of changes it has observed across the system and also the progress of scanning.

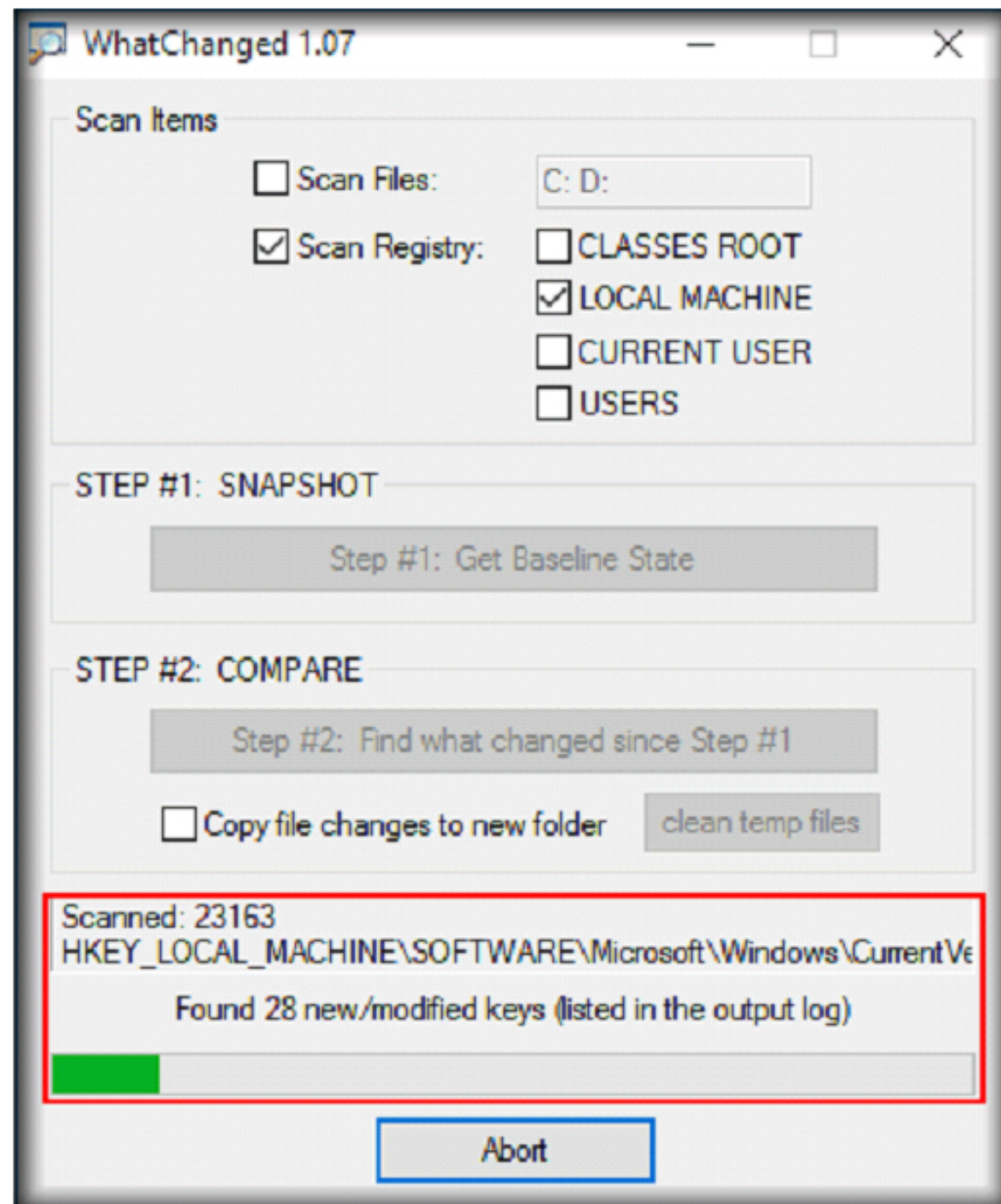


FIGURE 2.17: Comparison under process

22. On completion of scanning process, the tool will display a dialog box displaying the number of new entries it listed. Click the **OK** button.

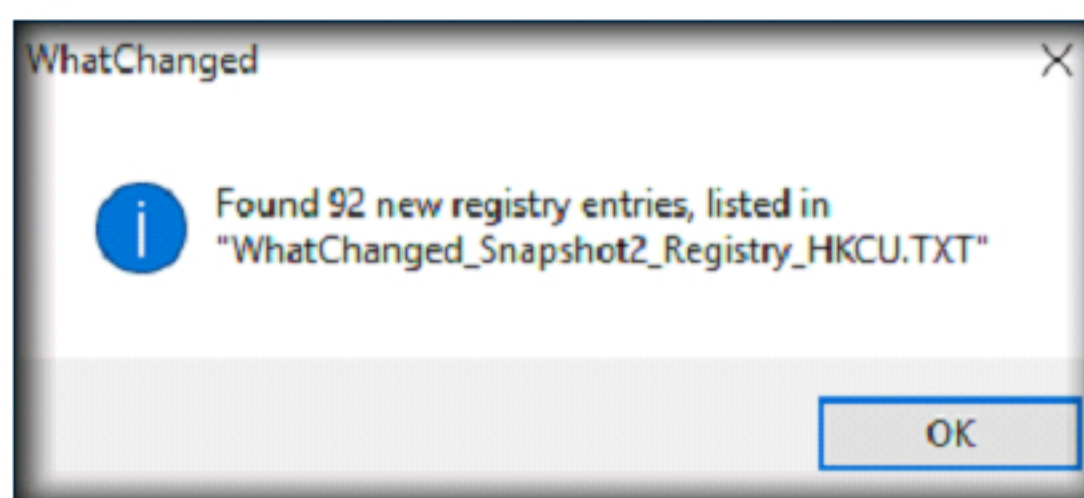


FIGURE 2.18: WhatChanged tool displaying the resultant changes after comparison

23. The tool saves a list of all the changed entries in a text file at the same location as the tool.

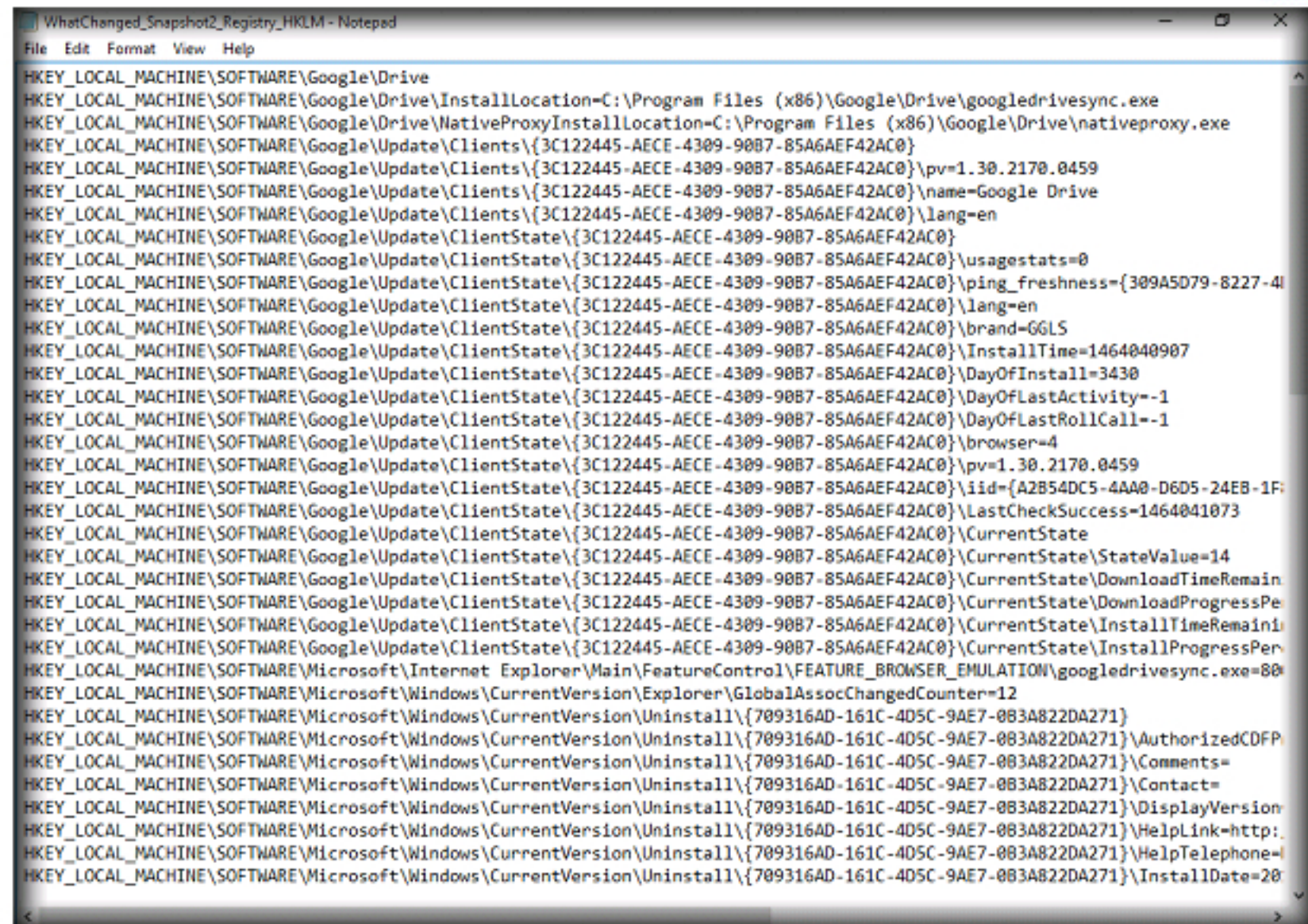


FIGURE 2.19: Notepad file showing the occurred changes

24. The Google Drive client makes many changes in the system such as creation of folders. It stores its configuration files in **C:\Users\<User Name>\AppData\Local\Google\Drive\user_default**.

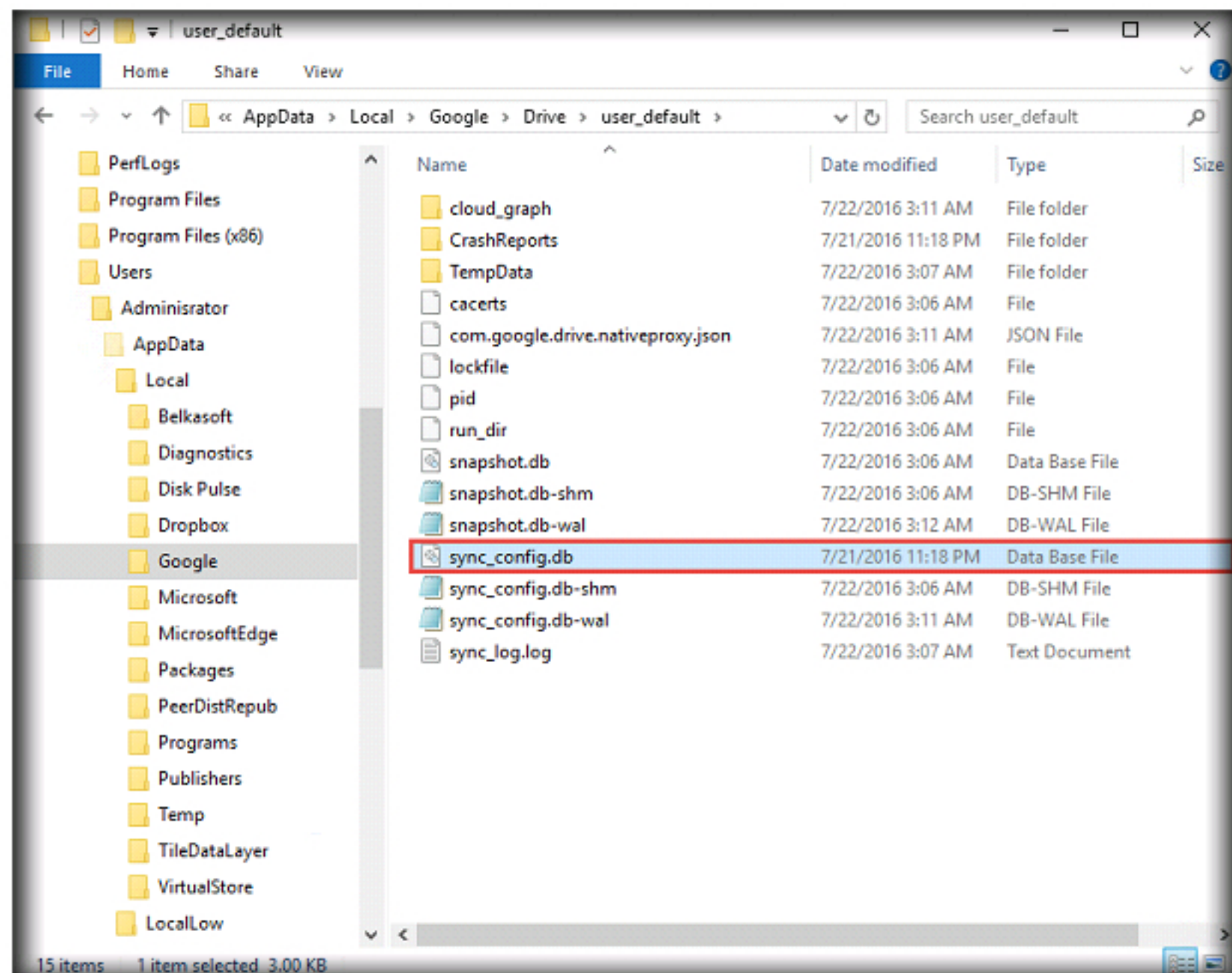


FIGURE 2.20: Screenshot showing the path of the Google Drive client

25. Other files created during installation include

- **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Drive\Google Drive.lnk**
- **C:\Windows\Prefetch\GOOGLEDRIVESYNC.EXE-NNNNNNNN.pf**
- **C:\Windows\Prefetch\GOOGLEUPDATE.EXE-NNNNNNNN.pf**

