

Security Analysis, Techniques and procedures

Lab 8a

Wales Institute of Science and Art
Applied Computing
I.Q Building, Room 205
Swansea
SA1 8EW

Introduction

The Computer Forensics investigation is a methodological approach of preparing for an investigation, collecting and analyzing digital evidence. It is also managing the case from the reporting of the crime till the case's conclusion. The process takes place in a computer forensic lab.

Computer forensics plays a vital role in the investigation and prosecution of cyber criminals. The process includes acquisition, inspection, and reporting of information stored across computers and networks related to a civil or criminal incident. Forensic investigators are trained professionals who can extract, analyze, report, and investigate cases that involve technology as the source or the victim of a crime.

As a computer forensics investigator, it is important to have knowledge of the process involved during a forensics investigation, such as collecting digital evidence, building a computer forensics lab, recovering the deleted data, etc.

Task 1:

- Sign in **www.tryhackme.com**
- Go to Hacktivities → select free only from the **show** pop down list → walkthrough from the **Type** pop down list.
- Select **Forensics** and attempt a lab of your choice. Each week try to complete a different one.

Task 2: Forensics 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.

Overview of Dropbox Investigation

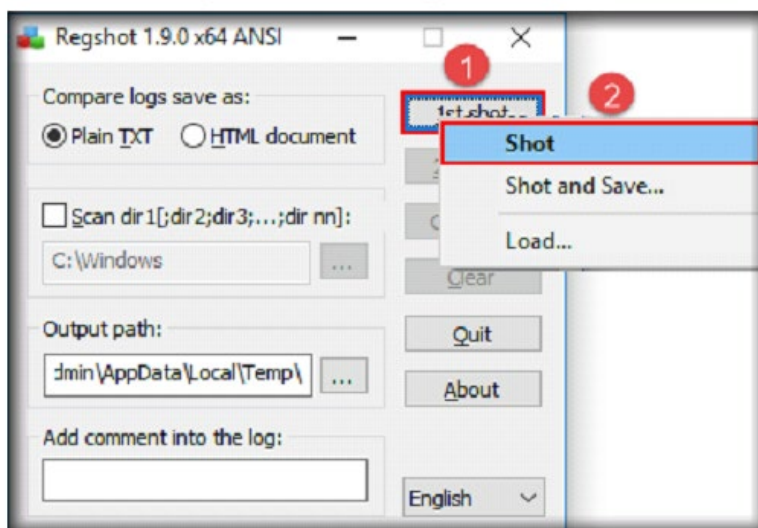
The process includes searching of system files, registries, history, and cache folders to find the traces of Dropbox and use them as evidence to proceed.

Lab Tasks

1. Before beginning this lab, log in to **windows 10** virtual machine and install WhatChanged, Disk Pulse, Directory Monitor, RAM Capturer, HxD, and WebBrowserPass View tools from the location: https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308
2. The regshot tools 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 https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308 for Regshot tool 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**.

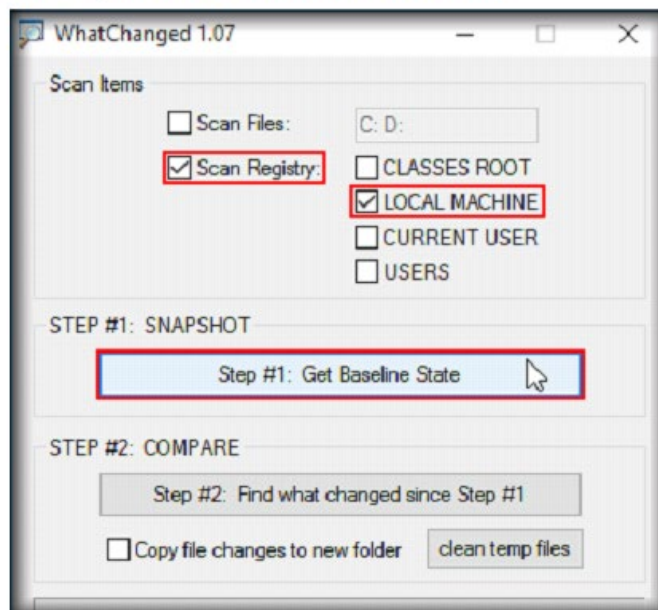
4. To capture the snapshot of the system, click the **1st shot** button and select the **Shot** option from the drop-down list.



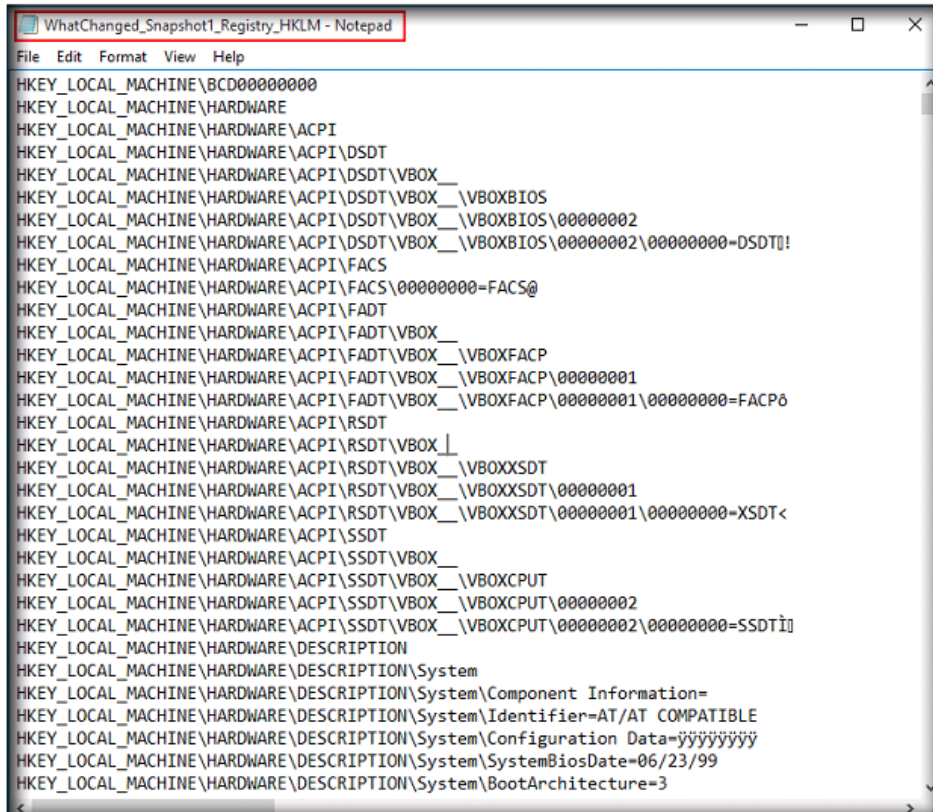
5. After taking the snapshot, investigator needs to find the files that change when an user installs a cloud application.
6. Navigate to https://uwotds-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwotds_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308 for WhatChanges Portable, and double-click WhatChangedPortable.exe to launch the application.

WhatChanged GUI appears; check the **Scan Registry** and **LOCAL MACHINE** options from **Scan Items**.

7. Click the **Step #1: Get Baseline State** button.

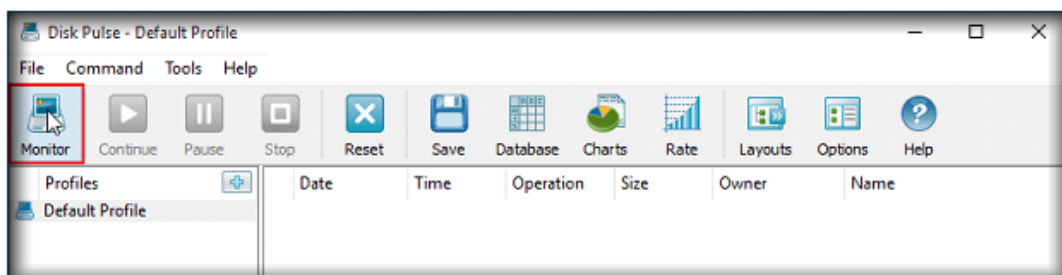


8. The tool will also generate a notepad file with the name **WhatChanged_Snapshot1_Registry_HKLM** in same folder as the location of the executable. The notepad contains all the local machine addresses.

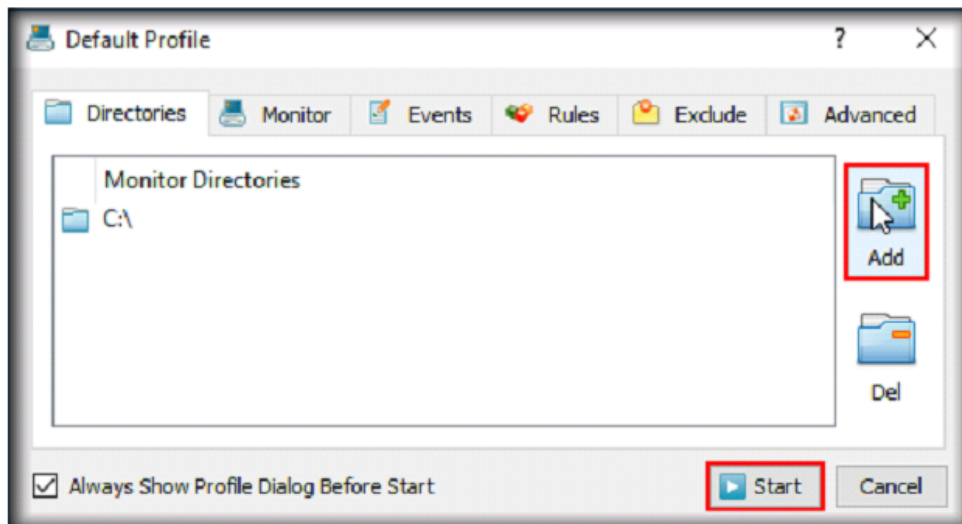


9. Navigate to https://uwotds-my.sharepoint.com/:f/g/personal/carlene_campbell_uwotds_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308 for Disk Pulse, double diskpulse_setup_v8.7.26.exe and follow the wizard driven installation steps to install the application. At the final step of installation, 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.



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.

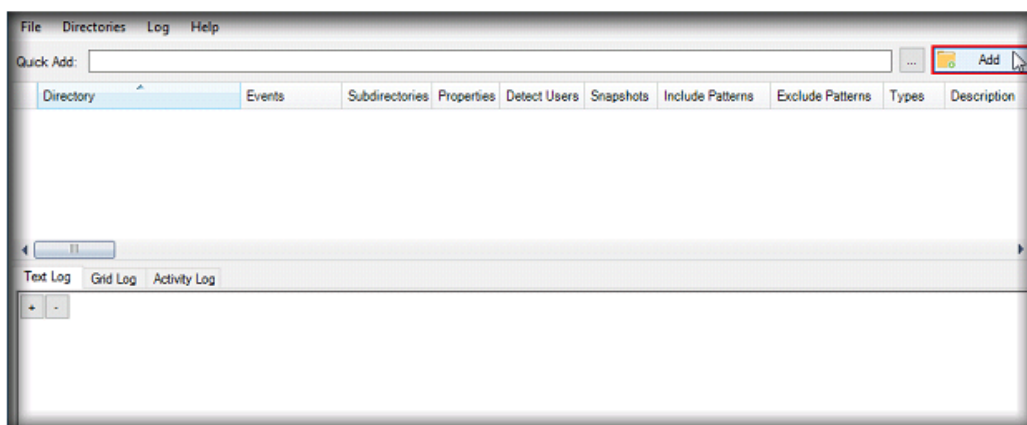


13. The investigator should observe the changes and application makes to the directories in the local system folder.

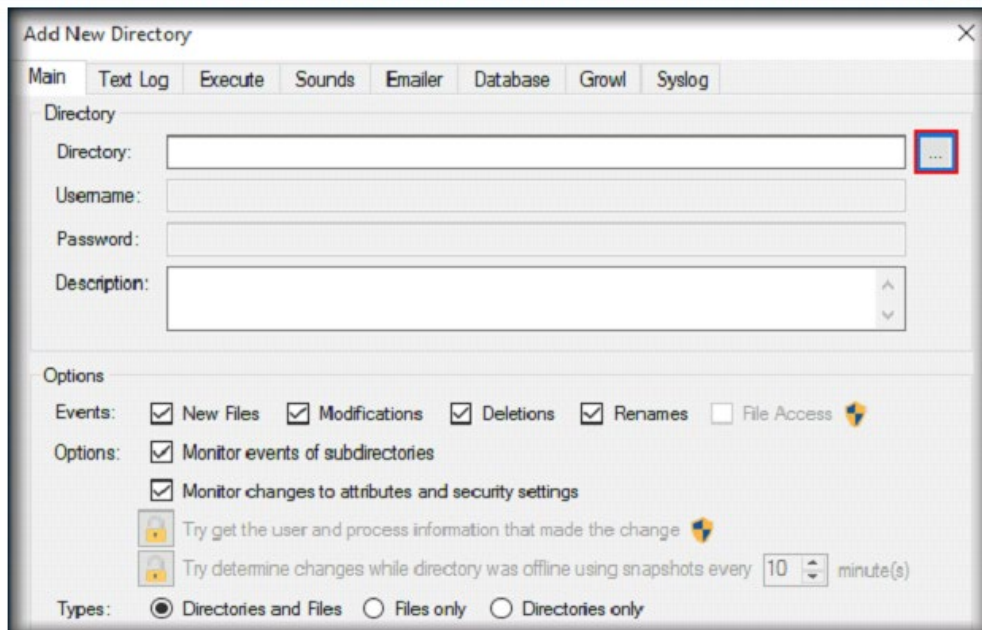
14. Navigate to https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308 for Directory Monitor, double-click

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**.

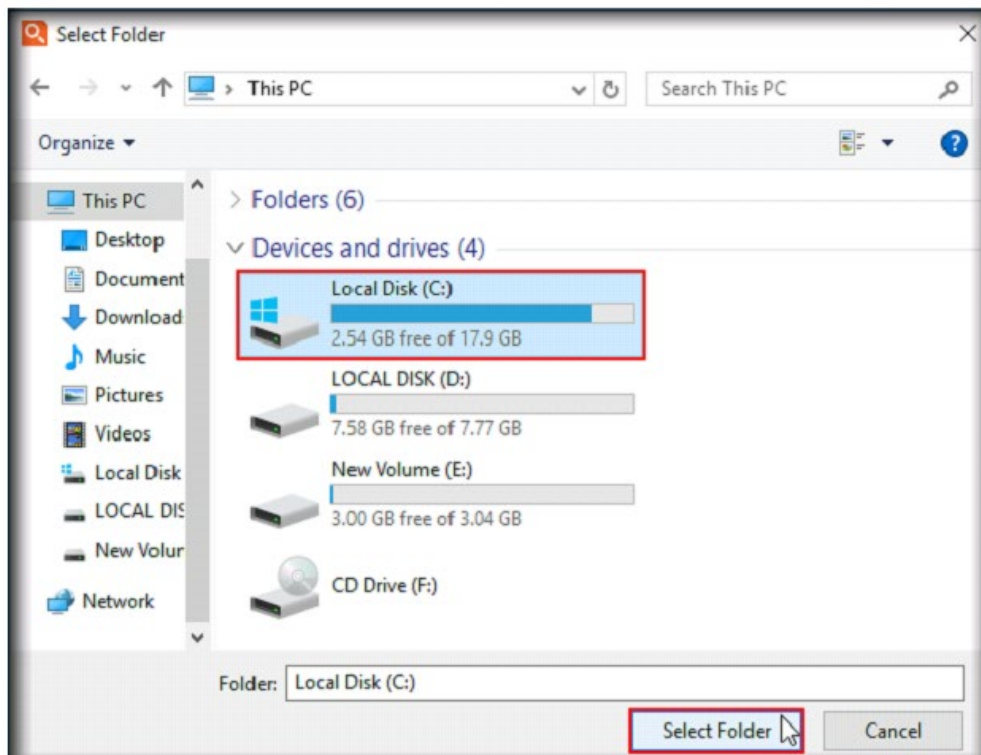
15. Directory Monitor GUI appears, click the **Add** button to add the directory you need to monitor.



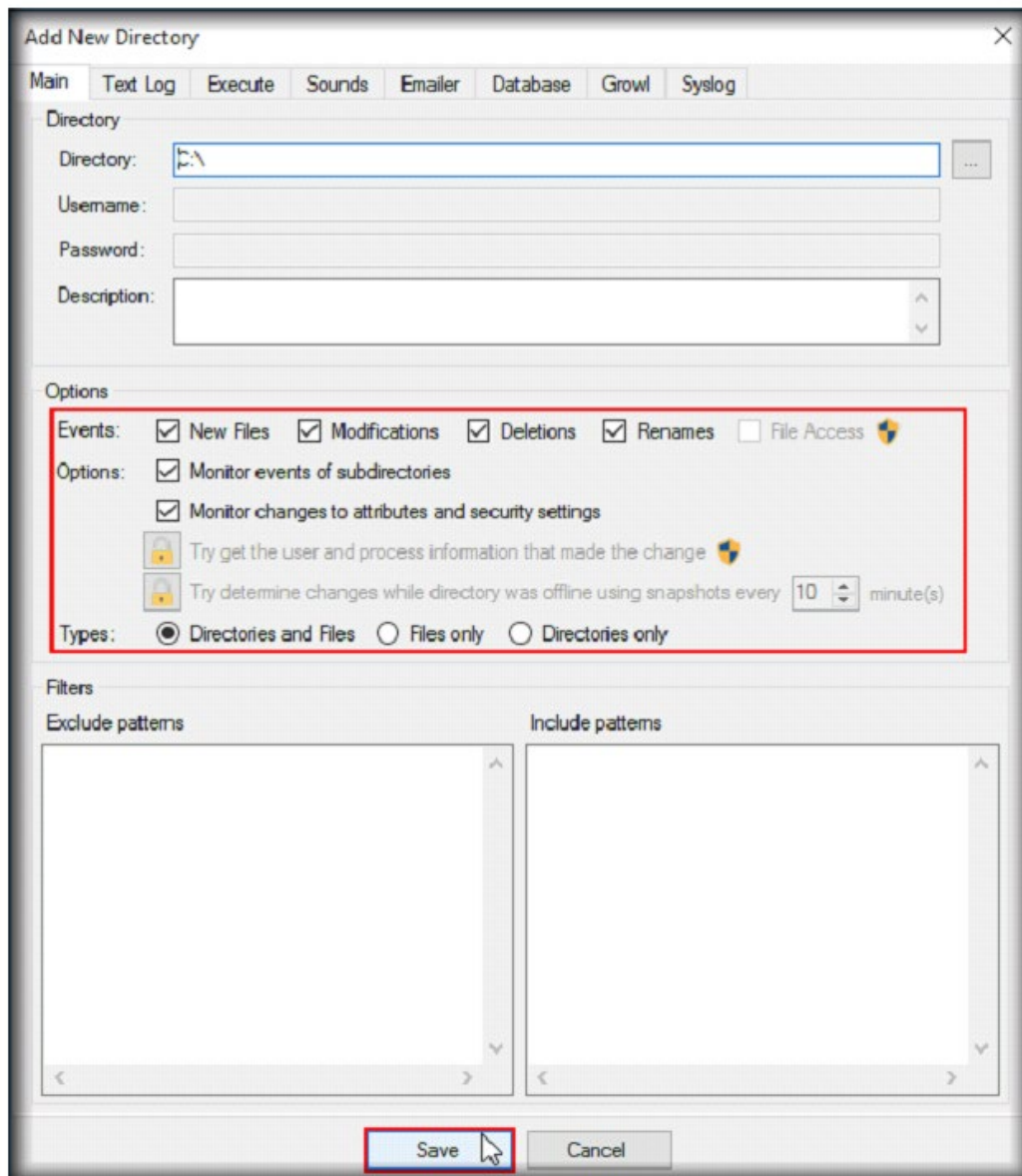
16. Click the **Ellipsis (...)** button to add the directories you need to monitor.



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

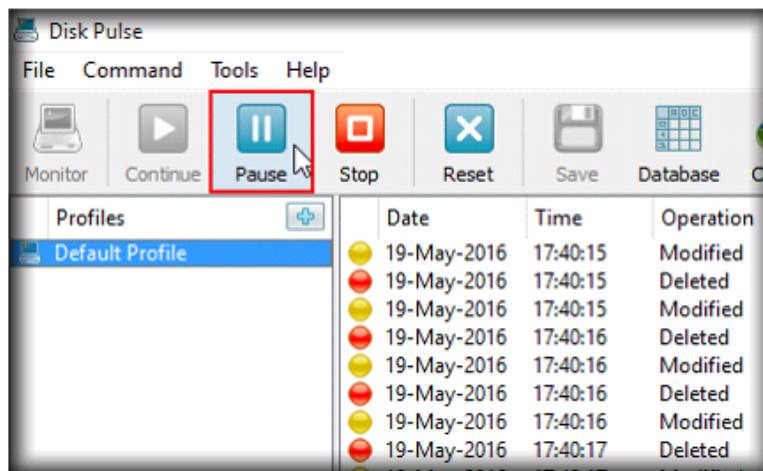


18. Select the required **Events**, **Options**, and **Types** from the **Options** section, and click the **Save** button. The tool will start recording all the activities from the selected folder and present them in the log activity in the form of **Text Log**, **Grid Log**, and **Activity Log**.

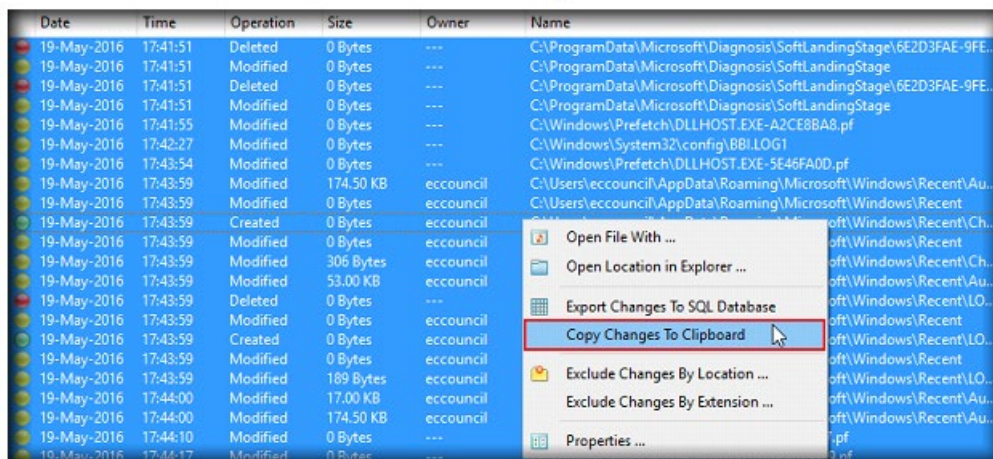


19. To install the Dropbox on the system, navigate to the location: https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308 for Dropbox Installer double-click DropboxInstaller.exe and follow the wizard driven steps. Once you complete the installation process, sign into the Dropbox account.