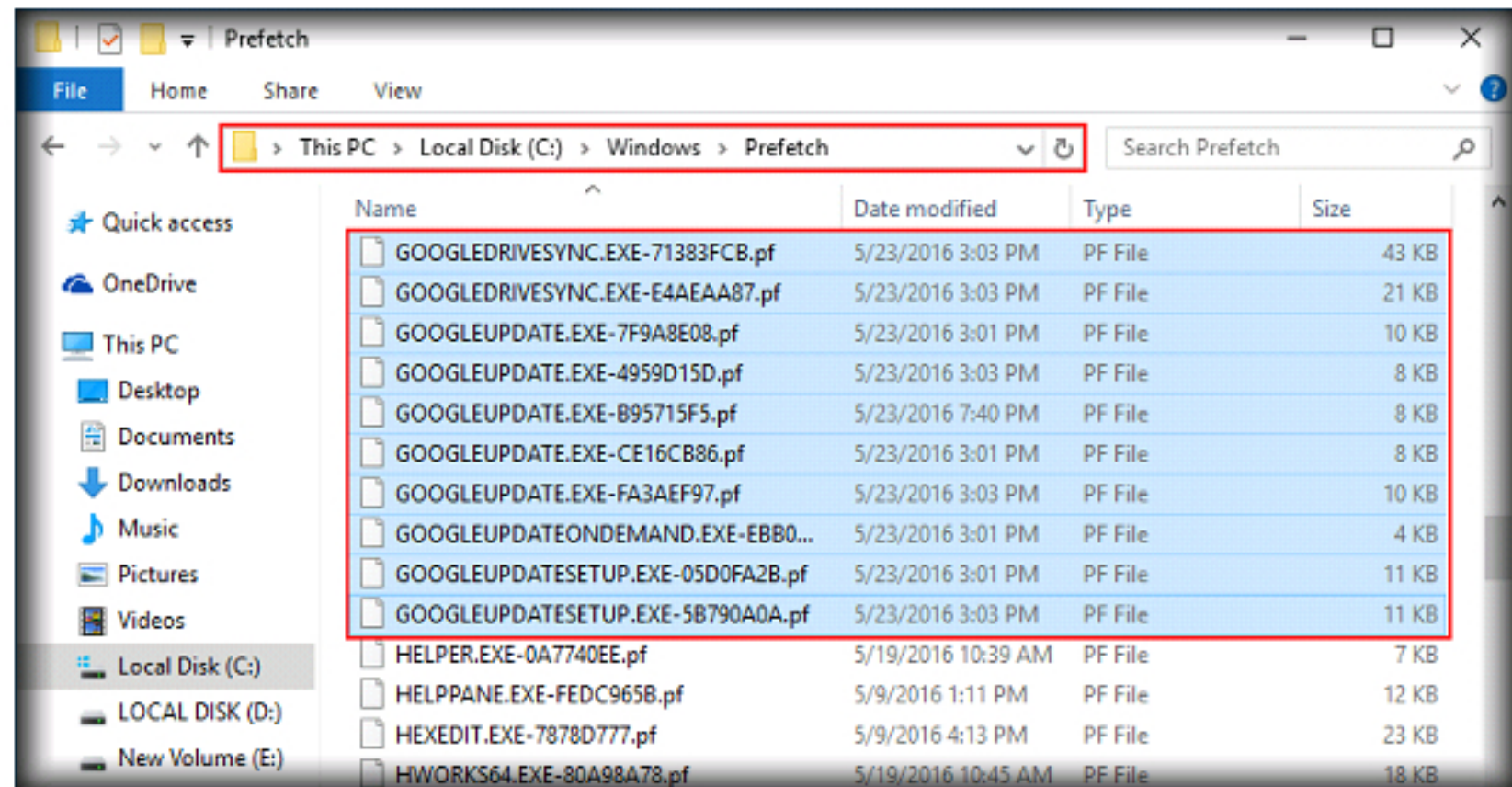


FIGURE 2.21: Screenshot showing the files created during installation

26. Run the **DB Browser for SQLite** tool and click the **Open Database** option.

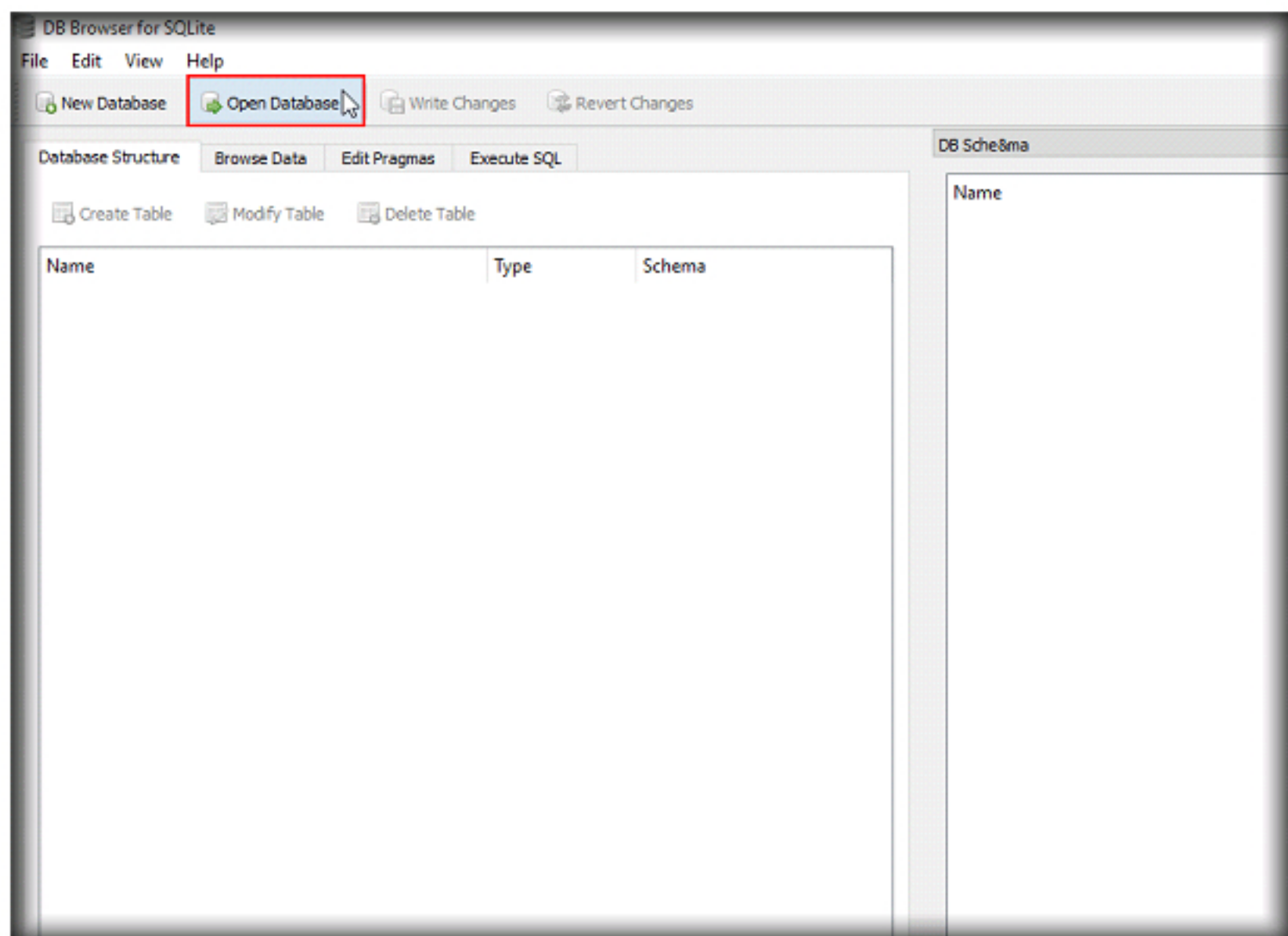


FIGURE 2.22: DB Browser for SQLite tool with Open Database option highlighted

27. Navigate to the location **C:\Users\<User Name>\AppData\Local\Google\Drive\user_default**, where Google Drive has stored the configuration files, select the **sync_config** database file, and click **Open** button.

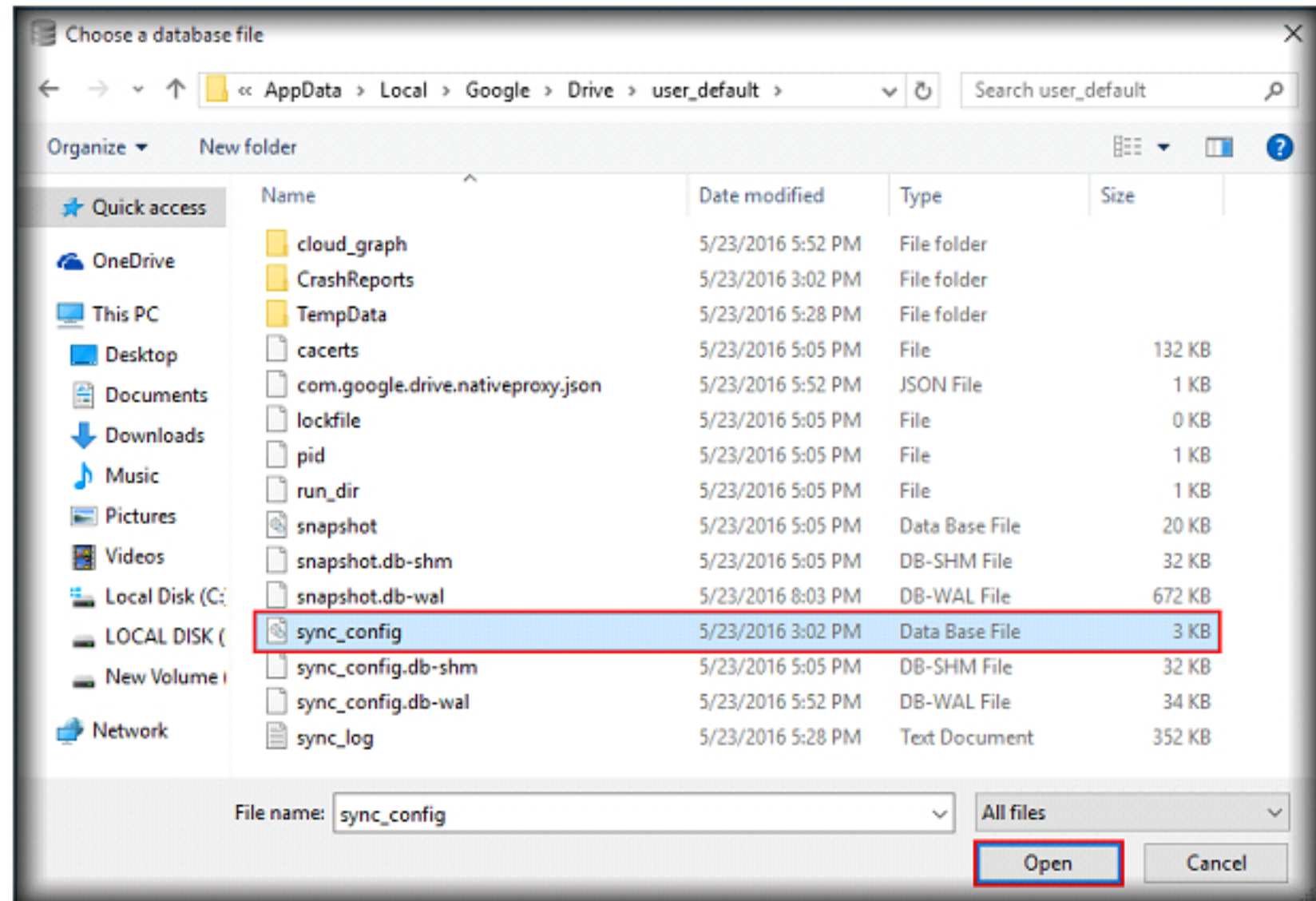


FIGURE 2.23: Opening sync_config database file

28. Click the **Browse Data** tab to view the details stored in the database file. The file stores data such as user's email address, local sync root path, and highest_app_version.

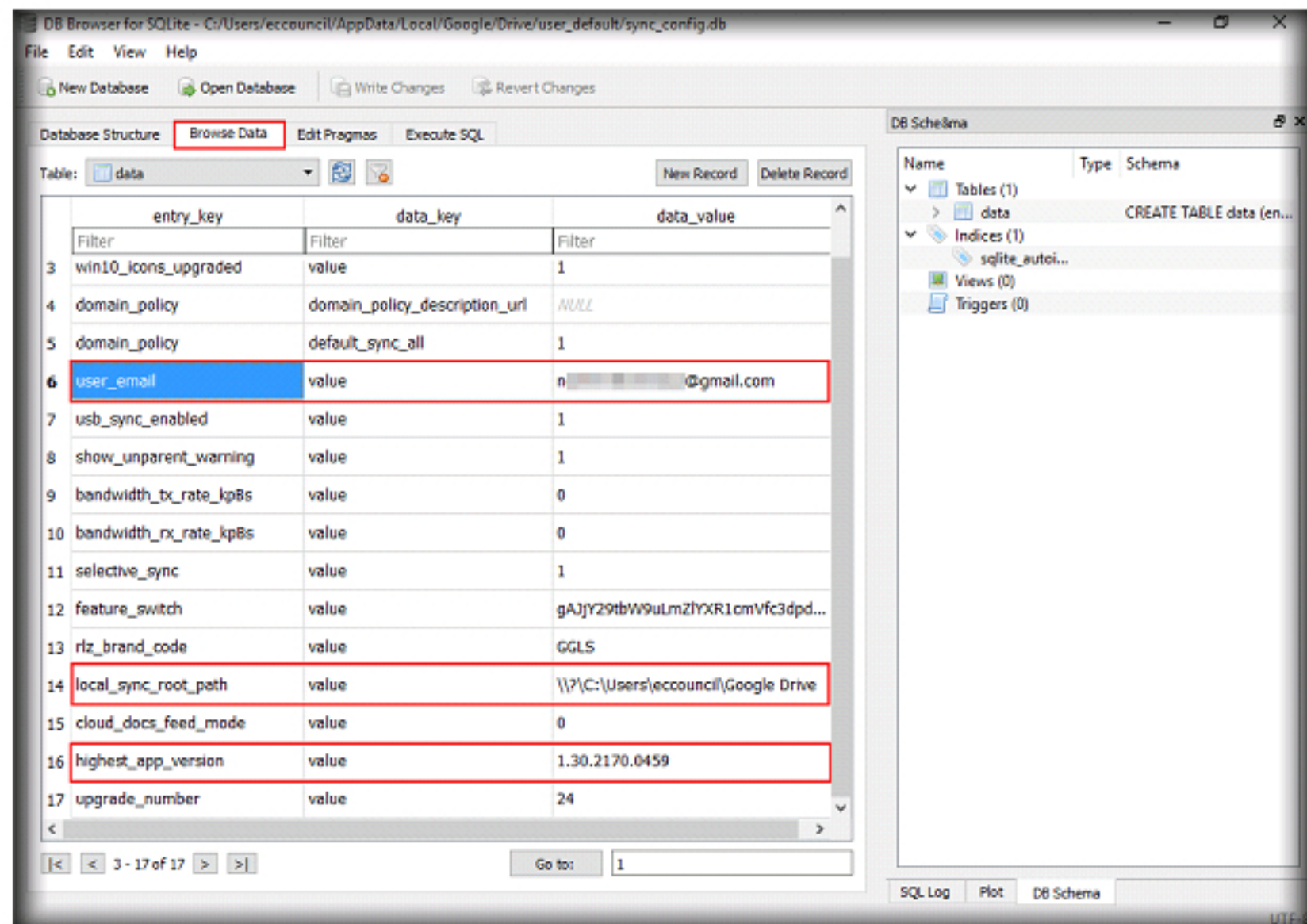


FIGURE 2.24: Viewing the details stored in the database file from Browse Data tab

29. Click **Open Database** button again and upload the snapshot database file from the location **C:\Users\<User Name>\AppData\Local\Google\Drive\user_default**.
30. The snapshot database file will display the process a user has opted to upload a file onto Google Drive. It differentiates them by mentioning if it is a cloud entry or a local entry.

Cloud entry refers to the files directly uploaded onto the drive (using Google Drive web/client application), whereas local entry refers to the files copied to the local sync folder associated with Google Drive.