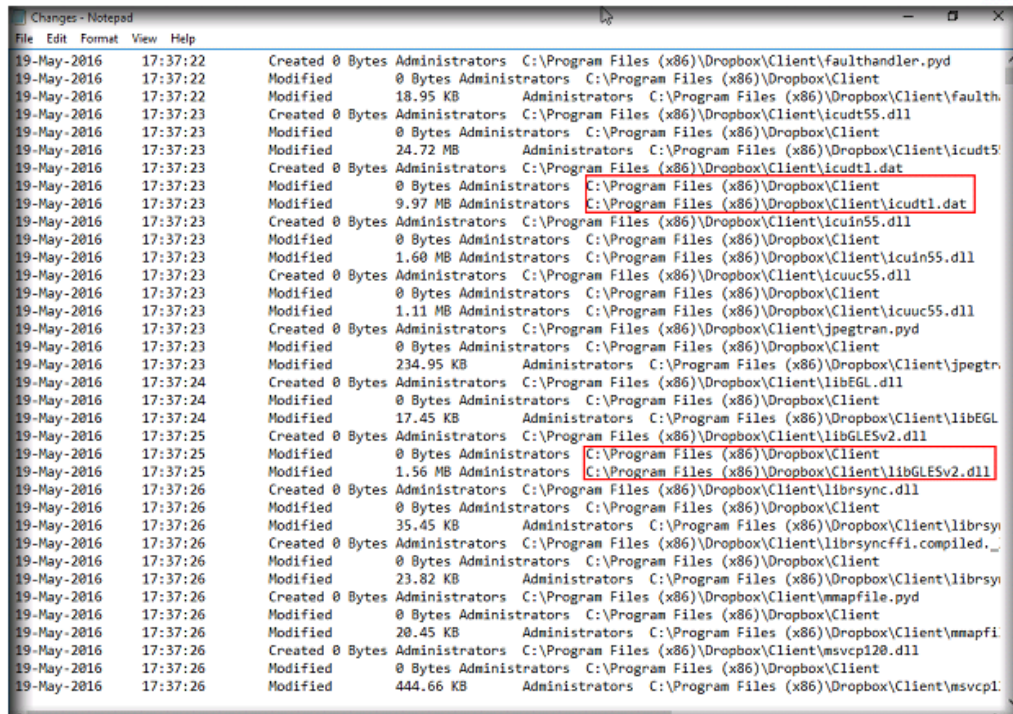
20. Now go to the already running **Disk Pulse** tool and pause the recording by clicking on the **Pause** button.



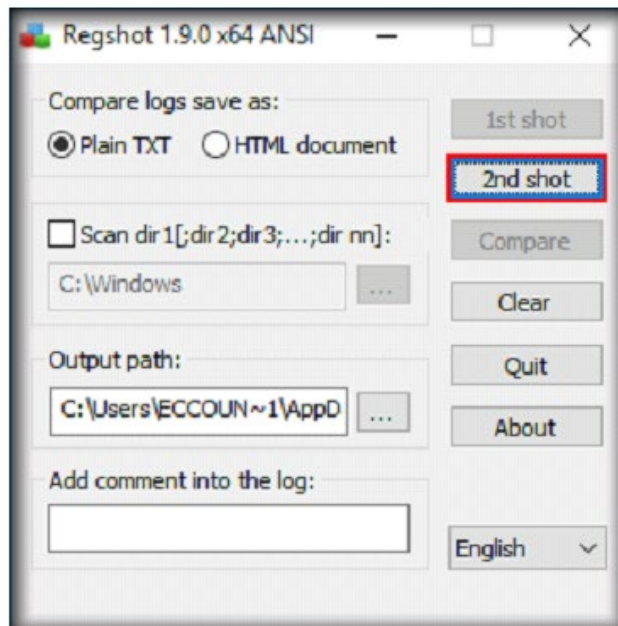
21. Select all the changes Disk Pulse has noted, right click the results, and click **Copy Changes To Clipboard** option.



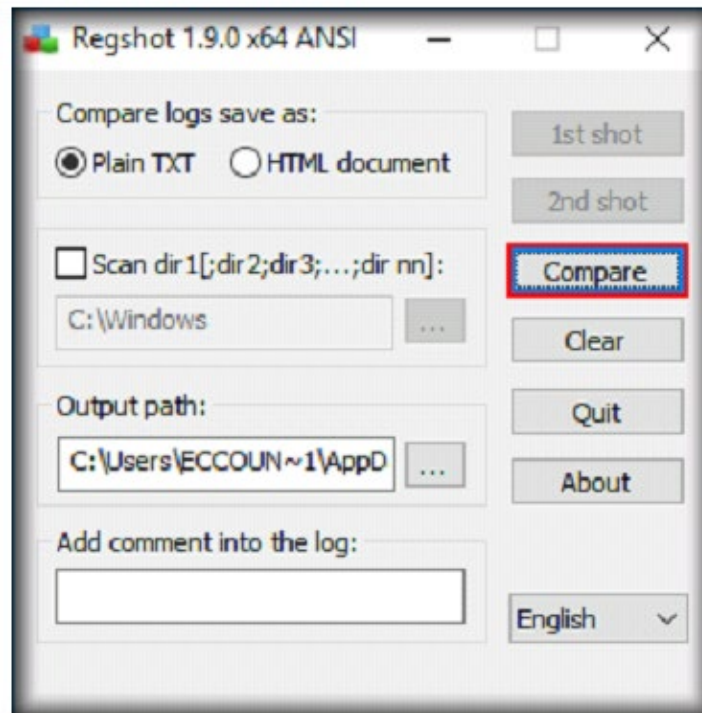
22. Copy the changes to a text file for easy analysis. The tool provides details of all the folders modified during installation, thus giving a list of addresses to check for traces of Dropbox.



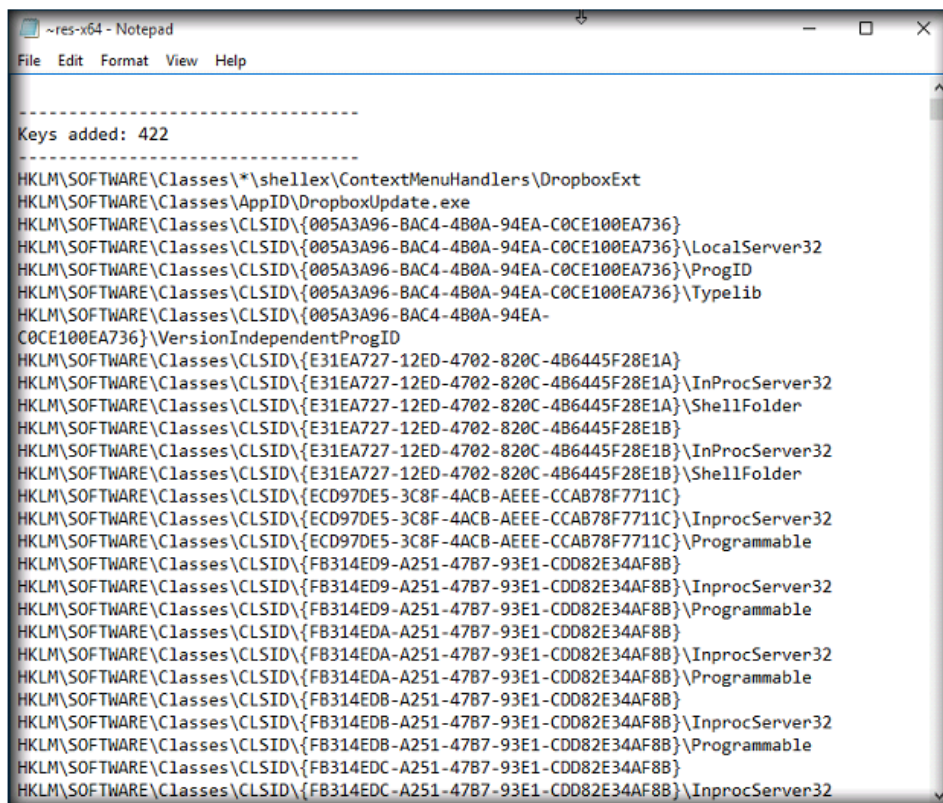
23. Run the **Regshot** tool. Click the **2nd shot** button to capture the second snapshot of the system.



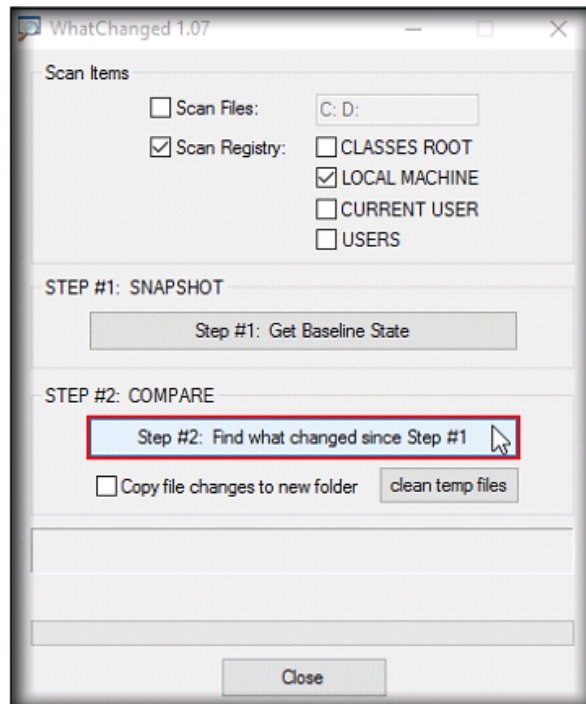
24. Now click the **Compare** button.



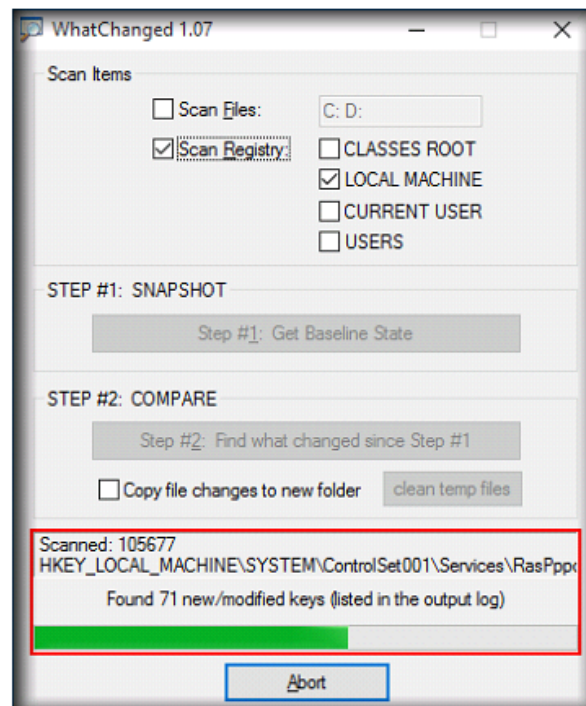
25. Regshot tool creates a result notepad file that consists of all the changes made to system files.



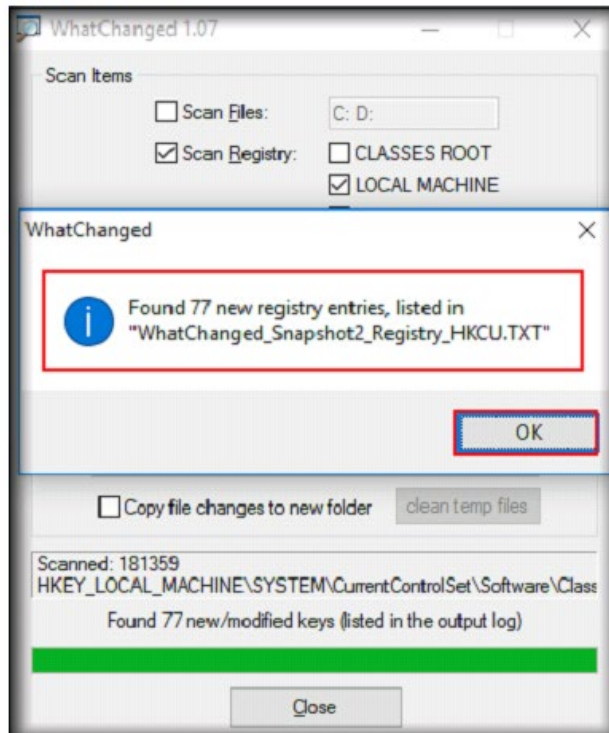
26. Go to the **WhatChanged** tool, click **Step #2: Find what changed since Step #1** button to take the snapshot of the system.



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.



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.



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 (WhatChanged Portable), i.e. at https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308
31. The notepad consists details of changes made to the **LOCAL MACHINE** along with address and the type of action involved.

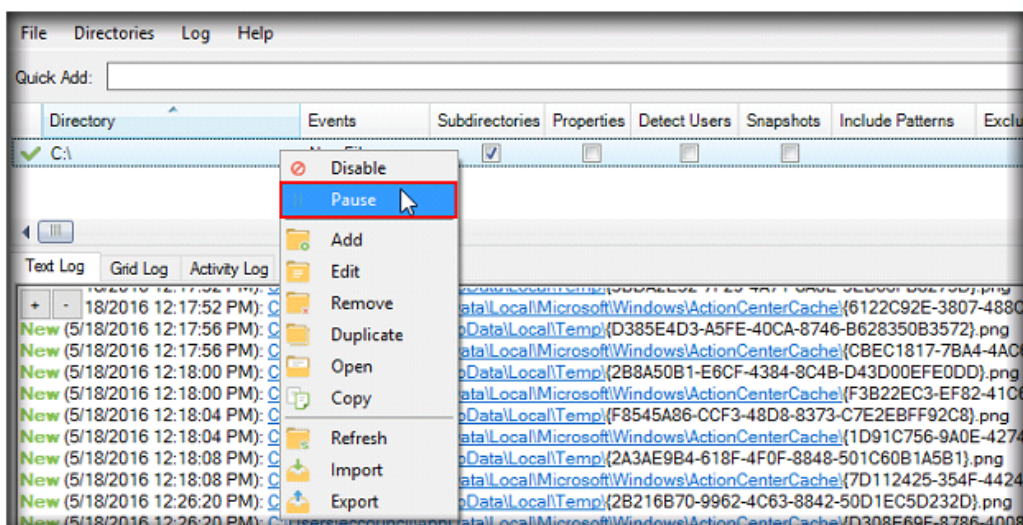
32. Here, you can observe that most of the changes are as part of installation of Dropbox onto the system. The folders and addresses reflected in the notepad store traces of information that could help in the investigation of the case.

```

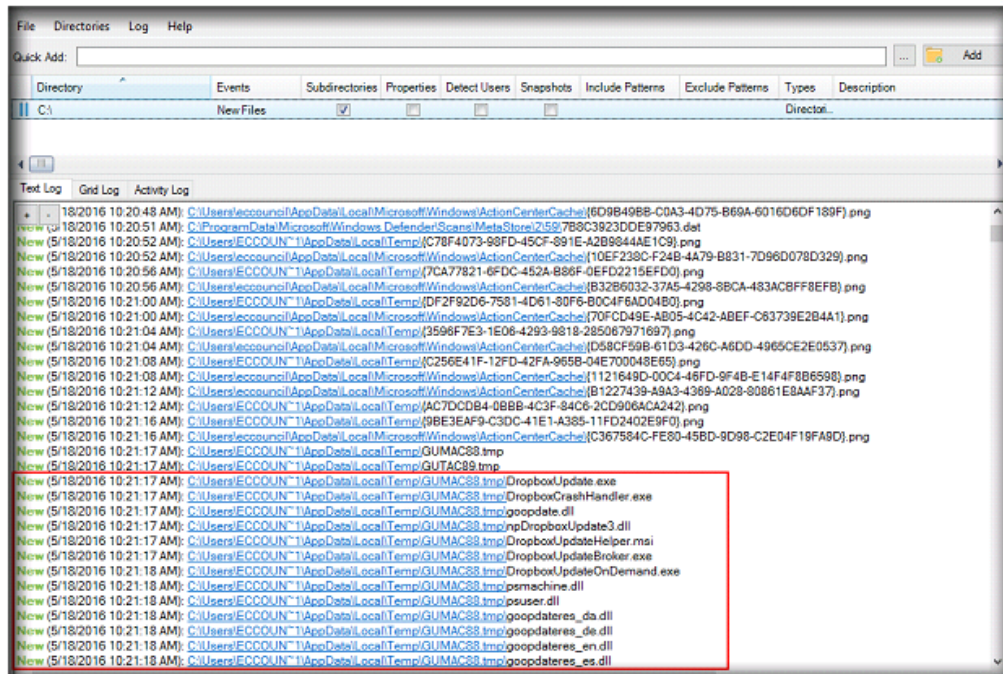
WhatChanged_Snapshot2_Registry_HKLM - Notepad
File Edit Format View Help
- CDD82E34AF8B}=DropboxExt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Extensions\Approved\{FB314EDF-A251-47B7-93E1-
- CDD82E34AF8B}=DropboxExt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Extensions\Approved\{FB314EE0-A251-47B7-93E1-
- CDD82E34AF8B}=DropboxExt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Dropbox="C:\Program Files (x86)\Dropbox
\Dropbox.exe" /systemstartup
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\UninstallString="C:\Program
Files (x86)\Dropbox\DropboxUninstaller.exe" /InstallType:MACHINE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\InstallLocation=C:\Program
Files (x86)\Dropbox\Dropbox\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\DisplayName=Dropbox
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\Publisher=Dropbox, Inc.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\DisplayIcon=C:\Program
Files (x86)\Dropbox\Dropbox.exe,0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\DisplayVersion=3.20.1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox
\URLInfoAbout=https://www.dropbox.com
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox
\HelpLink=https://www.dropbox.com
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\NoModify=1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\NoRepair=1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1297639565-
1588305015-3262420064-1001\RefCount=5
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\*\shellex\ContextMenuHandlers\DropboxExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\background\shellex\ContextMenuHandlers\DropboxExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\shellex\ContextMenuHandlers\DropboxExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\shellex\CopyHookHandlers\DropboxCopyHook
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Dropbox.AutoplayEventHandler\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Dropbox.AutoplayEventHandler\CurVer
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Dropbox.AutoplayEventHandler.4
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Dropbox.AutoplayEventHandler.4\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile\shellex\ContextMenuHandlers\DropboxExt
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MUI\StringCacheSettings\StringCacheGeneration=266
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Epoch\Epoch=1244
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules

```

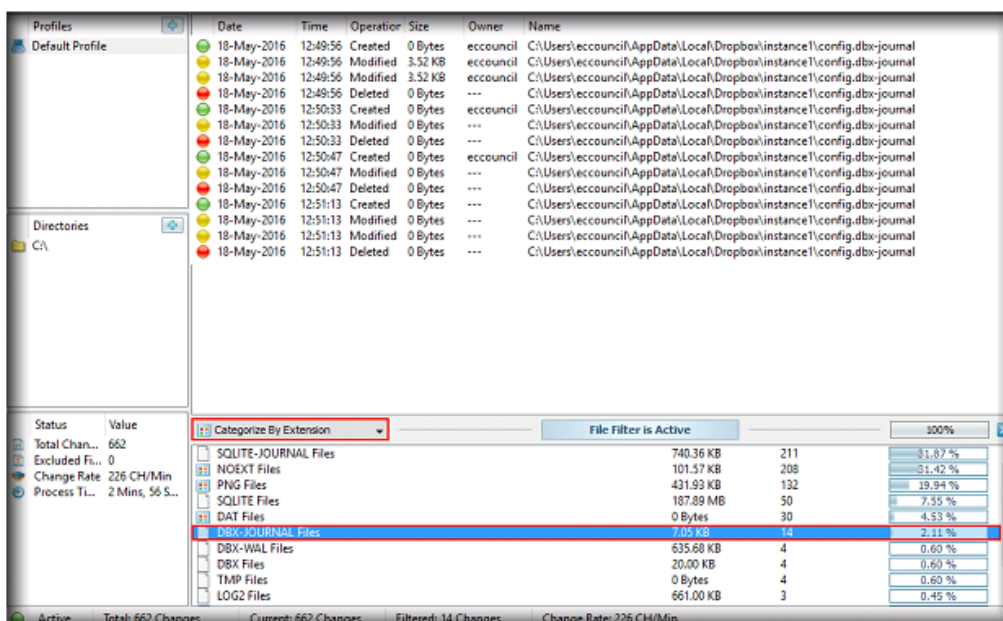
33. Open the already running Directory Monitor program and pause the scan. Right click a process and select **Pause** option from the list.



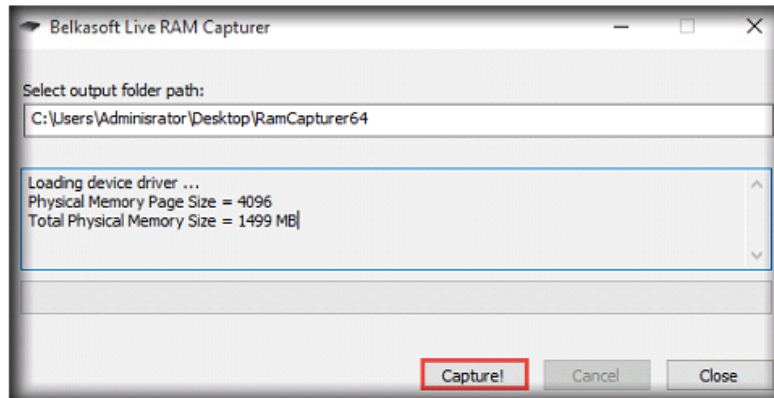
34. The tool will display all the actions that have contributed to changes in the system. On observing closely, you can see that the Dropbox installation process has added various new directories and folders to various system files.



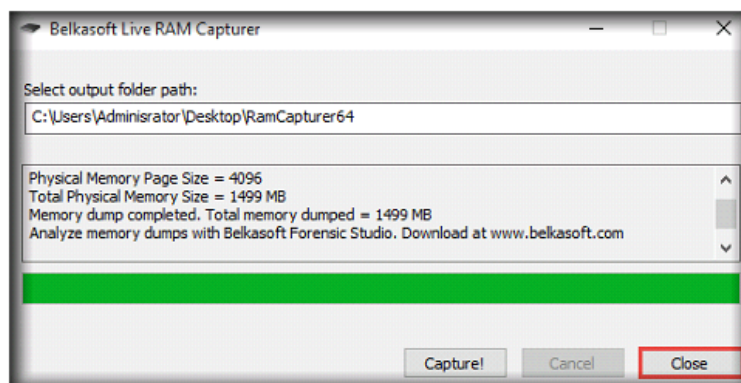
35. Open the already running **Disk Pulse** tool. Click the **DBX-JOURNAL Files** in the **Categorize By Extension** section of the tool to view all the changes the Dropbox files make to the system during configuration. All the Dropbox files hold the **.dbx** extension.



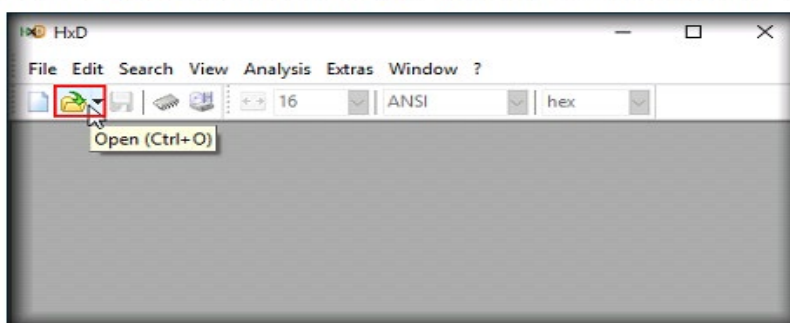
36. Launch the **RAM Capturer** tool from the location https://uwotd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwotd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308
37. Specify the **Output folder path** where you want to store the captured data and click the **Capture!** Button.



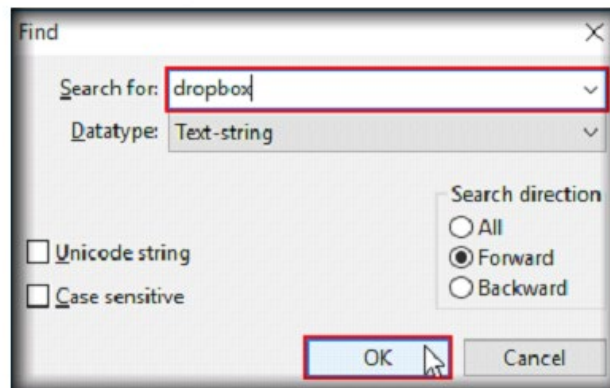
38. Click **Close** button after the tool completes capturing the RAM data.