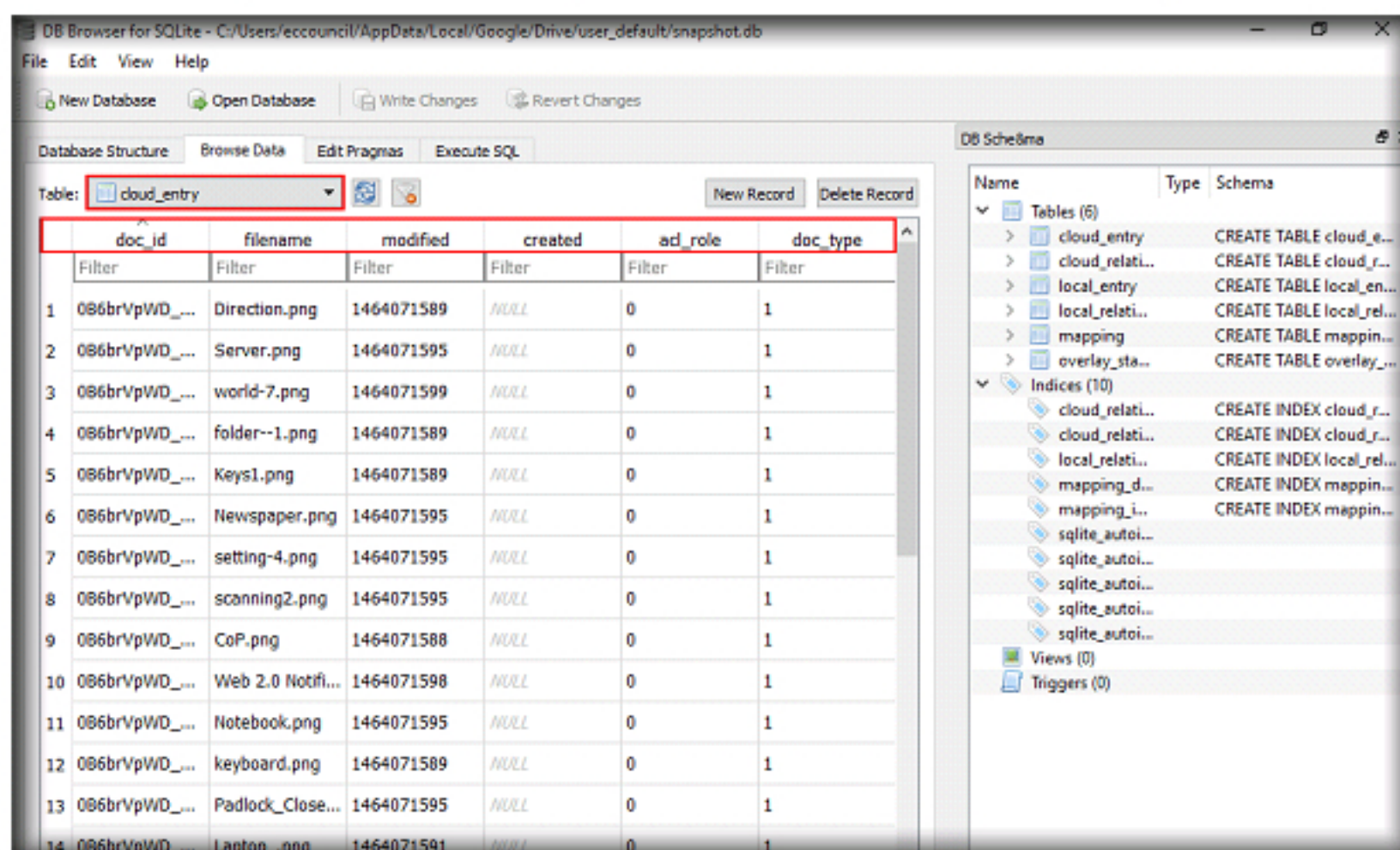


FIGURE 2.25: Viewing the files in cloud entry location

31. The database file also contains information about all files added to the local sync folder of the cloud storage.

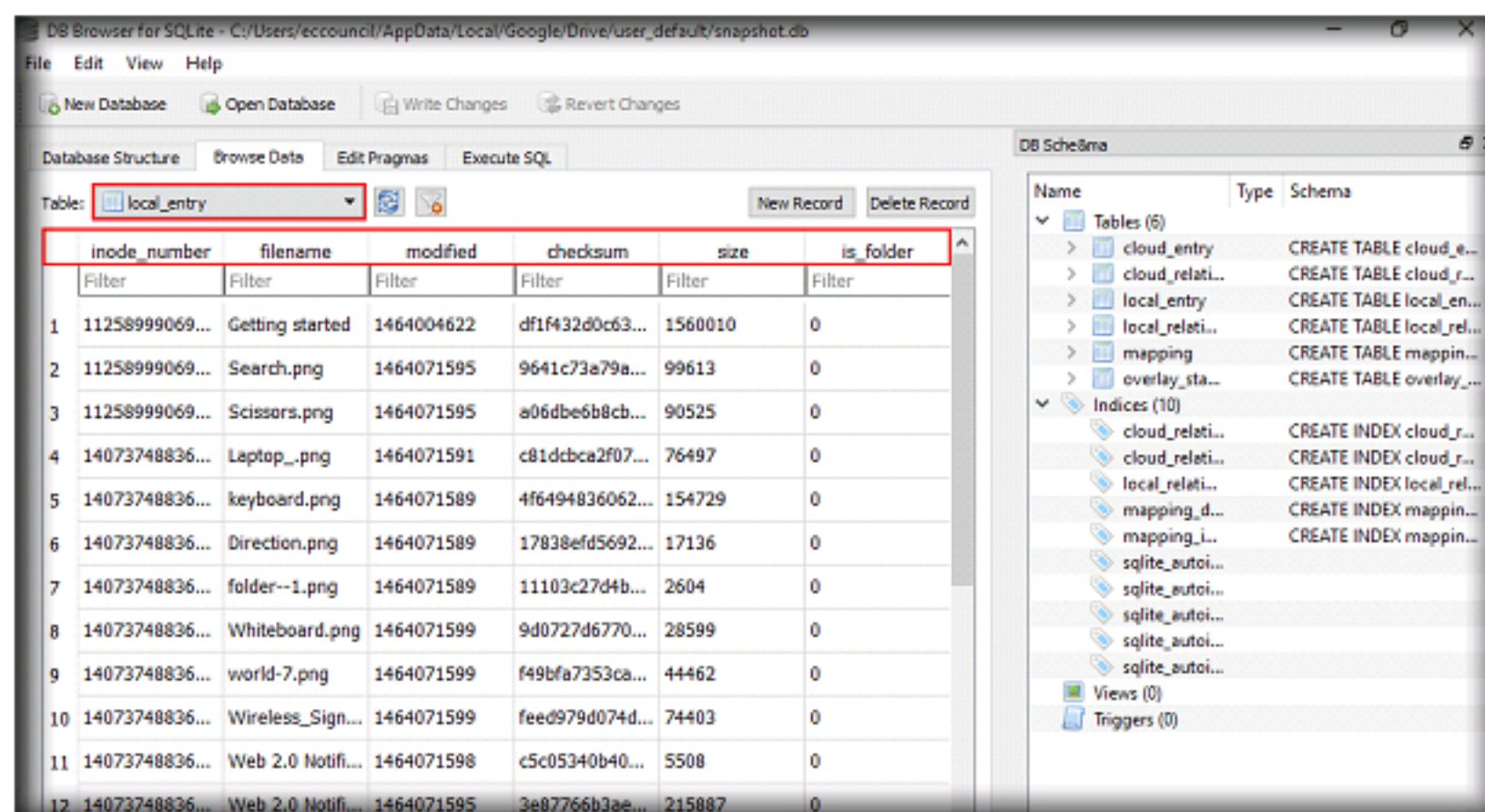


FIGURE 2.26: Viewing the files in local sync folder

32. Navigate to the Google Drive's configuration folder, i.e., **C:\Users\<Username>\AppData\Local\Google\Drive\user_default** and open the **Sync_log.log** file.
33. The file stores details of activities across the account and also provides details about them.

```

sync_log - Notepad
File Edit Format View Help
(SyncType.UNKNOWN_SYNC_TYPE)) - Read request - nowhereforensics@gmail.com
2016-05-23 17:52:29,289 -0700 INFO pid=3236 3864:FeatureSwitchPoller apiclient.discovery:762
URL being requested: GET https://www.googleapis.com/drive/v2internal/settings?fields=items
%2Fkey%2Citems%2Fvalue&reason=304&namespace=FEATURE_SWITCH&alt=json
2016-05-23 17:52:29,289 -0700 INFO pid=3236 3864:FeatureSwitchPoller oauth2client.client:515
Attempting refresh to obtain initial access_token
2016-05-23 17:52:29,289 -0700 INFO pid=3236 3864:FeatureSwitchPoller oauth2client.client:735
Updated access_token read from Storage
2016-05-23 17:52:29,289 -0700 INFO pid=3236 3864:FeatureSwitchPoller common.proxy_manager:354
Removing stale proxy entry from cache
2016-05-23 17:52:29,289 -0700 INFO pid=3236 3652:Worker-2 common.persistence.sqlite:276
Open master connection to C:\Users\ECCOUN~1\AppData\Local\Google\Drive\user_default
\snapshot.db
2016-05-23 17:52:29,289 -0700 INFO pid=3236 3652:Worker-2 common.persistence.sqlite:276
Open master connection to C:\Users\ECCOUN~1\AppData\Local\Google\Drive\user_default
\sync_config.db
2016-05-23 17:52:29,289 -0700 INFO pid=3236 3652:Worker-2 common.threads.threads:130
AddCleanupCallback persistence_sqlite:8207c25277024fc0aa8cbd38e5709639C:\Users
\ECCOUN~1\AppData\Local\Google\Drive\user_default\snapshot.db
2016-05-23 17:52:29,289 -0700 INFO pid=3236 3652:Worker-2 common.threads.threads:130
AddCleanupCallback persistence_sqlite:3ad3fcba3d454d1698f18189fa2d9dc5C:\Users
\ECCOUN~1\AppData\Local\Google\Drive\user_default\sync_config.db
2016-05-23 17:52:29,289 -0700 INFO pid=3236 3652:Worker-2
common.worker.command_factory:175 Registered worker command types:
  
```

FIGURE 2.27: Viewing the information stored in Sync_log.log file

34. Open a web browser and open Google Drive home page by entering the URL **https://www.google.co.in/drive** in the address bar. Google Drive homepage appears, click **Go to Google Drive** button.