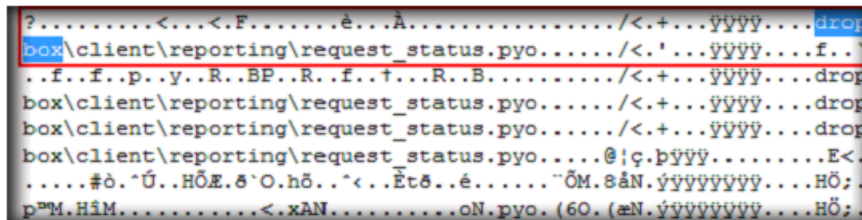
39. Navigate to https://uwotd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwotd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308 for Hex Editor (HxD) and double click the setup.exe file to run the HxD tool.
- Click the **Open** icon from the top right side of the menu bar.



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



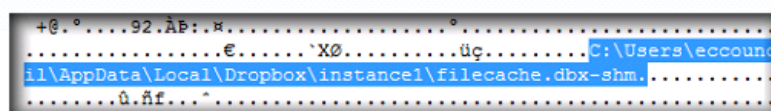
44. The tool will go to a line having keyword in it. Press **F3** to move forward and search for more such strings.



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.



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



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.

```

.....D.r.o.p.b.o.x. .O.p.s.....".D.r.o.p.b.o.x.....
.....C.a.l.i.f.o.r.n.i.a.....p.o.s.t.a.l.C.o.d.e.....
.....9.4.1.0.7...r.n.i.a.....S.T.R.E.E.T...o.d.e.....
.....4.3.4.8.2.9.6.....D.e.l.a.w.a.r.e...g.&
U.....filteredStyleSheets.0...U.....authorStyleDisabled...
U.....preferredStyleSheetSet..U.....PageStyle:StyleSheets...
.....O.="D.r.o.p.b.o.x......I.n.c..."yleSheets...
.....C.=U.S...o.p.b.o.x.....D.r.o.p.b.o.x. .O.p.s...
.....".D.r.o.p.b.o.x.....C.a.l.i.f.o.r.n.i.a.....
.....p.o.s.t.a.l.C.o.d.e.....9.4.1.0.7...r.n.i.a.....
.....S.T.R.E.E.T...o.d.e.....4.3.4.8.2.9.6.....
.....D.e.l.a.w.a.r.e...U.....persisted.9.6...eated...
U.....PageVisibility:Show....@[E.à_E.text/html.yleSheets...
U.....oncommandupdate.....U.....oncommandupdate.....
U.....text/html.lity:Show....U.....http://mzl.la/1Dls1DC...
U.....text/html.StyleSheets...U.....text/html.o.p.b.o.x...
U.....about:newtab.....\E. ]E.https://www.dropbox.com.
U.....https://www.dropbox.com.U.....https://.b.o.x...tor...
U.....www.dropbox.com.i.a...U.....www.dropbox.com.d.e...
U.....dropbox.com.sole.....U.....Enter Reader View...
U.....Roger@1234...6.....U.....Roger@1234...r.e...
U.....password-notification...U.....www.dropbox.com.led...
U.....R.o.g.e.r.@.1.2.3.4.....U.....Remember.:StyleSheets...
U.....Enter Reader View.x.....àE.à_E.http://mzl.la/1Dls1DC...
U.....oncommand.gger.....U.....TypeError: .x. .O.p.s...
U.....popuphidden.o.x...r.....U.....Roger@1234...r.n.i.a...
U.....Roger@1234...C.o.d.e.....loadingPrincipal...
U.....Link:SetIcon.....U.....Home - Dropbox...
U.....TabAttrModified...ditor.U.....Home - Dropbox..o.x...
U.....Home - Dropbox.ce.....filteredStyleSheets...
U.....authorStyleDisabled.s...U.....preferredStyleSheetSet...
U.....PageStyle:StyleSheets.....O.="D.r.o.p.b.o.x...e...
......I.n.c..."formance.....C.=U.S...T...or...

```

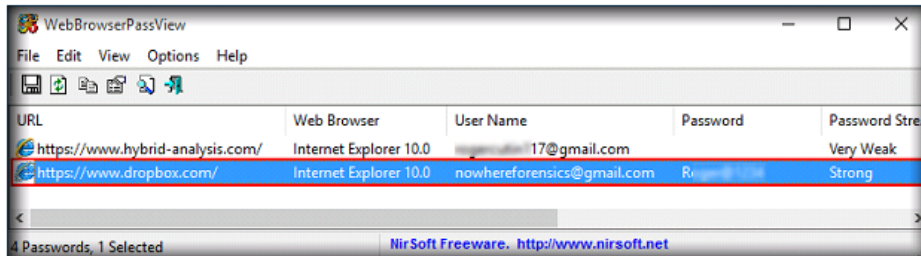
49. Google's Chrome browser also stores the password in the RAM that can be traced in the RAM captured data.

```

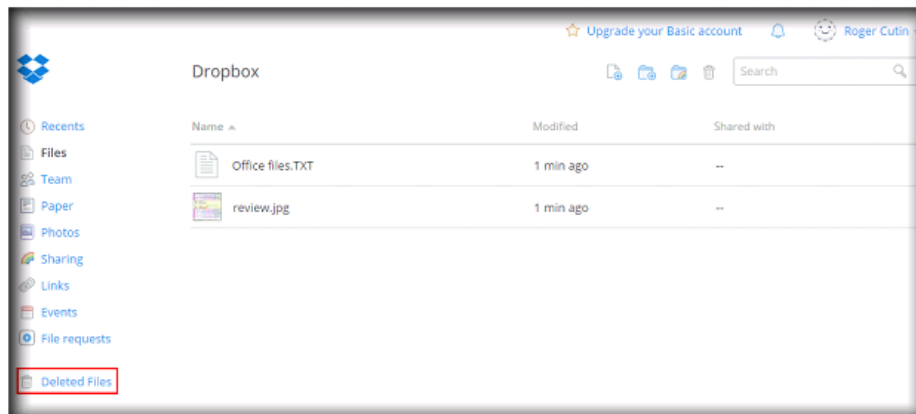
U.....www.dropbox.com...€...U.....https://www.dropbox.com.
U.....https://.r...%.>f..Q..U.....www.dropbox.com...€...
U.....https://www.dropbox.com.U.....https://.%.x.%.>f.Đ...
U.....www.dropbox.com...€...U.....https://www.dropbox.com.
U.....formOrigin..0.%.>f.à8..U.....https://www.dropbox.com.
U.....www.dropbox.com.6.%. %.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.%.ø...>f.`...
U.....keypress.>f.à<...€...U.....keypress...€...%.@...
U.....keypress..%.X.%.>f.P¥..U.....hostname.>f.e.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.pĖ...
U.....oldPasswordField...€...U.....nsILoginInfo...%.À...
U.....%.nsILoginInfo...%.>f.@`.U.....nsILoginInfo..ù..B..€...
U.....nsILoginMetaInfo...%. %.%.€%.nsILoginMetaInfo.>f.°...
U.....nsILoginMetaInfo...€...U.....nsIFactory.€...P.%.€...
U.....À.%.À%.nsIFactory...%.>f.8D..U.....nsIFactory..88..J..€...
U.....nsIPromptFactory...%.à%. %.%.nsIPromptFactory.>f.δ<...
U.....nsIPromptFactory...€...U.....nsIObserver.h...%.@...
U.....€.%.nsIObserver.y.%.>f..M..U.....nsIObserver..Q..R..€...
U.....nsIAuthPrompt...p.%. %.à%.%.nsIAuthPrompt...>f..j...
U.....nsIAuthPrompt...V..€...U.....nsIAuthPrompt2..Đ%.%.
U.....@%.`%.nsIAuthPrompt2...>f. e..U.....nsIAuthPrompt2..Z..€...
U.....nsILoginManagerPromter...%.À%.nsILoginManagerPromter...

```

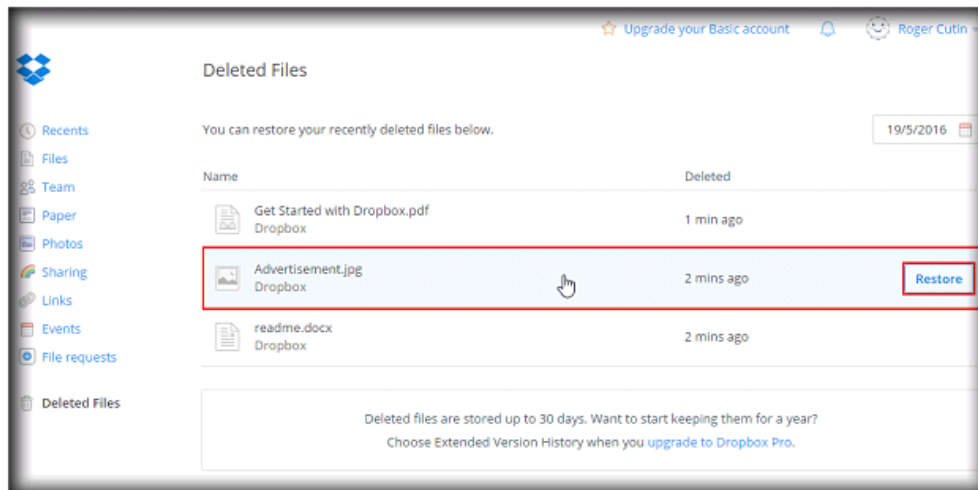
50. In case the passwords are not available in the hex data of the captured RAM data, run the **WebBrowserPassView** tool to find the usernames and password of the email accounts logged in through browsers as well as the accounts using clients to connect to the server.
51. The tool reveal details such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



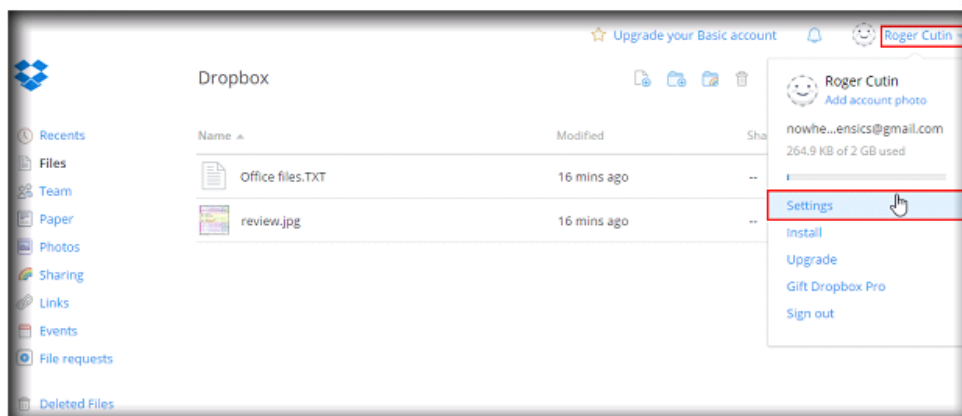
52. Use the username and password credentials of the Dropbox account to logon into it. Find the traces of files the perpetrator has deleted.
53. In the homepage of the Dropbox, click the **Delete Files** option from the left pane.



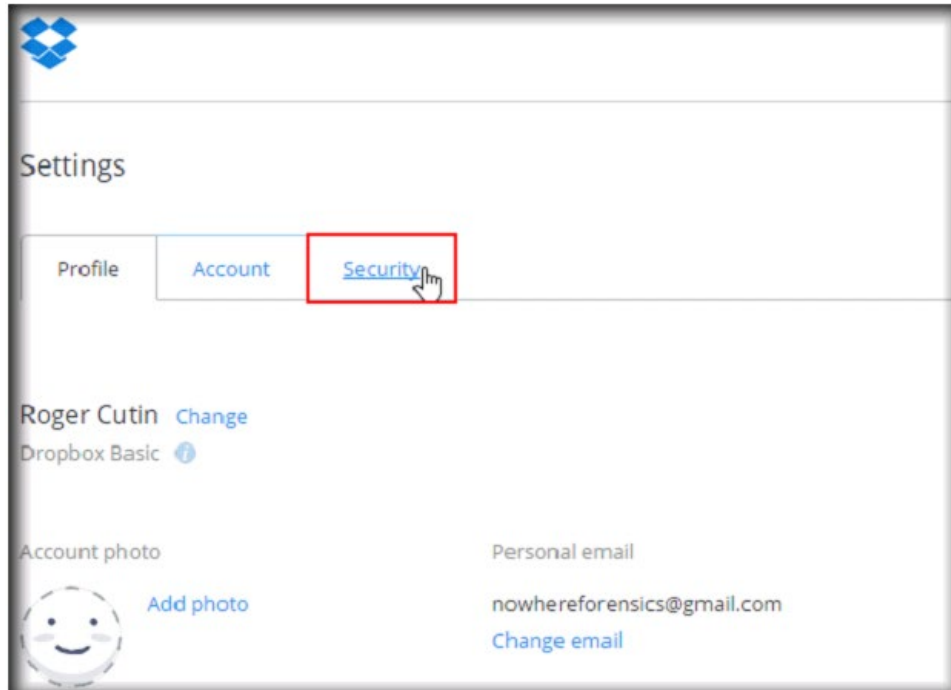
54. The website will navigate to the **Deleted Files** page. You can see all the deleted files here. To restore a deleted file, hover the mouse over the file you want to recover and click **Restore** button.
55. Restoration will help you in getting the original file and help to check its impact on the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



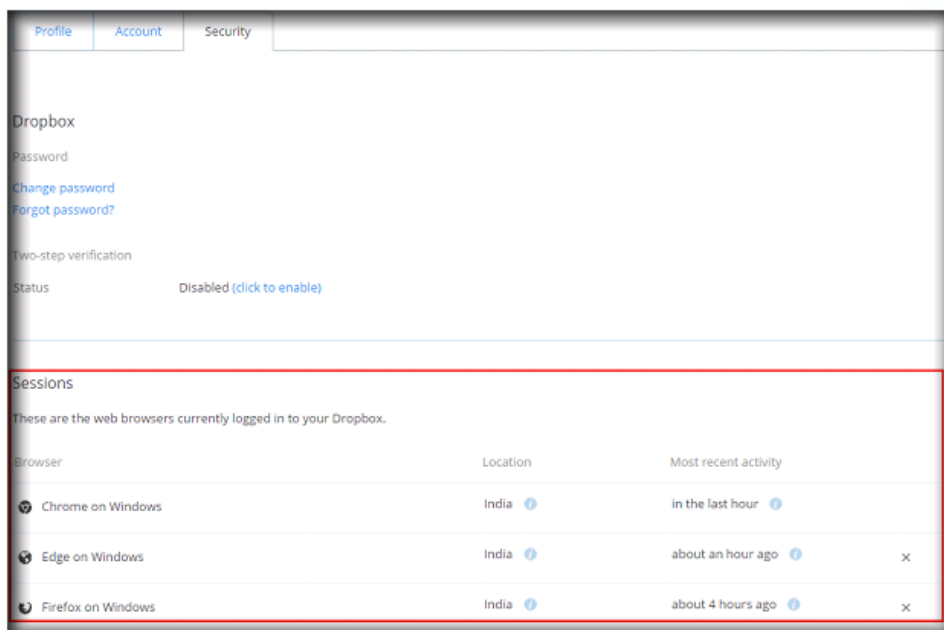
56. As part of the investigation, you should always try to find if someone had accessed the account from a different source along with details such as time and location.
57. To find out previous sessions or logs of the account, go to the sessions section of Dropbox website. In the account homepage, click the **Username** on the top right corner and select **Settings** from the dropdown list.



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

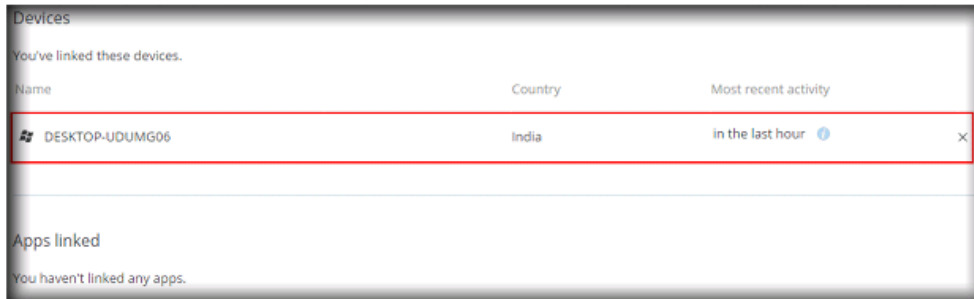


59. The security tab contains **Password**, **Session**, **Devices**, and **APPs** sections. Scroll down to **Sessions** section to view previous logins and browsers used to login.



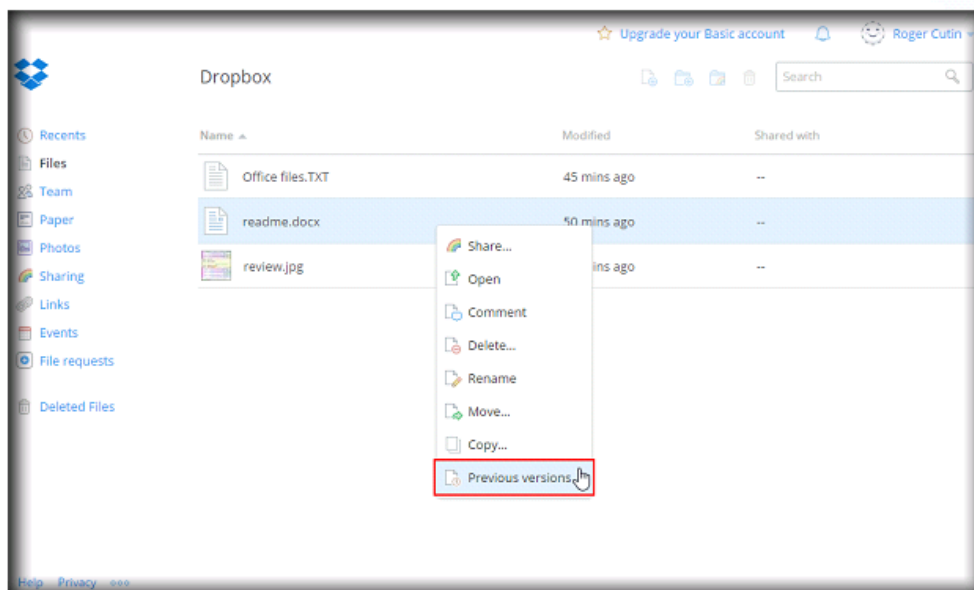
60. Scroll further to view the **Devices** section, which contains a list of devices that have accessed the Dropbox account through a client.

61. In addition, it displays the applications accessing the account.

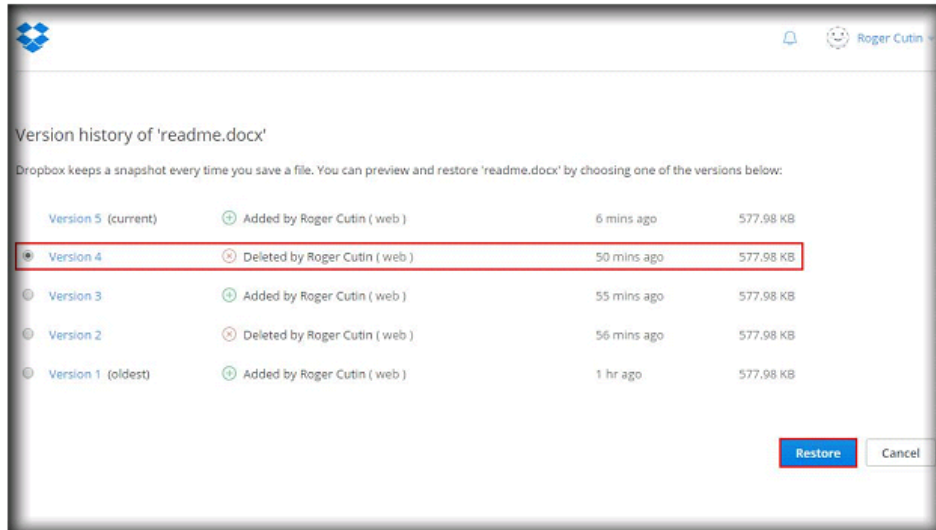


62. Dropbox also stores the details about each file uploaded in the form of versions and also allows you to recover any of the previous versions of a modified file.

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.

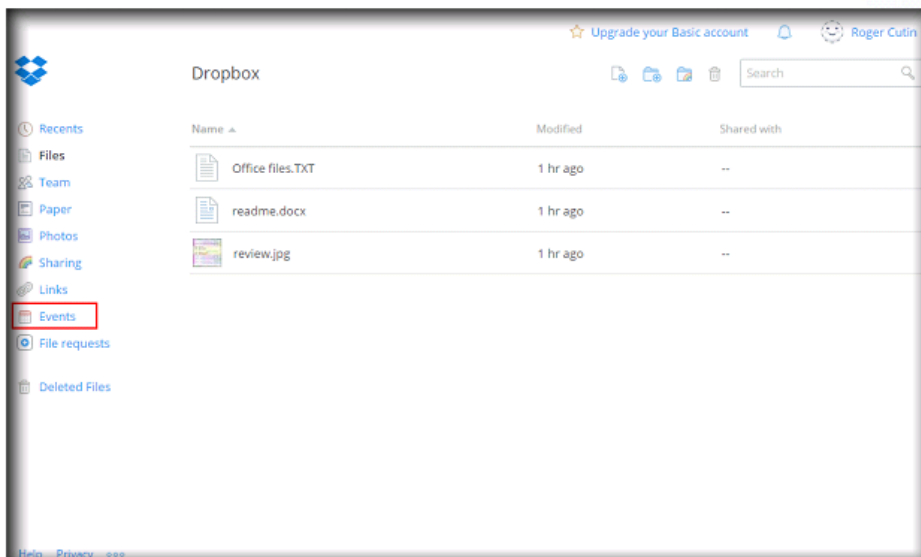


64. The tool will prompt you to the **Version History of <filename>** page, wherein you can select the version of the file you want to recover and click the **Restore** button.

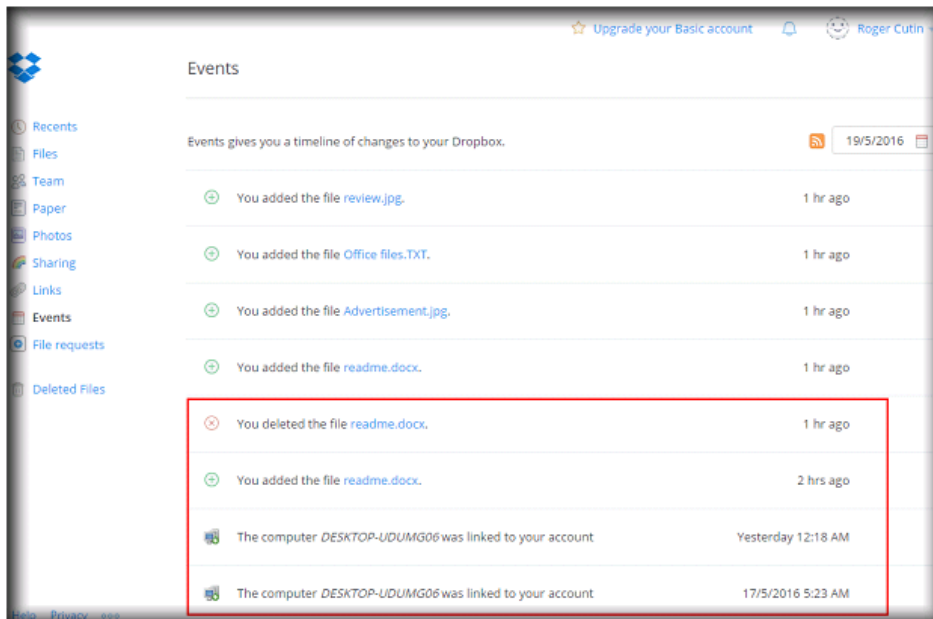


65. Other artifacts of Dropbox include events occurring over time. Dropbox stores record of all the events in the Events menu.