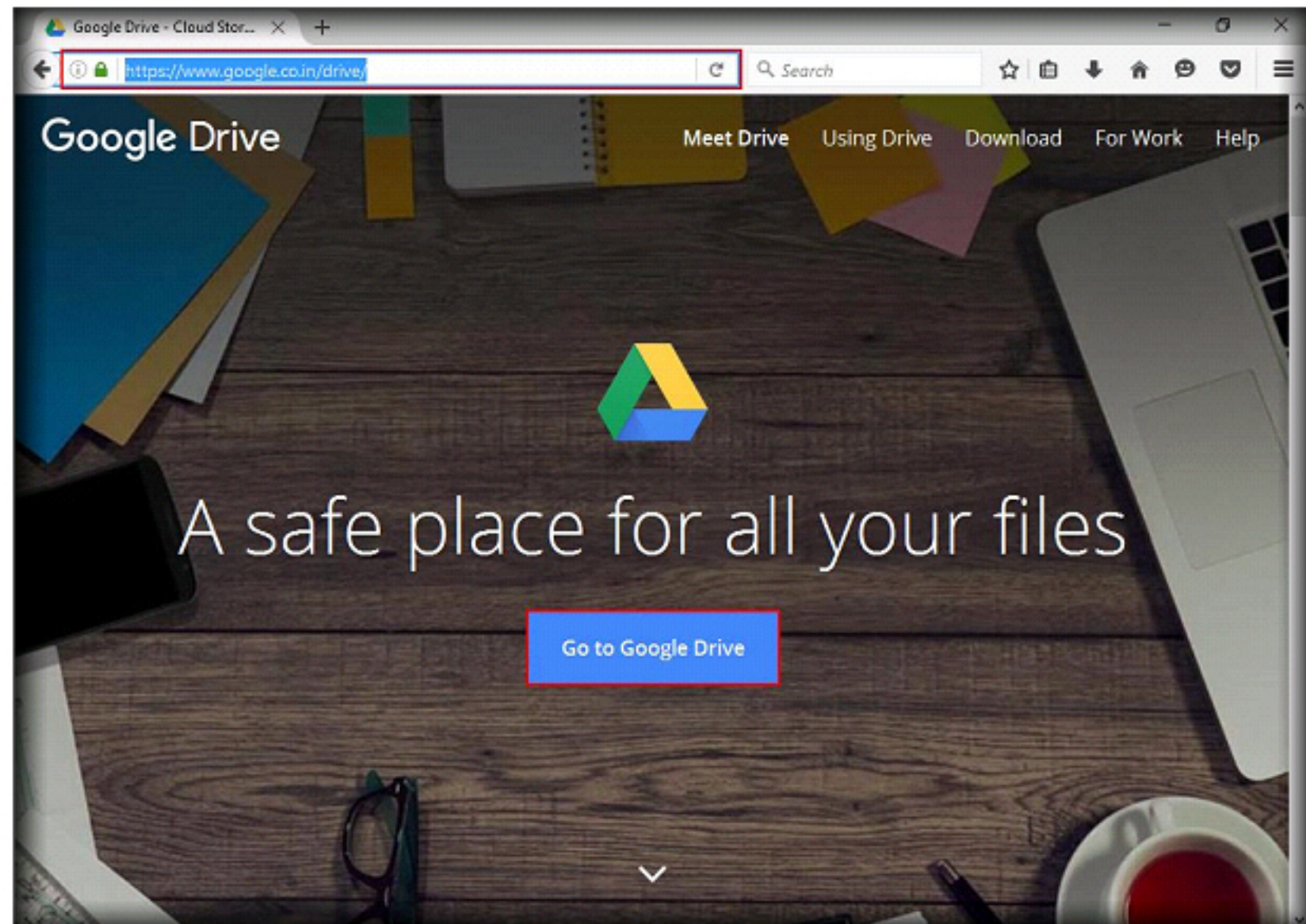


FIGURE 2.28: Google Drive home page

35. Enter the email ID of the Dropbox account in the provided box and click the **Next** button.

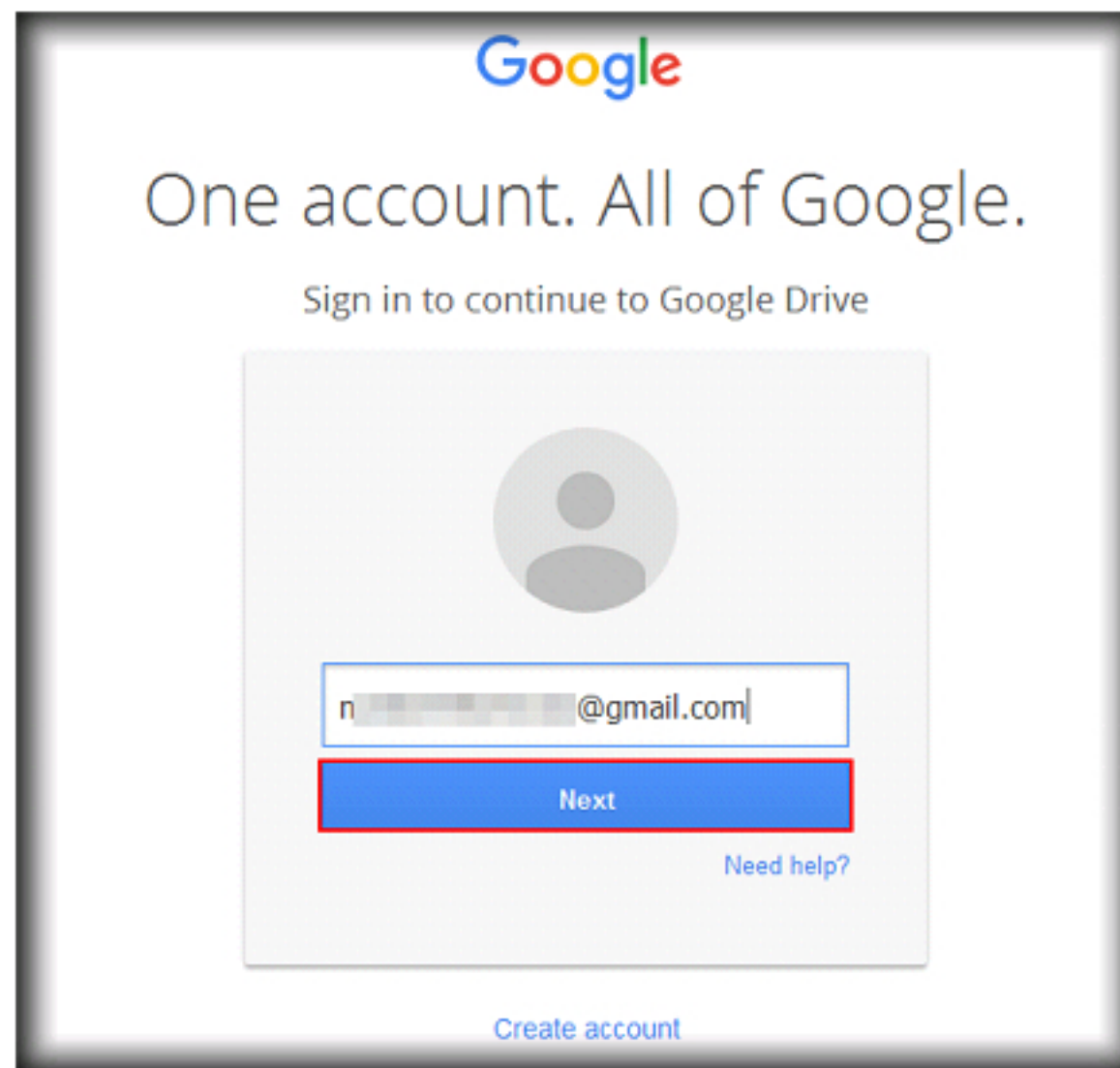


FIGURE 2.29: Entering email address of the Google Drive Account

36. Enter password for the account and click the **Sign In** button.

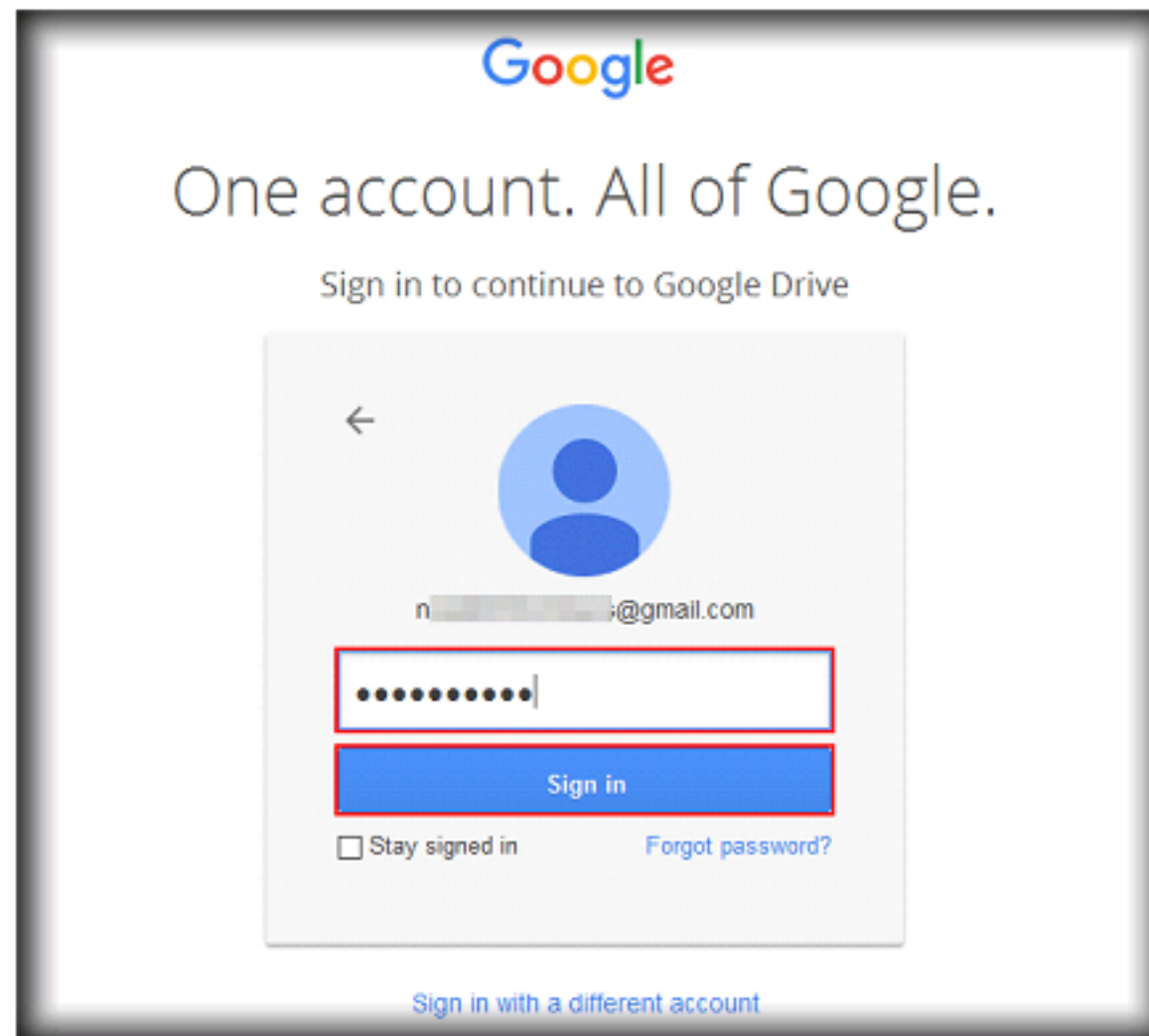


FIGURE 2.30: Entering password of the respective Google Drive Account

37. The browser access of a Google Drive account will help you to search for deleted files, check and manage versions of a file, view recent activity, as well as review details and activity of any file present.
38. On the homepage of a Google Drive account, click **Trash** in the left pane to view the deleted files. The page will navigate to the Trash section, you can right click any image to see options such as **Restore** and **Delete Forever**.

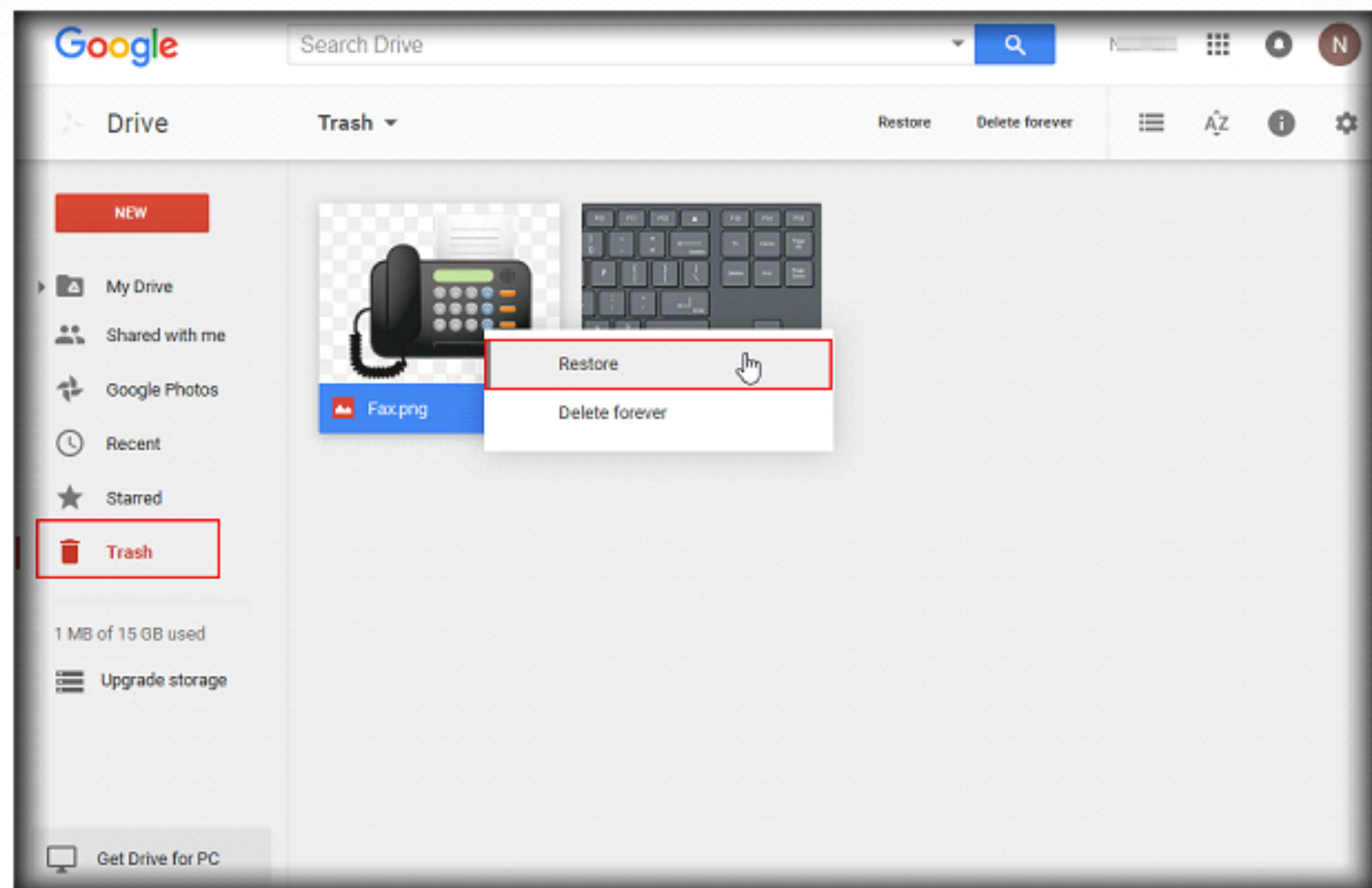


FIGURE 2.31: Viewing the Trash section in the Google Drive account

39. In the **My Drive** section, right click any image to get options and click **Manage versions...** option to see its versions.

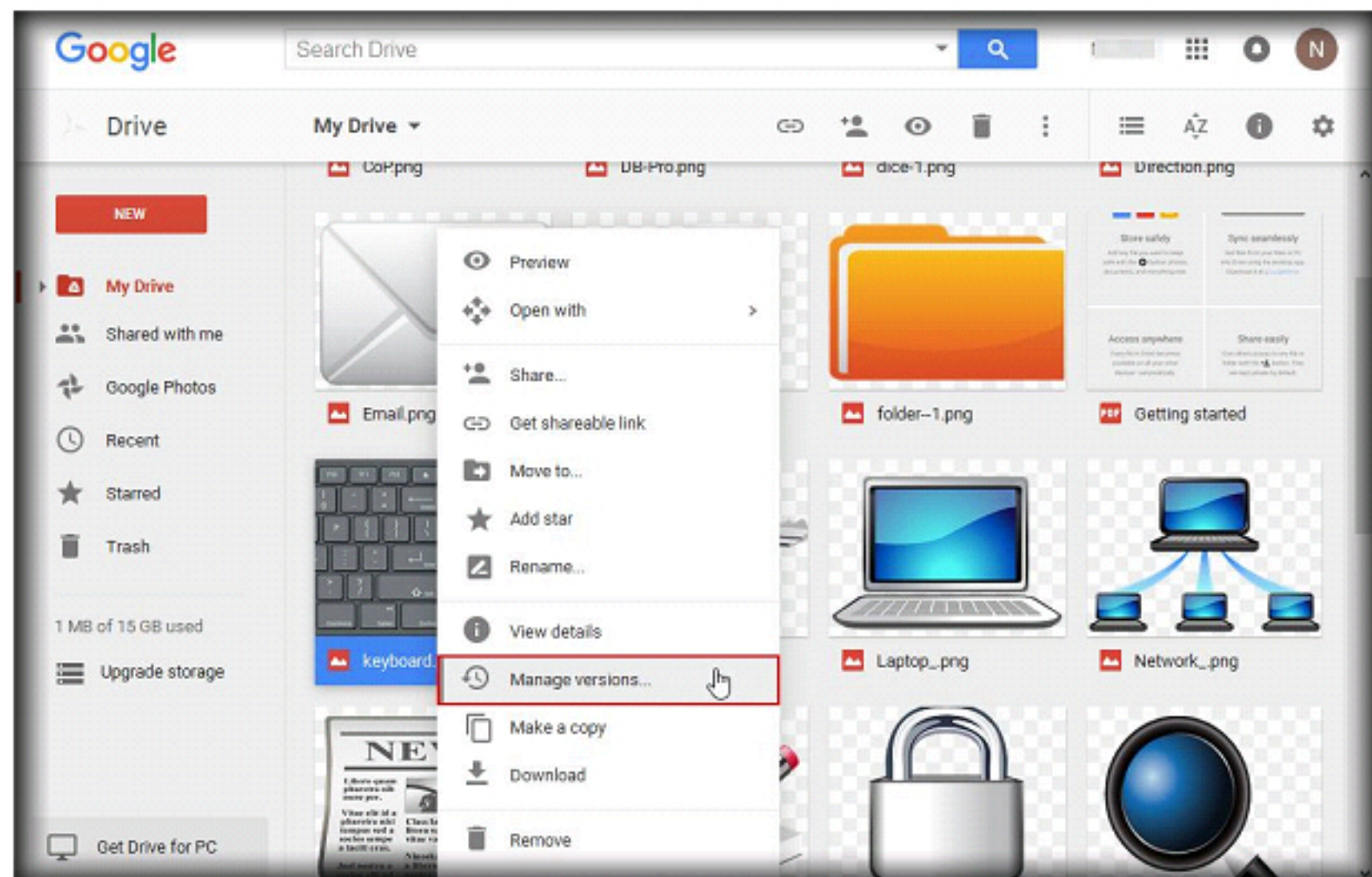


FIGURE 2.32: My Drive section

40. In the **Manage Versions** dialog box, you can click the **Ellipsis** (⋮) button related to a file from the extreme right to download the file.

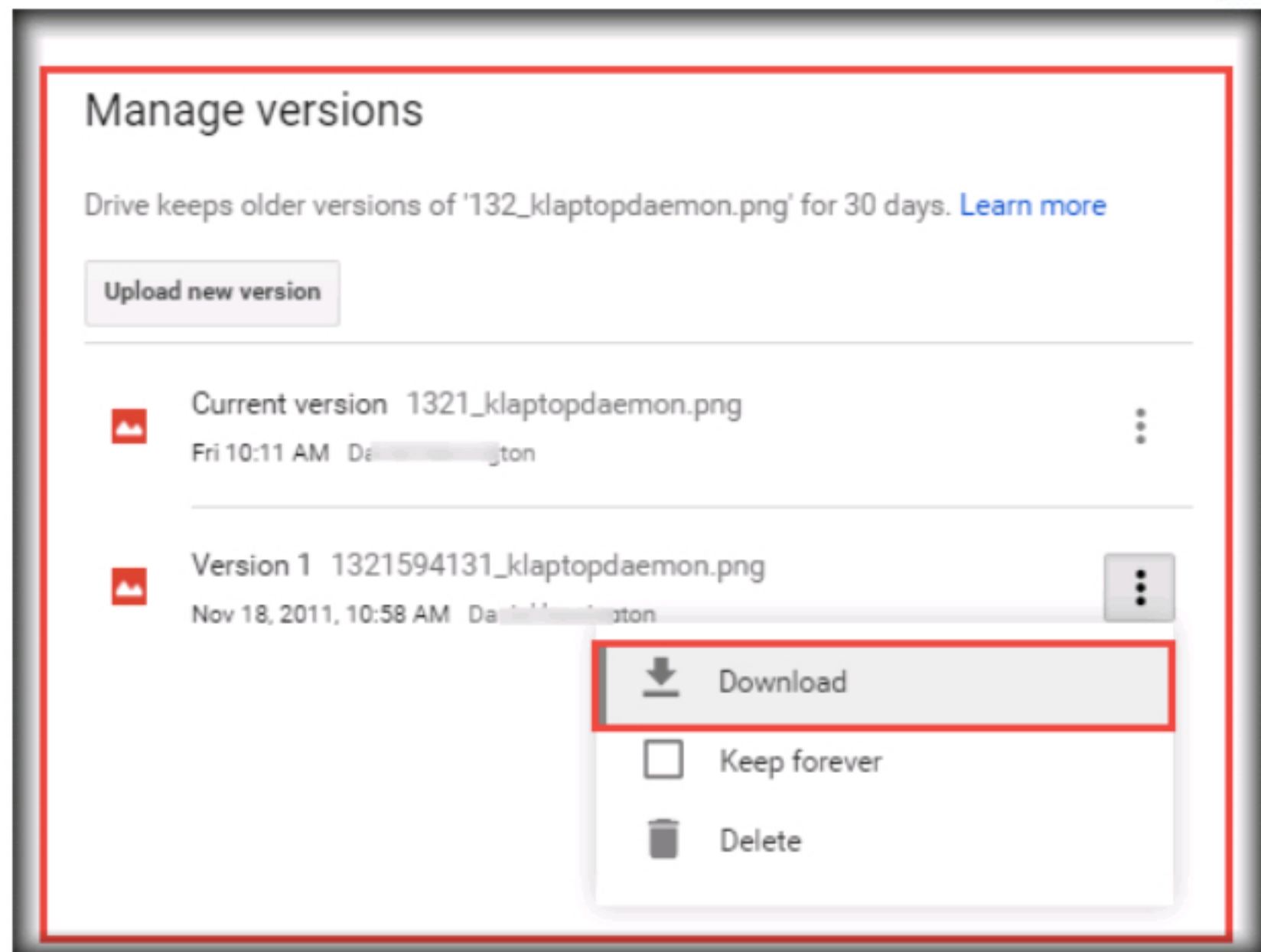


FIGURE 2.33: Manage Versions dialog box

41. To view the details of any file, select the file and click the information icon from the menu bar. Click **Details** tab to view details of the file.

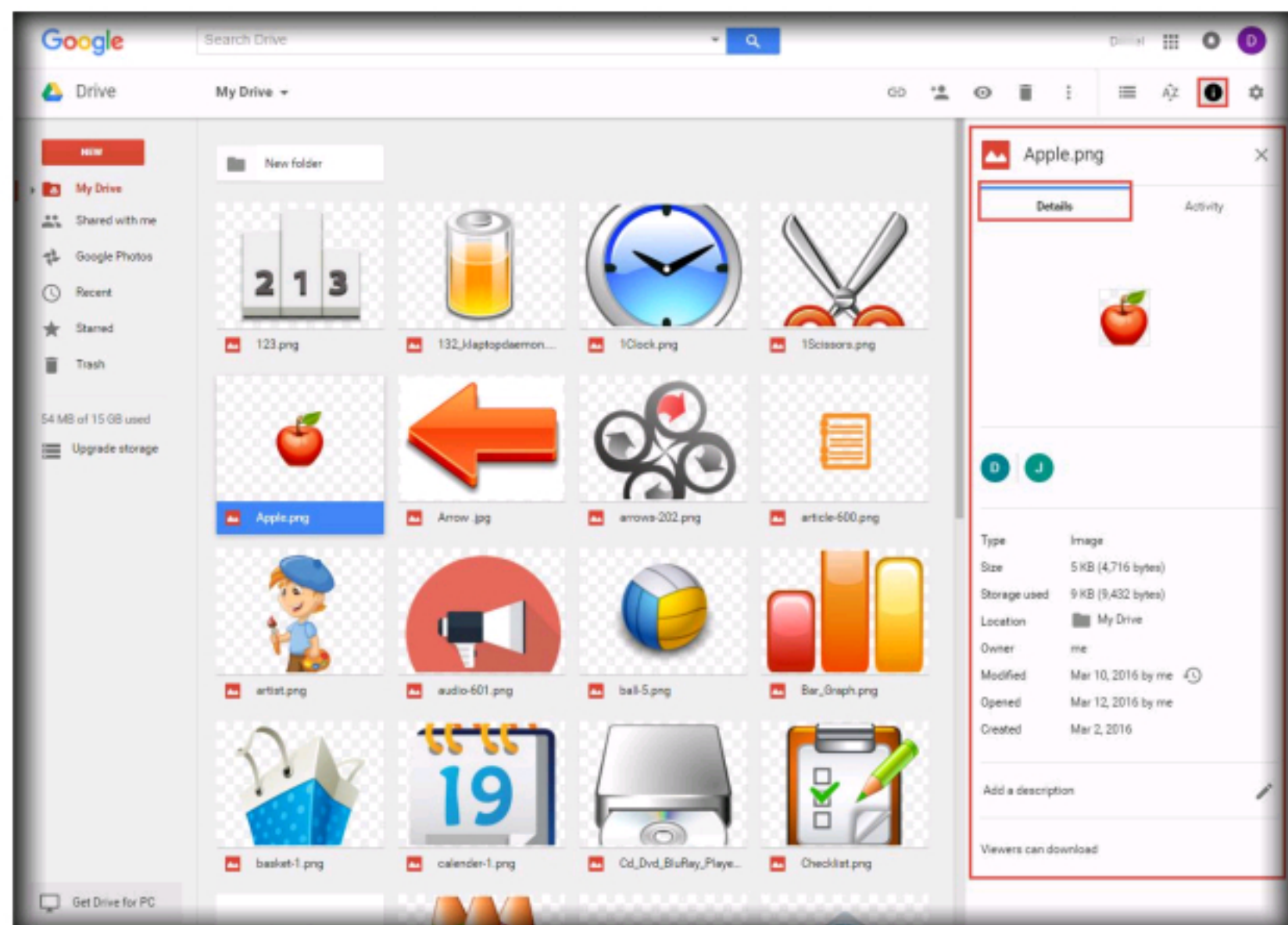


FIGURE 2.34: Viewing details of a file

42. Click the **Activity** tab to view all the activities related to a particular file.

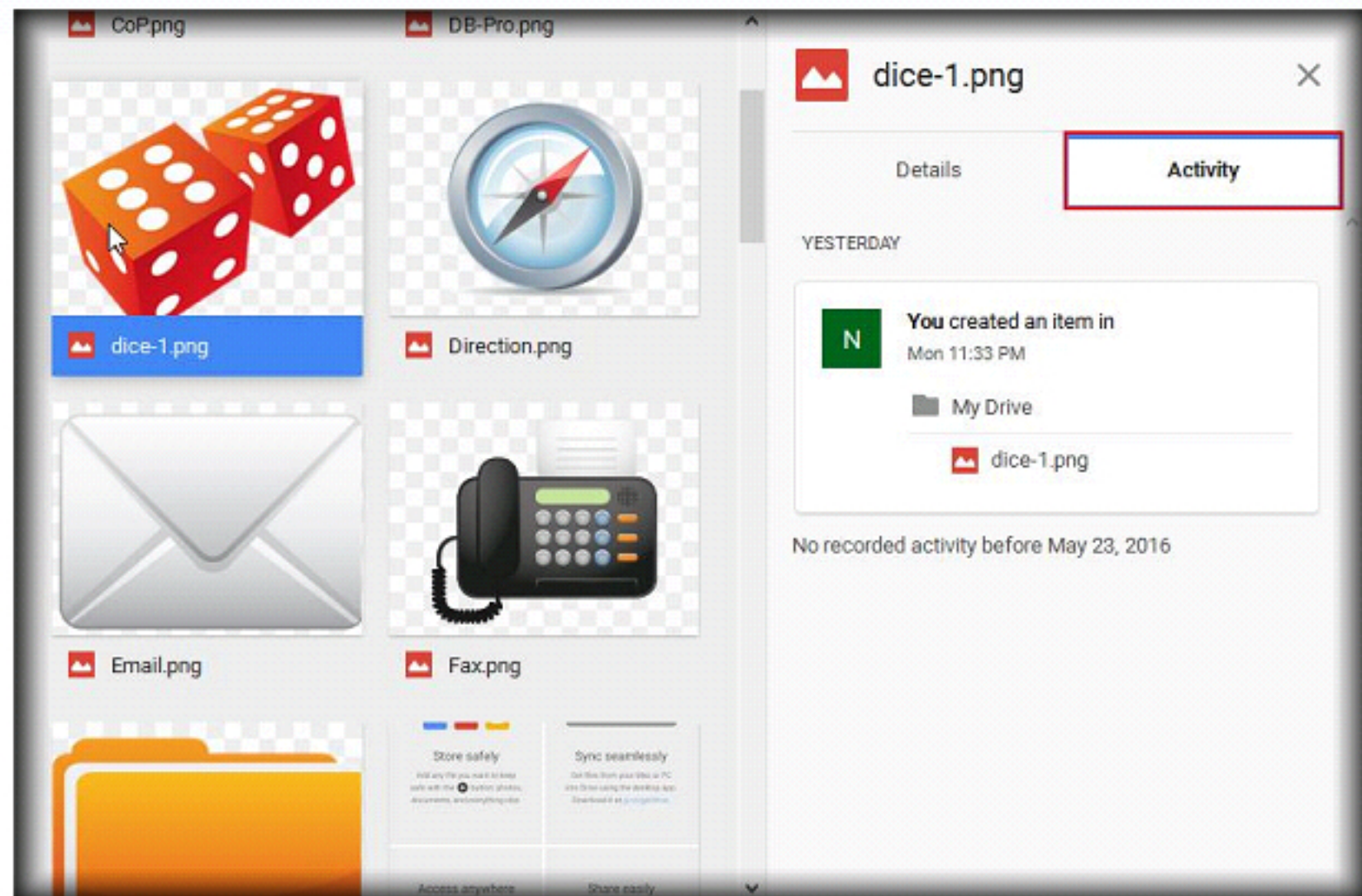


FIGURE 2.35: Screenshot showing Activity tab

43. Click the **Recent** in the left pane to see recently accessed files.

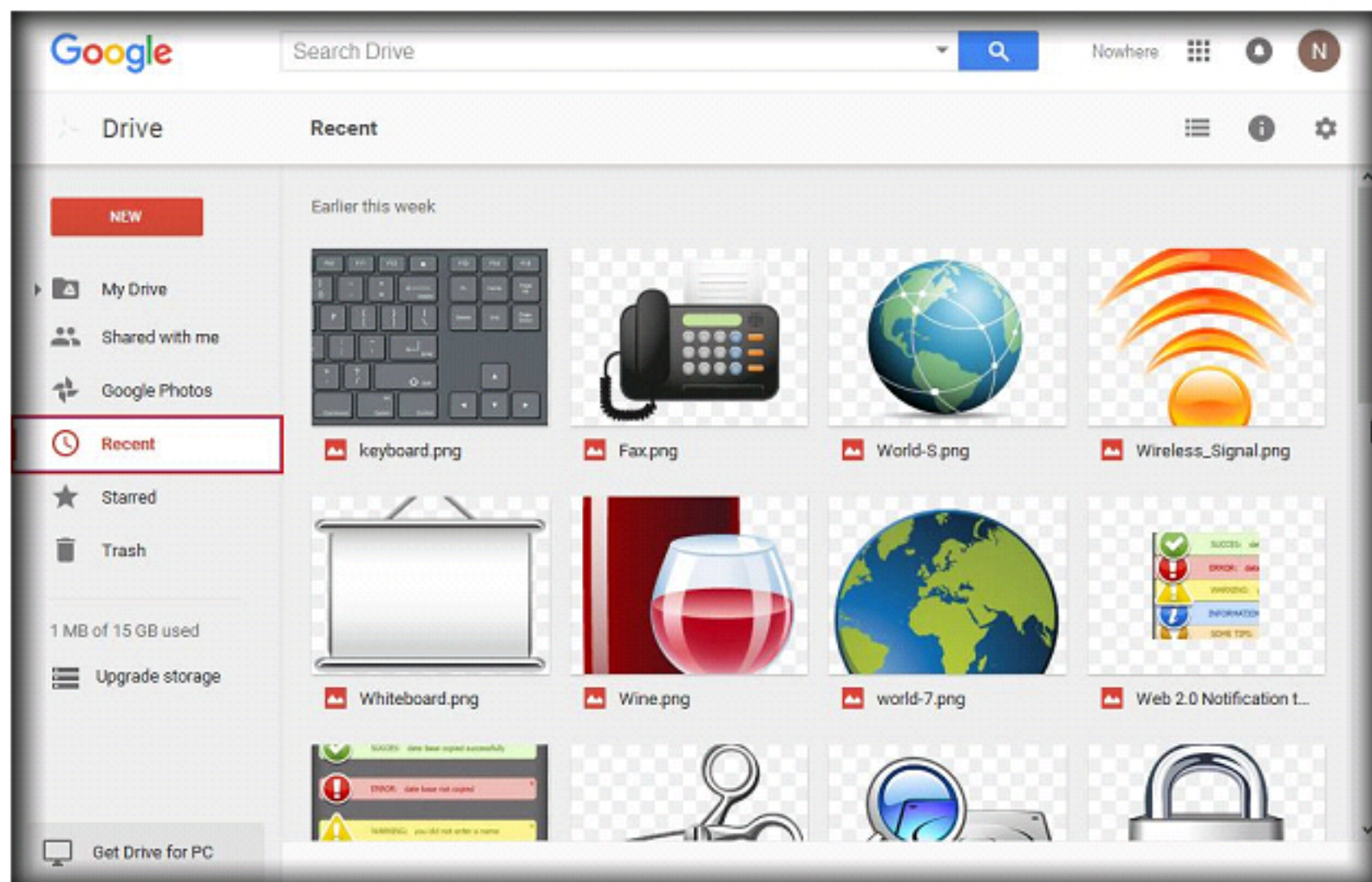


FIGURE 2.36: Viewing the Recent section in the Google Drive account

44. Now run the RAM Capturer tool. To run the tool, navigate to the location **Z:\CHFIv9 Module 10 Cloud Forensics\RAM Capturer** and double-click **RamCapture64.exe**. RamCapture window appears, click the **Capture** button.

Note: If Ram Capturer displays an error while launching, copy the RAM Capturer folder located at **Z:\CHFIv9 Module 10 Cloud Forensics** to desktop and try running the tool.