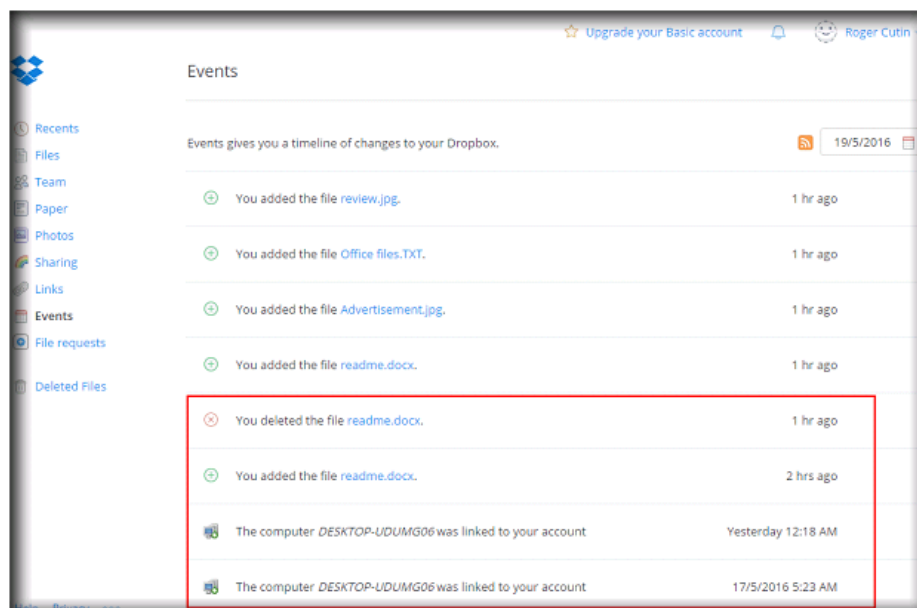
66. In the **Dropbox** account homepage, click the **Events** option from the left menu pane to view the events list.



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

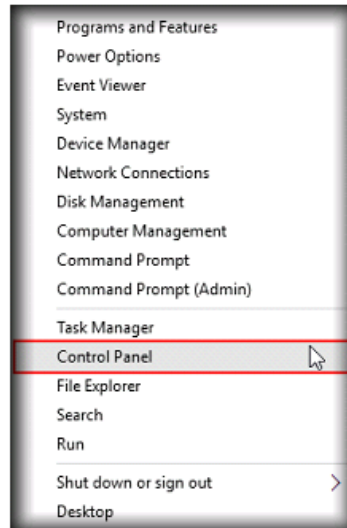


67. The events section stores all events, including adding and deleting of files, linking accounts to systems and applications, etc.

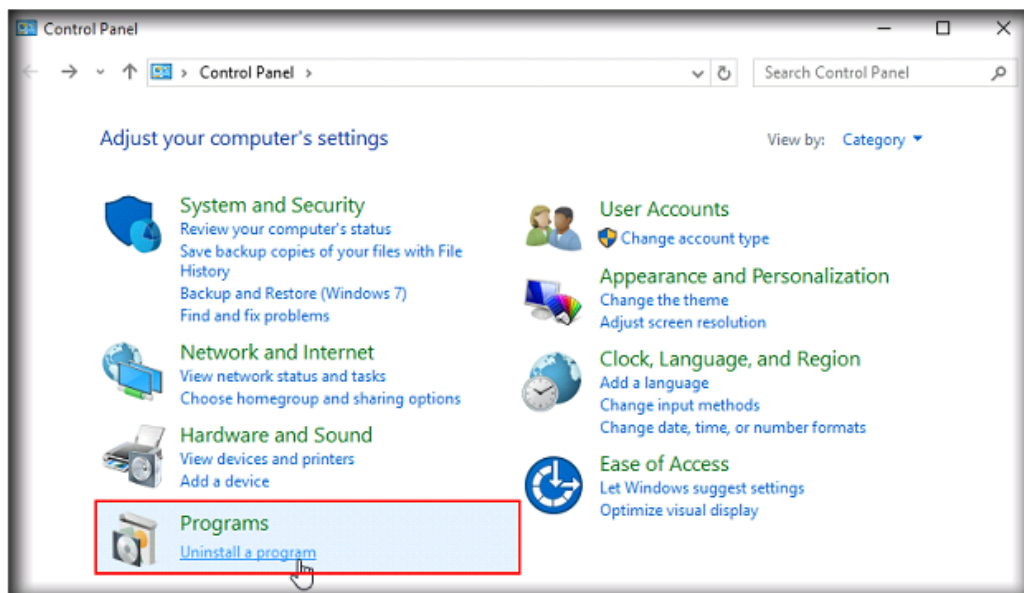


68. Now you need to know about the files a system retains when a user uninstalls Dropbox. Investigators can analyze these files to gather any available evidence.

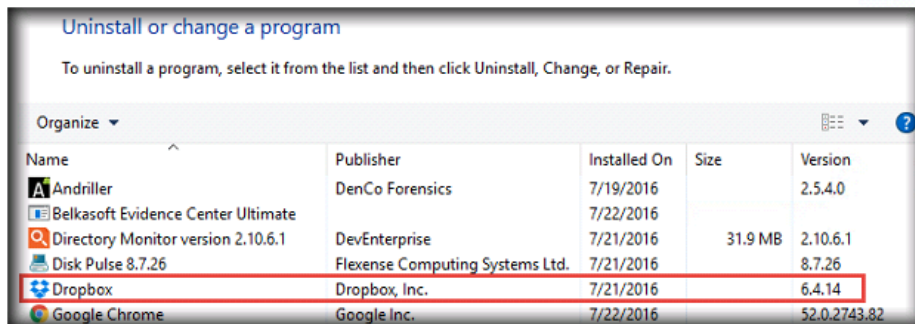
69. Run the already installed **Regshot** and **Disk Pulse** tools and follow the steps 2, 6, 7 and 8 in order to capture the system information before installing an application.
70. Right click the **Windows** icon at the lower left corner of the screen and select **Control Panel** option.



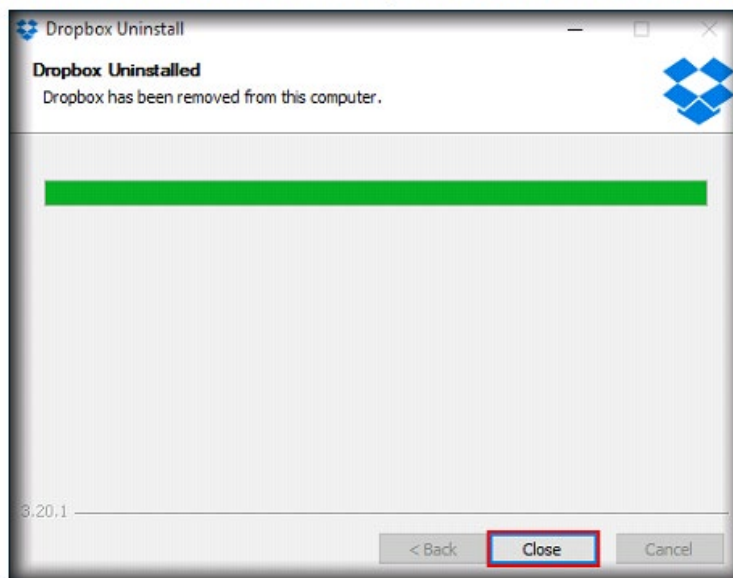
71. In the **Control Panel** window, click the **Uninstall a Program** link under the Programs section.



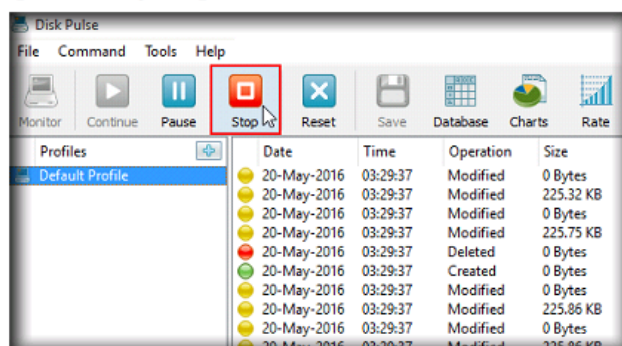
72. In the Uninstall or change a program section double click the **Dropbox** option to uninstall it.



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



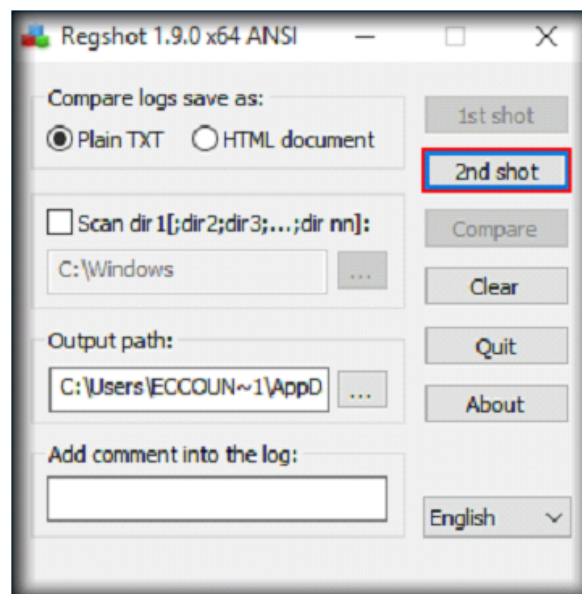
74. Go to the **Disk Pulse** tool and click the **Stop** button from the tool bar to stop recording the processes.



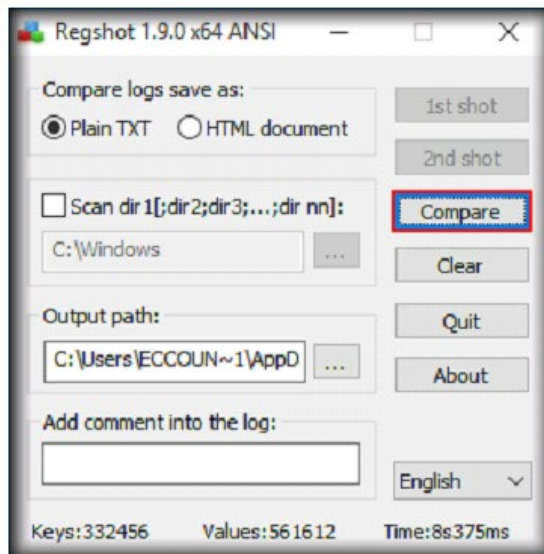
75. Select all the changes, right click, and select the option **Copy Changes To Clipboard**. This will help you to create a text or notepad file with all the modified addresses.