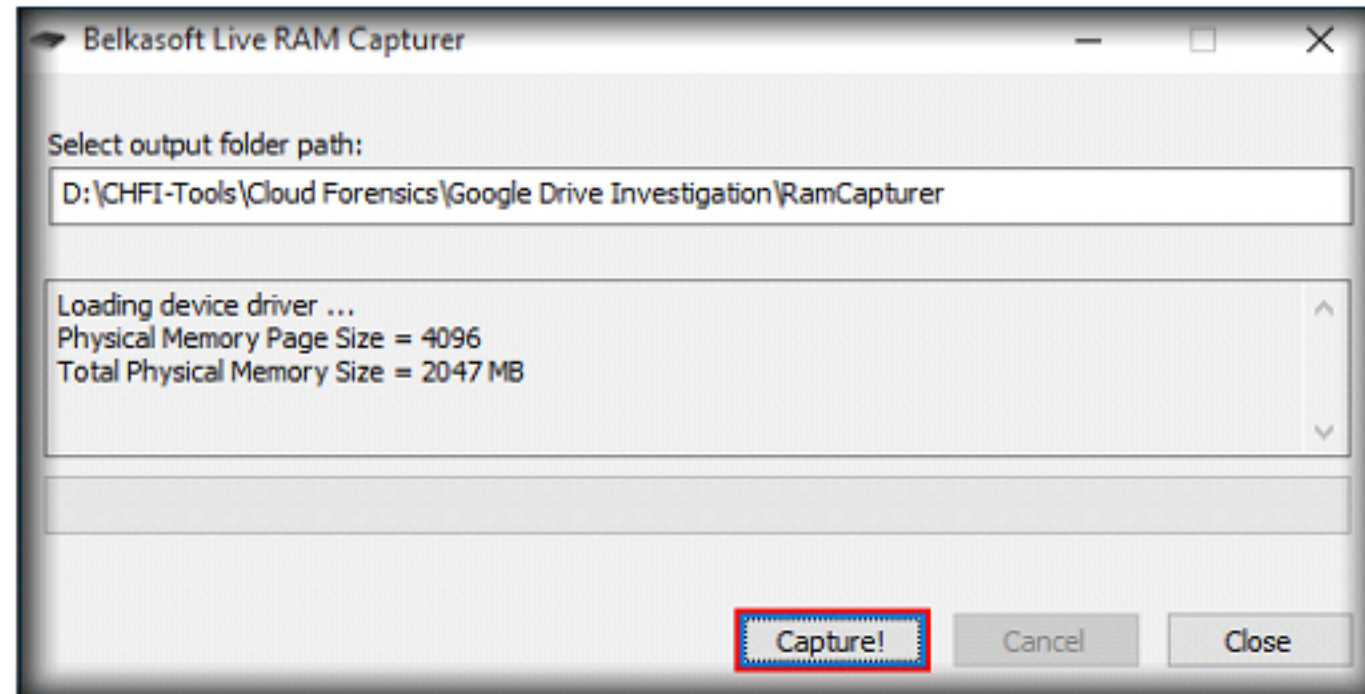


FIGURE 2.37: RAM Capturer tool

45. Once the tool completes the process, click the **Close** button

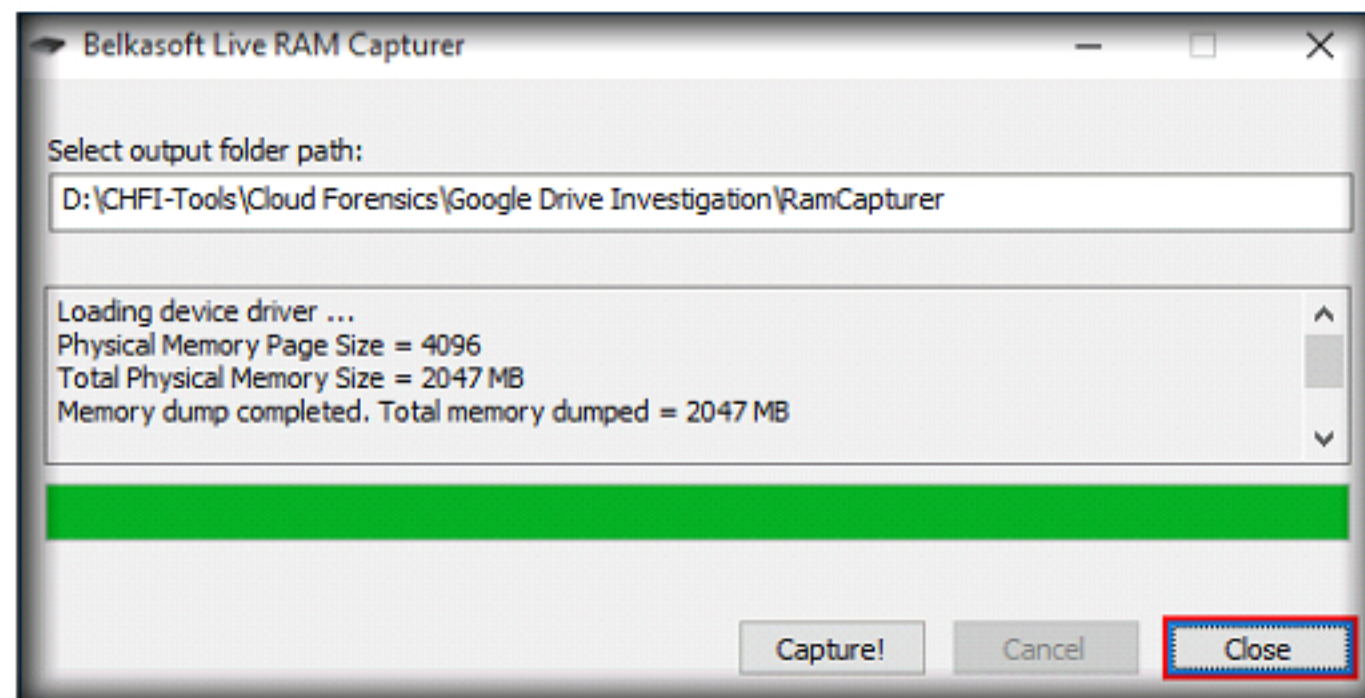


FIGURE 2.38: RAM Capturer tool

46. Run the **HxD** tool to view the Hex value of capture RAM data. Click the **Open** icon to add a file.

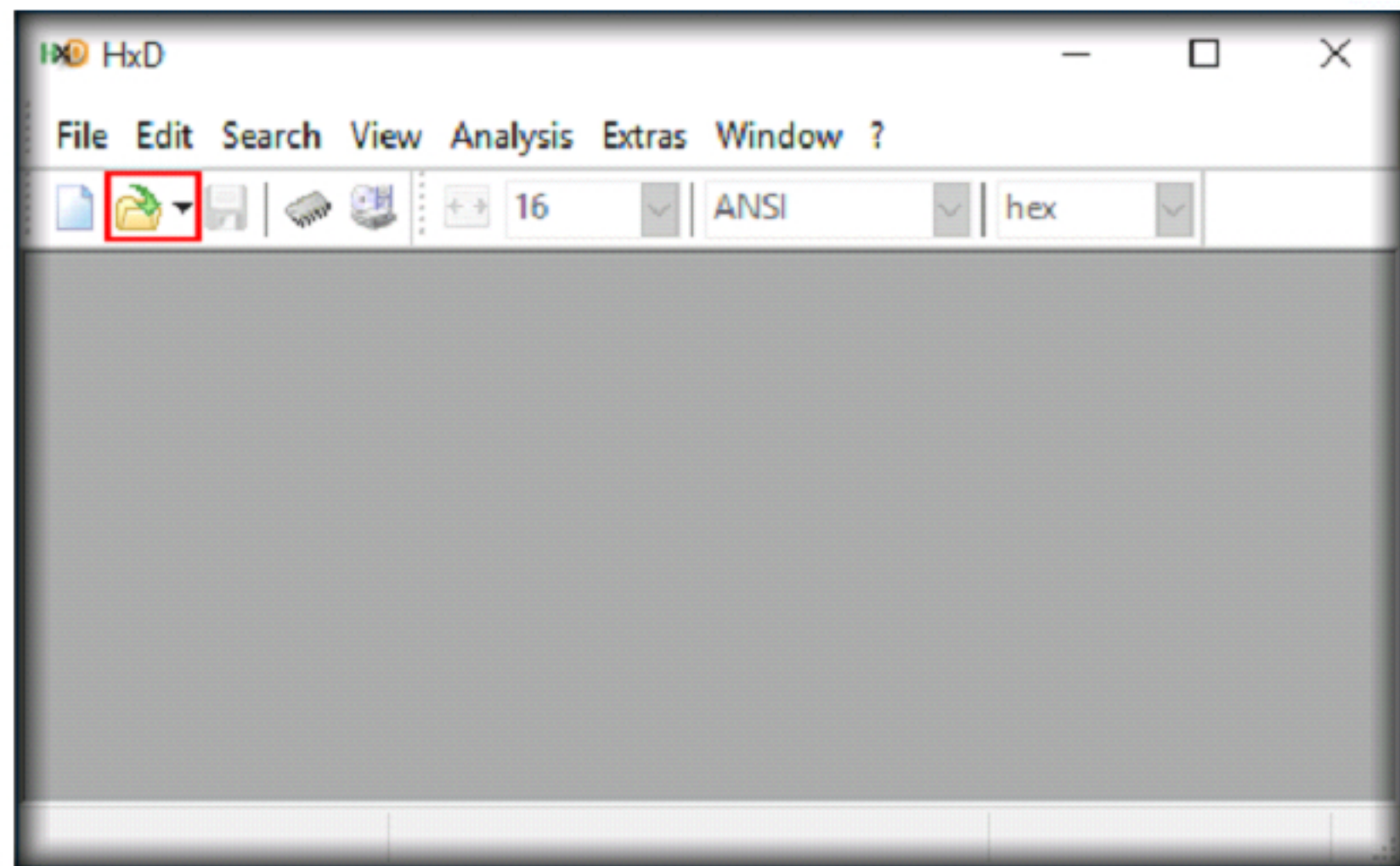


FIGURE 2.39: HxD tool main window

47. Navigate to the **Z:\CHFIV9 Module 10 Cloud Forensics\RAM Capturer** folder, select the captured RAM data file, and click **Open**.

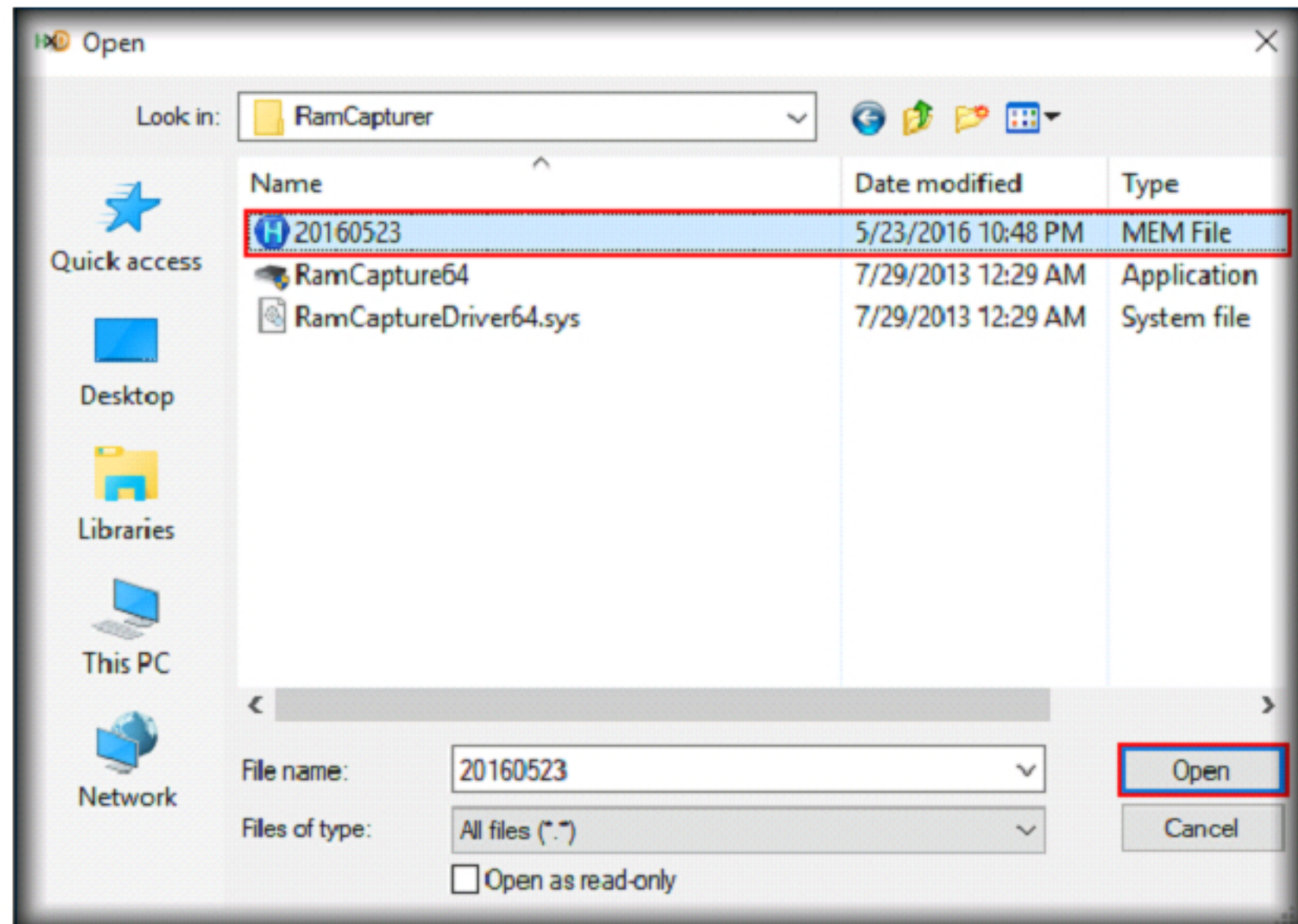


FIGURE 2.40: Opening the captured RAM data file

48. Now analyze the hex data using **Find** function and keywords such as `user_email`, `version number`, `local_sync_folder_path`, `snapshot.db`, and `sync_config.db`.
49. Press **ctrl+f** to activate **Find**, provide the keyword, and click the **OK** button to search across the hex data.

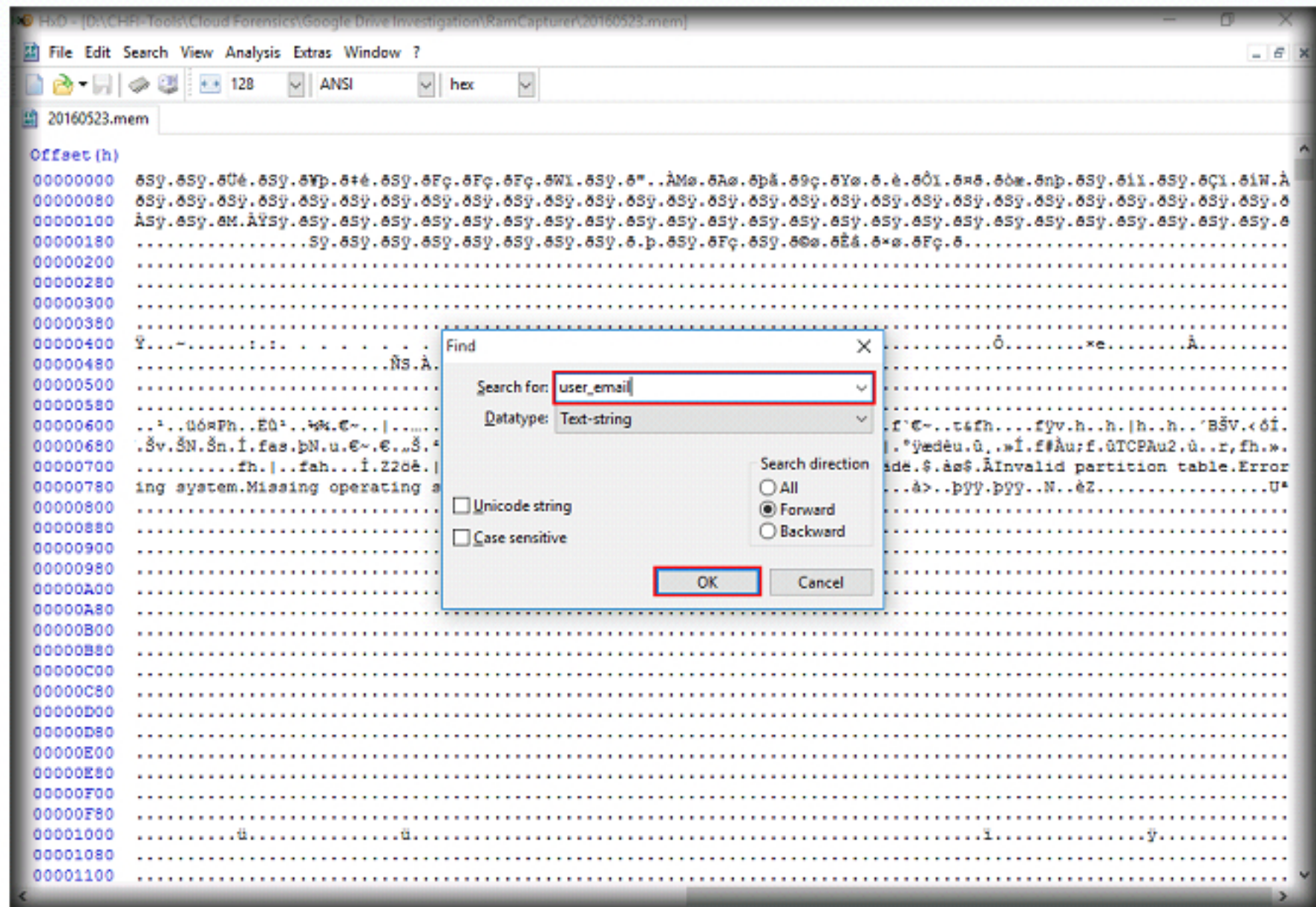


FIGURE 2.41: Screenshot showing Find function

50. The tool will display data with searched string that would be having the email of the Google drive account.

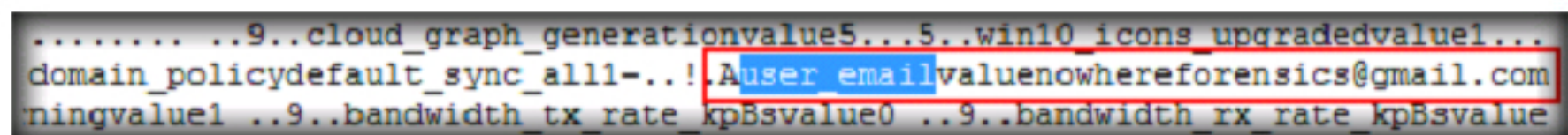


FIGURE 2.42: Screenshot displaying the searched string

51. Similarly search for other keywords. You can find the password of the account by searching for password-related keywords such as passwd, password, etc.

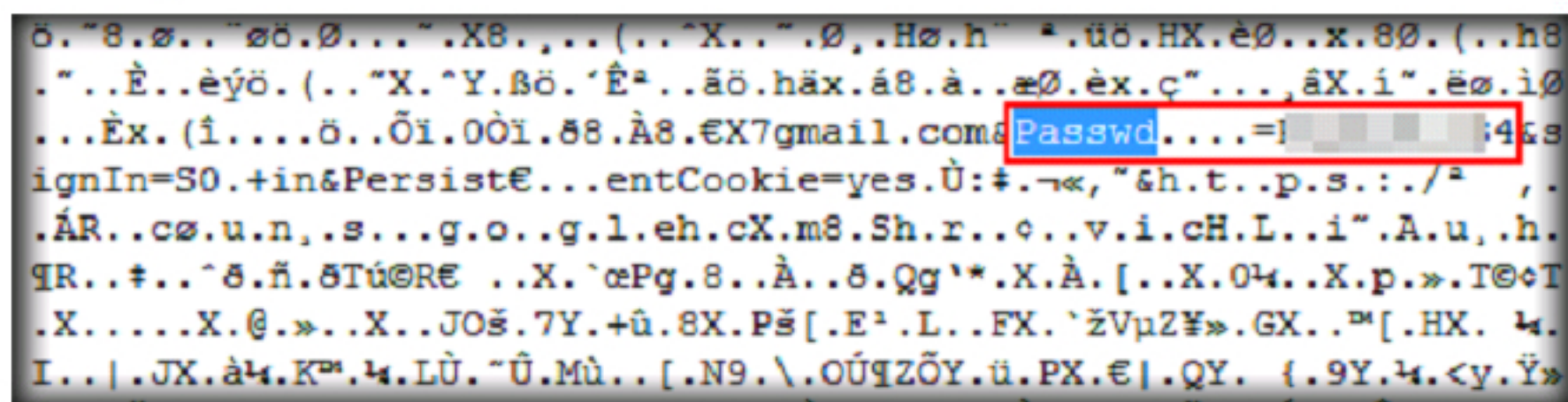


FIGURE 2.43: Screenshot displaying the searched string

52. Run the **WebBrowserPassView** tool from **Z:\CHFIv9 Module 10 Cloud Forensics\Google Drive Investigation Tools** to view the passwords when a user accesses the Google Drive account through a browser.

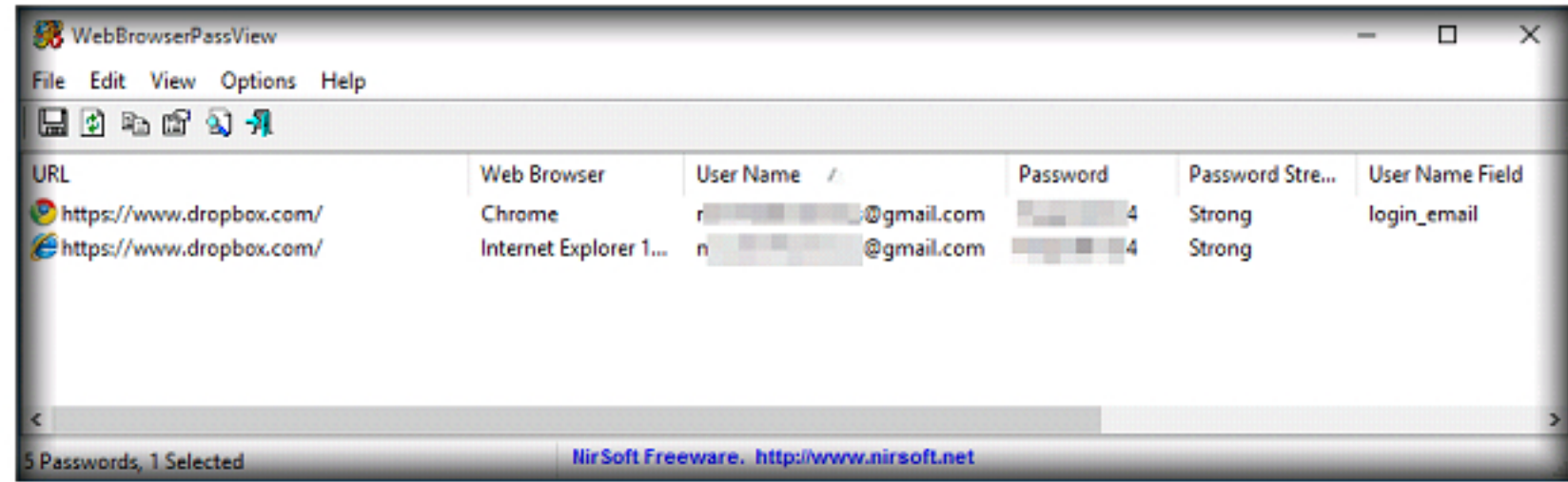


FIGURE 2.44: WebBrowserPassView tool

53. Run the **Disk Pulse** and **WhatChanged** tools similar to the steps above. Start the monitoring process and capture the first system snapshot.
54. Uninstall the Google Drive client to observe the artifacts it leaves behind that could help in investigation of an attack.
55. Go to **Control Panel** → Click the **Uninstall a Program** → Select **Google Drive** from the list of Programs and Features and click the **Uninstall** button.
56. Click **Yes** if the system prompts a dialog box for confirming uninstalling process.

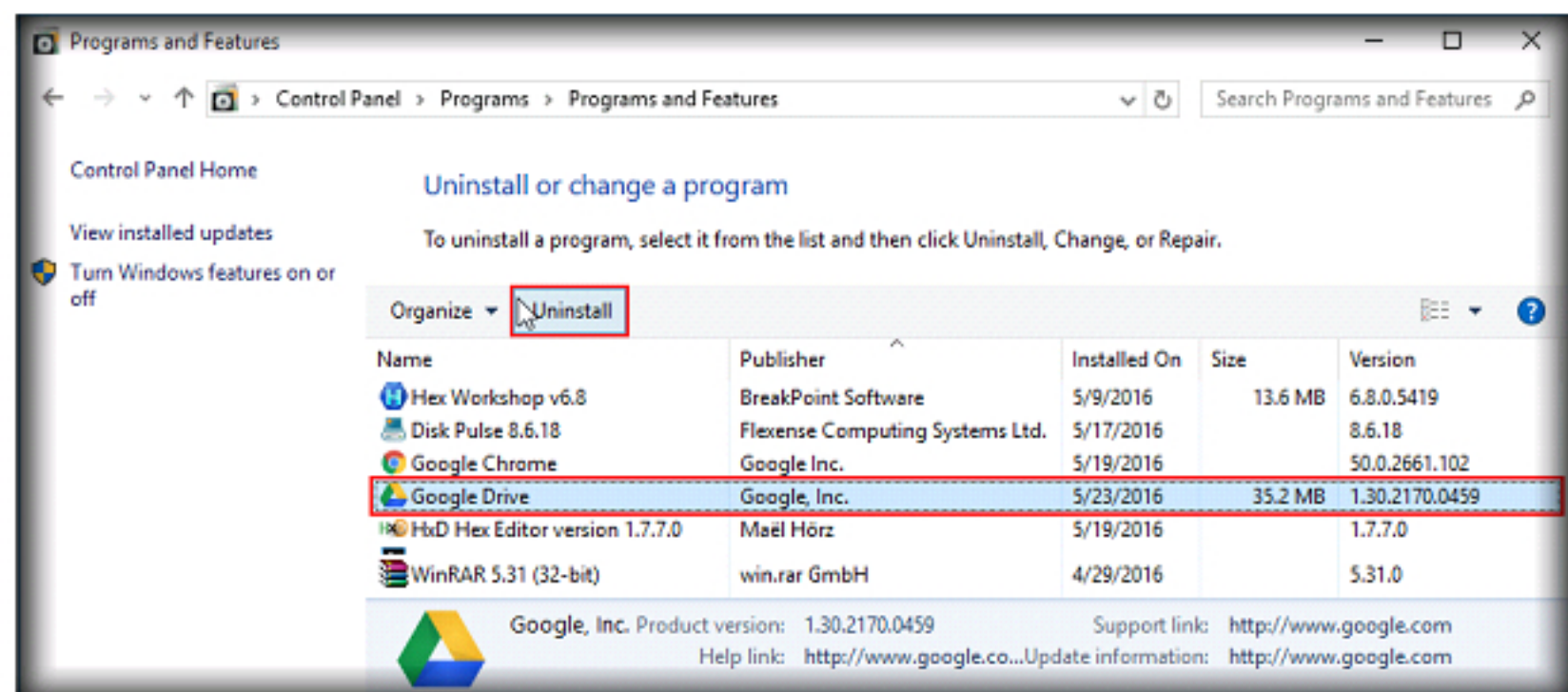


FIGURE 2.45: Uninstalling Google Drive application

57. After uninstalling the **Google Drive** client from the system, go to the **Disk Pulse** tool and stop the process. Click the **Save** button to save the report.

58. The report will contain the list of all the files modified during the uninstallation process.

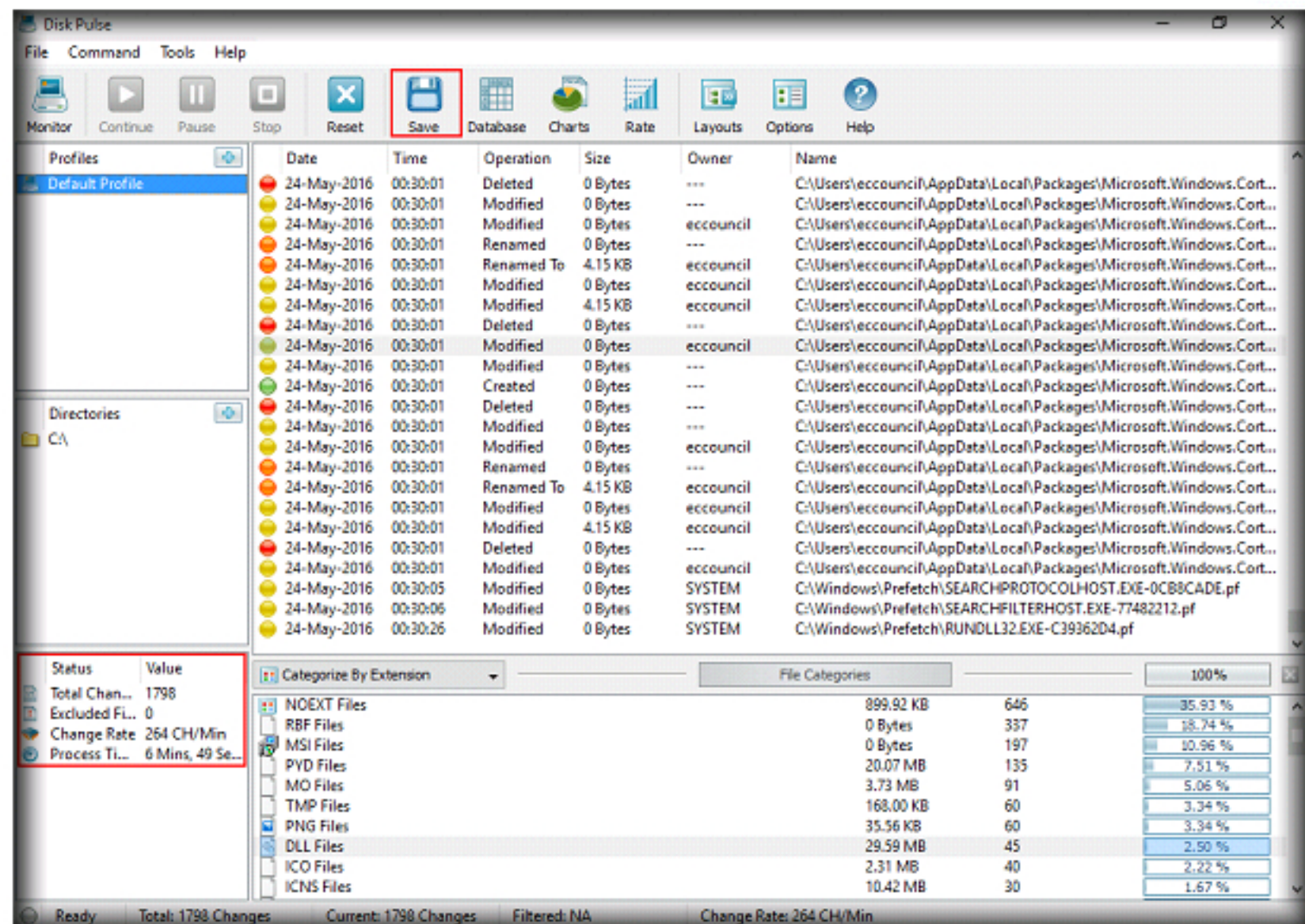


FIGURE 2.46: Recording the changes during the uninstallation process in Disk Pulse tool

59. Take the second snapshot of the **WhatChanged** tool. The tool displays that it has listed six changes in the selected registry of the system during uninstalling process.

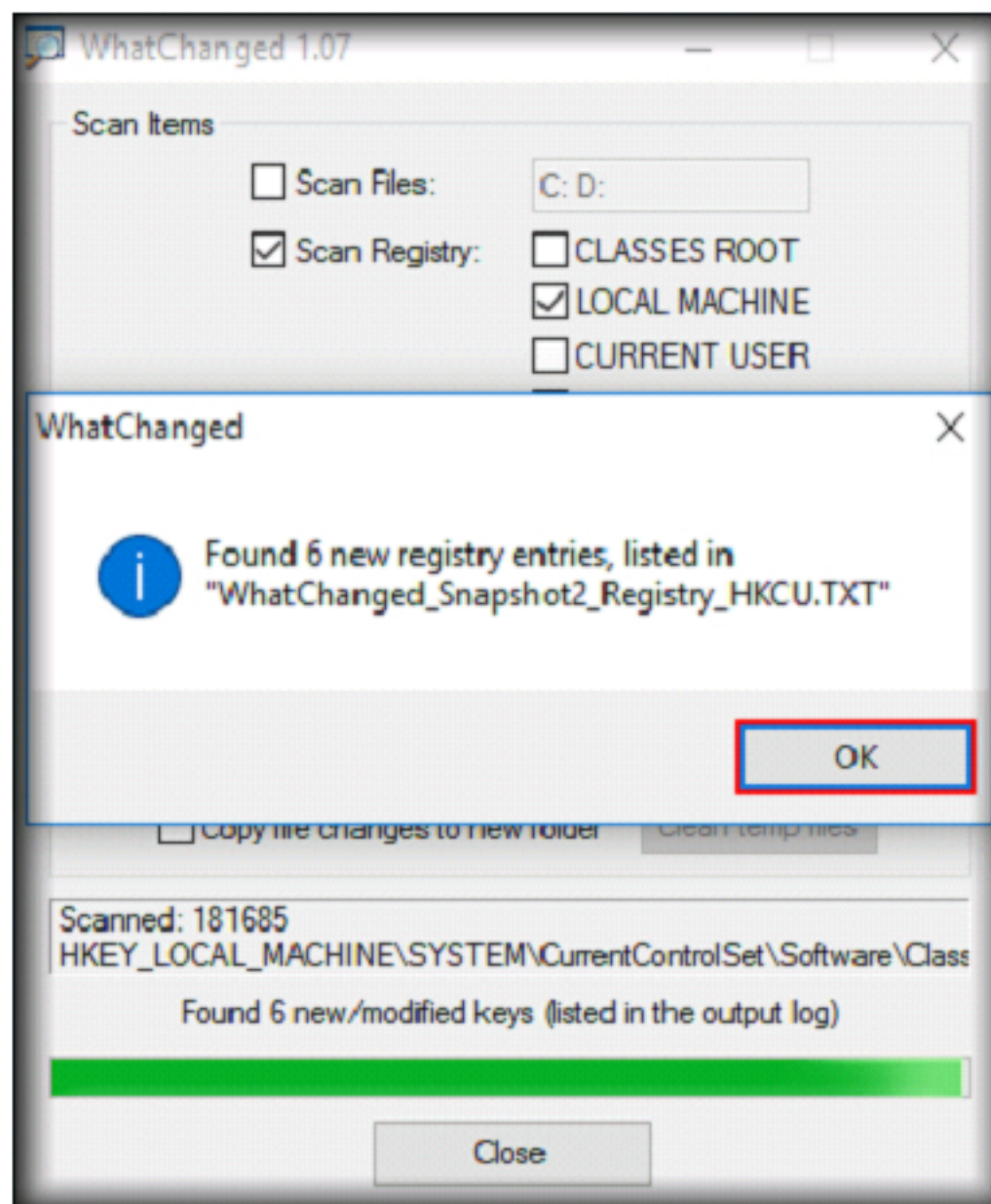


FIGURE 2.47: WhatChanged tool displaying the resultant changes after comparison

60. The tool gives output in the form of a text file, including addresses of all the modified files and folders.

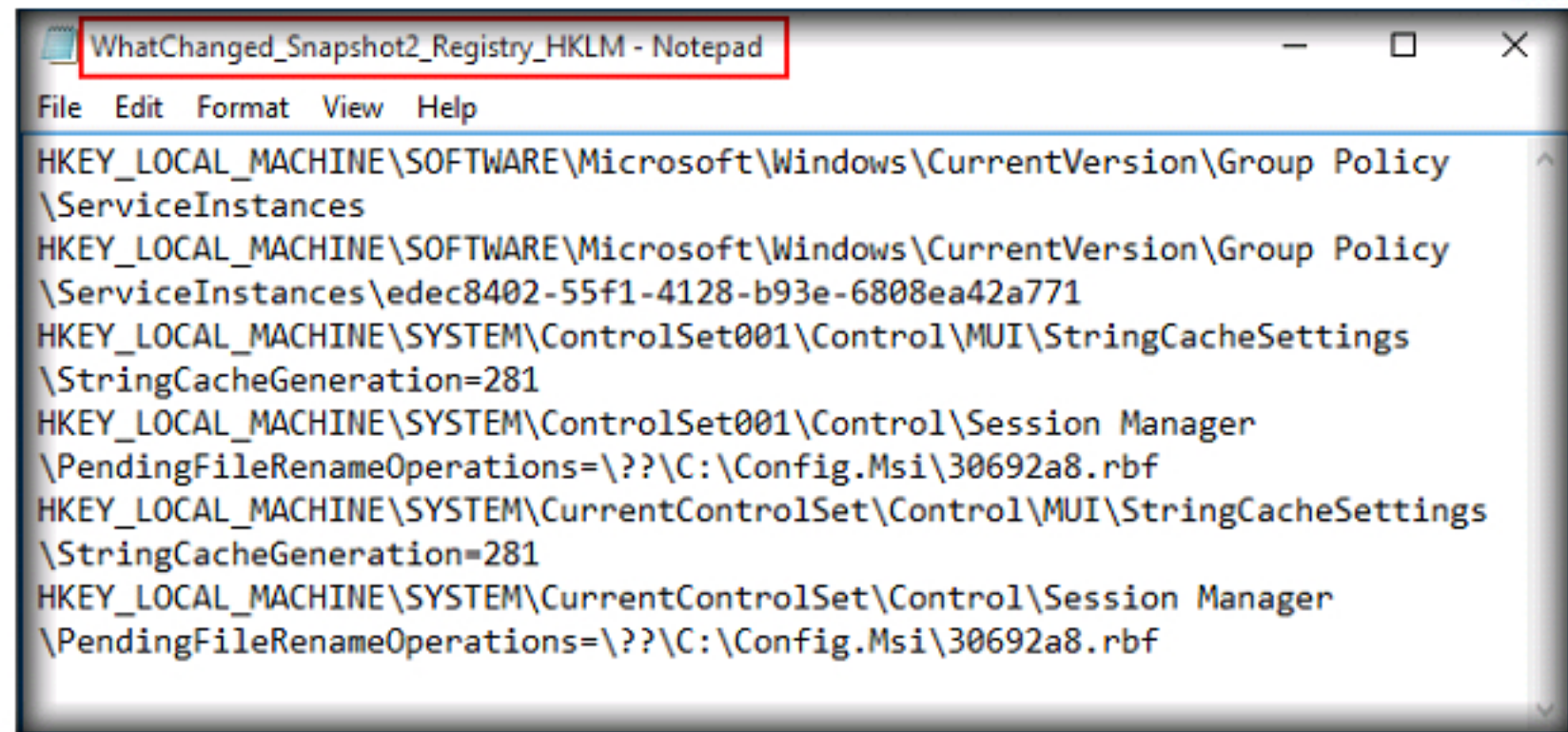


FIGURE 2.48: Notepad file showing the occurred changes

61. Uninstalling the client will result in
- Deletion of the client config folder (sync_config.db)
 - Preservation of a local copy of the file as well as the Prefetch files
62. Other files that can help you in recovering traces or evidences of the cloud storage service include
- Registry keys about recent files
 - LNK files
 - Browser history and cache
 - Thumbnails
 - Restore points/ Volume Shadow Copies
 - Pagefile.sys
 - Hiberfil.sys

63. Screenshot displaying the Drive folder present in the Google's Program Files directory before uninstalling the client:

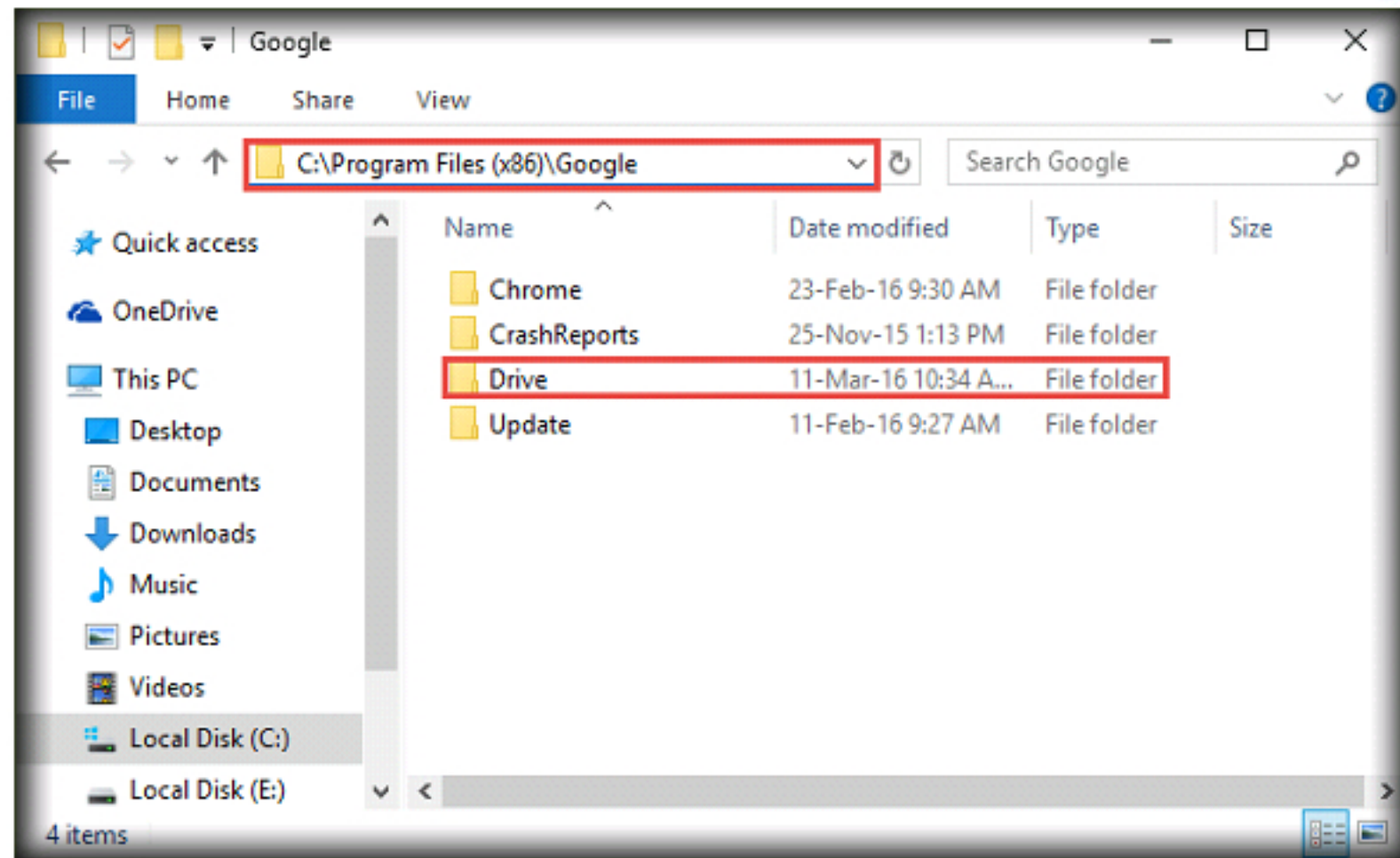


FIGURE 2.49: Screenshot of the Google folder before uninstallation

64. Screenshot displaying Google's Program Files directory (Drive folder disappears) after uninstalling the client:

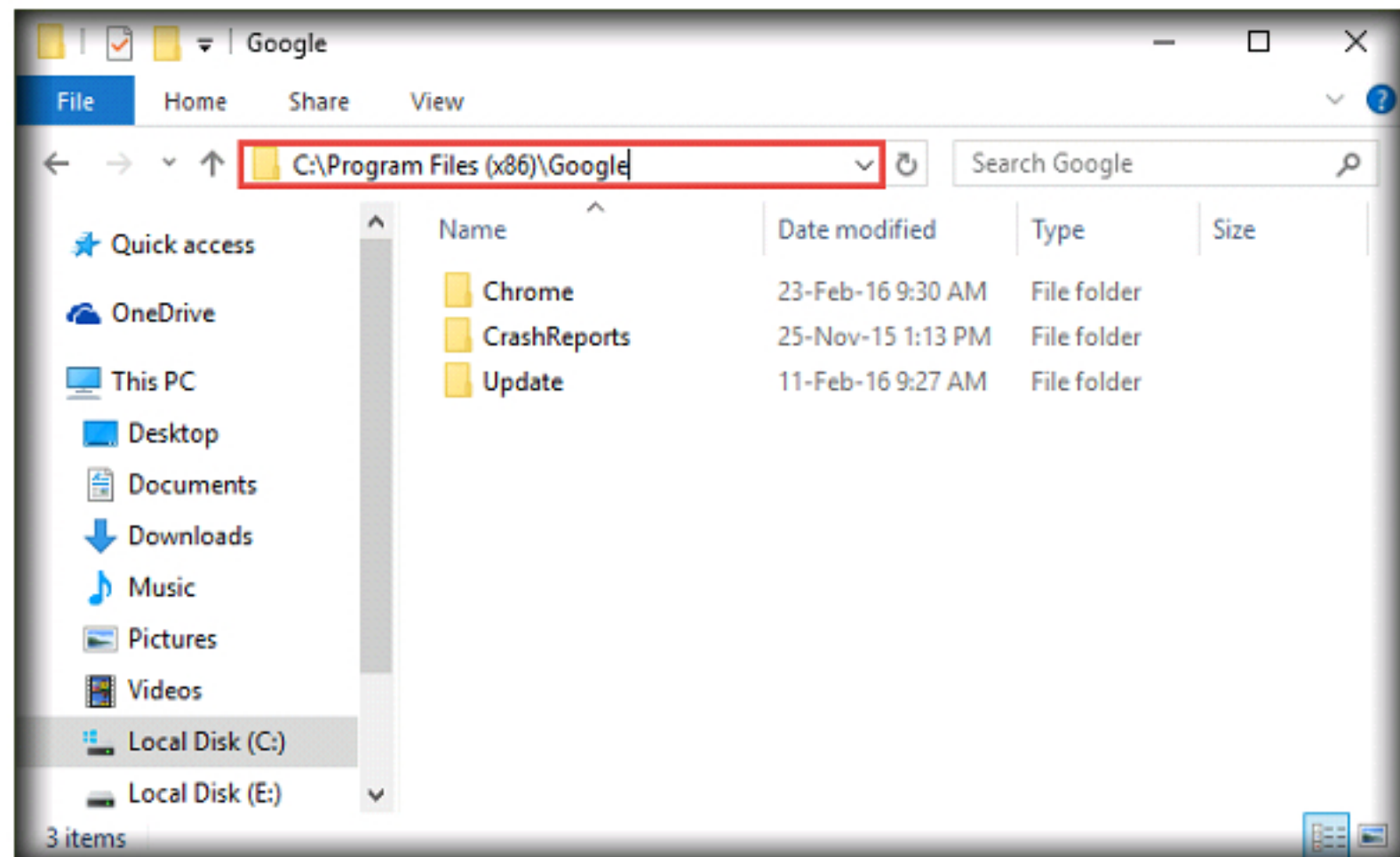


FIGURE 2.50: Screenshot of the Google folder after uninstallation

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.

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