Date	Time	Operation	Size	Owner	Name
20-May-2016	03:29:37	Modified	0 Bytes	Administrators	C:\Program Files (x86)\Dropbox
20-May-2016	03:29:37	Modified	225.75 KB	Administrators	C:\Users\eccouncil\AppData\Roaming\Dropbox\installer\1573ee6fa
20-May-2016	03:29:37	Deleted	0 Bytes	---	C:\Program Files (x86)\Dropbox\Client
20-May-2016	03:29:37	Created	0 Bytes	Administrators	C:\Program Files (x86)\Dropbox
20-May-2016	03:29:37	Modified	0 Bytes	Administrators	C:\Program Files (x86)\Dropbox
20-May-2016	03:29:37	Modified	225.86 KB	Administrators	C:\Users\eccouncil\AppData\Roaming\Dropbox\installer\1573ee6fa
20-May-2016	03:29:37	Modified	0 Bytes	Administrators	C:\Program Files (x86)\Dropbox
20-May-2016	03:29:37	Modified	225.86 KB	Administrators	C:\Users\eccouncil\AppData\Roaming\Dropbox\installer\1573ee6fa
20-May-2016	03:30:14	Modified	0 Bytes	---	C:\Windows\System32\cmd
20-May-2016	03:30:14	Modified	224.00 KB	SYSTEM	C:\Users\eccouncil\AppData\Roaming\Dropbox\installer\1573ee6fa
20-May-2016	03:31:49	Modified	226.53 KB	Administrators	C:\Users\eccouncil\AppData\Roaming\Dropbox\installer\1573ee6fa
20-May-2016	03:31:49	Deleted	0 Bytes	---	C:\ProgramData\Microsoft\Windows\CurrentVersion\Installer\1573ee6fa
20-May-2016	03:31:49	Created	0 Bytes	---	C:\ProgramData\Microsoft\Windows\CurrentVersion\Installer\1573ee6fa
20-May-2016	03:31:49	Modified	0 Bytes	---	C:\ProgramData\Microsoft\Windows\CurrentVersion\Installer\1573ee6fa
20-May-2016	03:31:50	Modified	330 Bytes	eccouncil	C:\Users\eccouncil\AppData\Roaming\Dropbox\installer\1573ee6fa
20-May-2016	03:31:53	Modified	226.92 KB	Administrators	C:\Users\eccouncil\AppData\Roaming\Dropbox\installer\1573ee6fa
20-May-2016	03:31:53	Deleted	0 Bytes	---	C:\Users\ECCOUN~1\AppData\Local\Temp\insnE3E6.tmp\modern-hea...
20-May-2016	03:31:53	Modified	227.01 KB	Administrators	C:\Users\eccouncil\AppData\Roaming\Dropbox\installer\1573ee6fa
20-May-2016	03:31:53	Modified	0 Bytes	Administrators	C:\Users\ECCOUN~1\AppData\Local\Temp\insnE3E6.tmp
20-May-2016	03:31:53	Modified	227.31 KB	Administrators	C:\Users\eccouncil\AppData\Roaming\Dropbox\installer\1573ee6fa
20-May-2016	03:32:15	Modified	224.00 KB	SYSTEM	C:\Users\eccouncil\ntuser.dat.LOG2
20-May-2016	03:33:28	Modified	0 Bytes	---	C:\Windows\Prefetch\AgGIUAD_S-1-5-21-1297639565-1588305015-326...
20-May-2016	03:33:28	Modified	0 Bytes	---	C:\Windows\Prefetch\AgGIUAD_P_S-1-5-21-1297639565-1588305015-3...

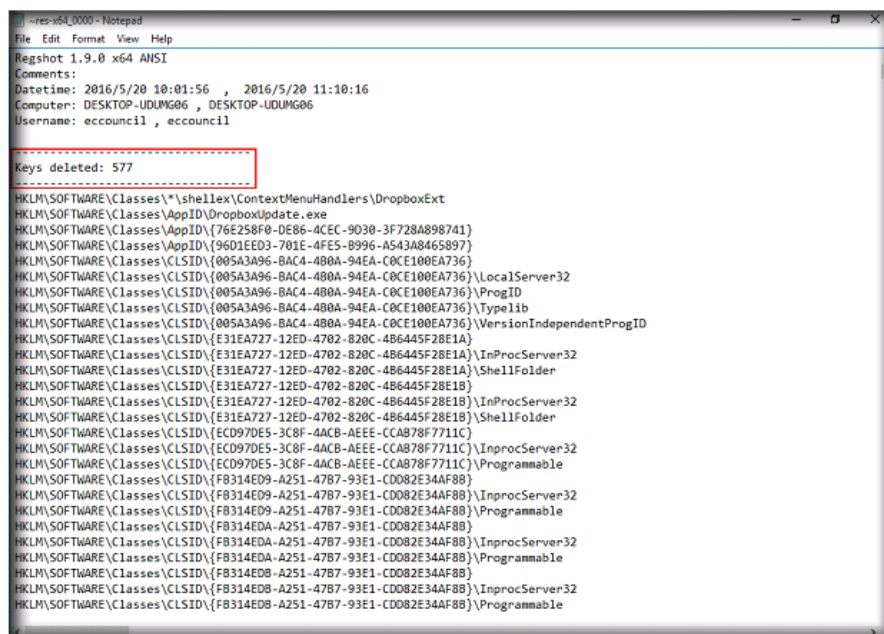
76. Now create a text file and paste the contents onto it. These modified files represent all the changes made while uninstalling the Dropbox client from the system.
77. Launch the **Regshot** tool and click the **2nd shot** button to capture the second snapshot of the system. This action will record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



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.



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.



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.

Task 3: 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.

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

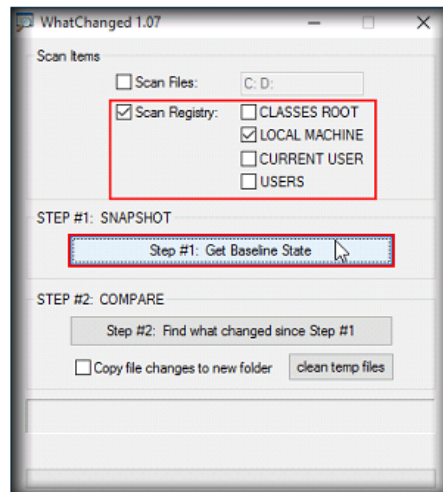
In this lab, you need:

- A computer running on Windows 10.
- Internet connection.
- Google Drive account.
- Tools such as WhatChanged, Disk Pulse, RAM Capturer, HxD Editor, WebBrowserView DB Browser tools are location at: https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308

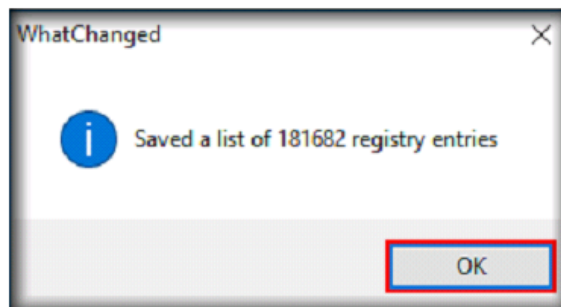
Lab Tasks

1. Navigate to https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308 and Install the tools WhatChanged, Disk Pulse, RAM Capturer, HxD Editor, WebBrowserView DB Browser

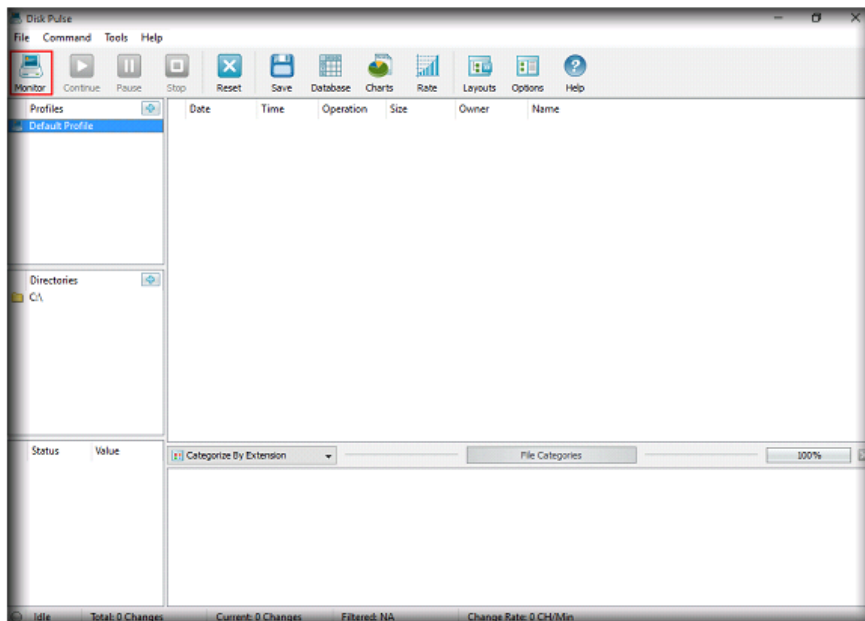
2. Run the **WhatChanged** tool to create a baseline state of the system. Select the **Scan Registry** option and also check the **LOCAL MACHINE** option.
3. Click the **Step #1: Get Baseline State** button to capture first snapshot or create baseline of the system.



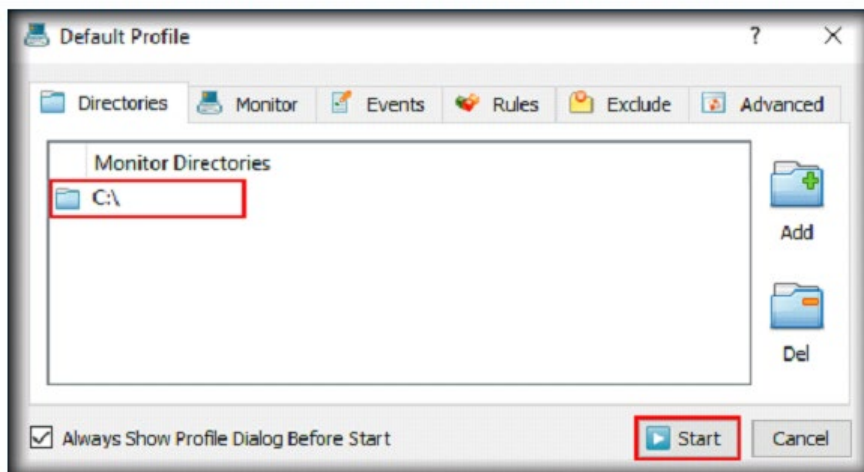
4. The tool will prompt a **WhatChanged** dialog box displaying the total number of entries it recorded. Click the **OK** button.



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



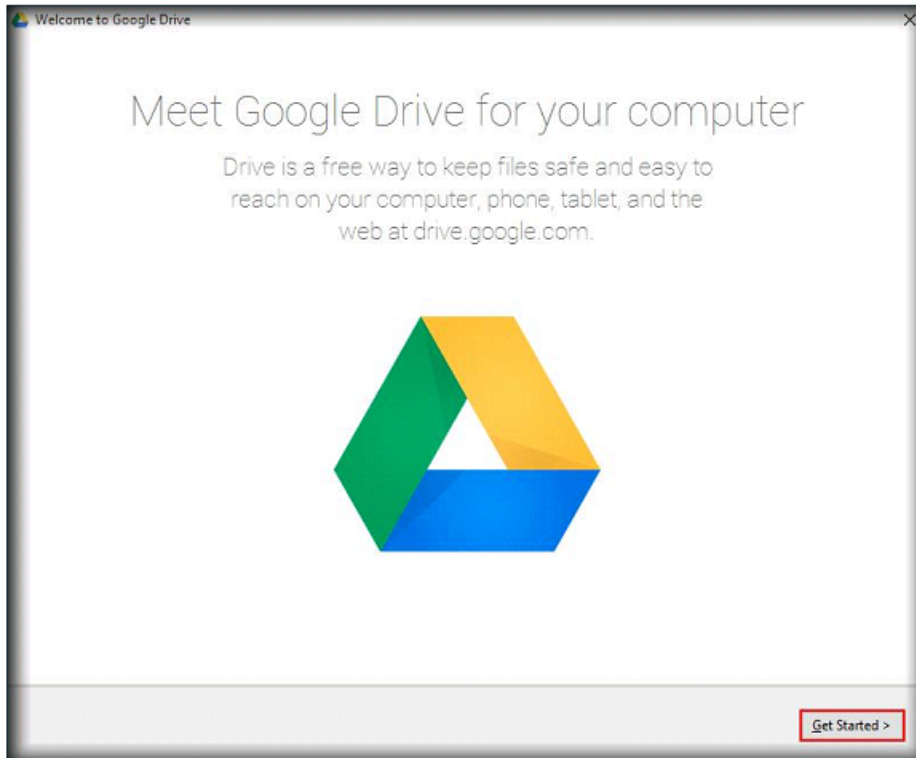
6. The tool will display a **Default Profile** dialog box which will allow the user to add directories you want to monitor. The tool adds **C:** directory to this profile by default.
7. Click **Add** to add more directories, else click the **Start** button.



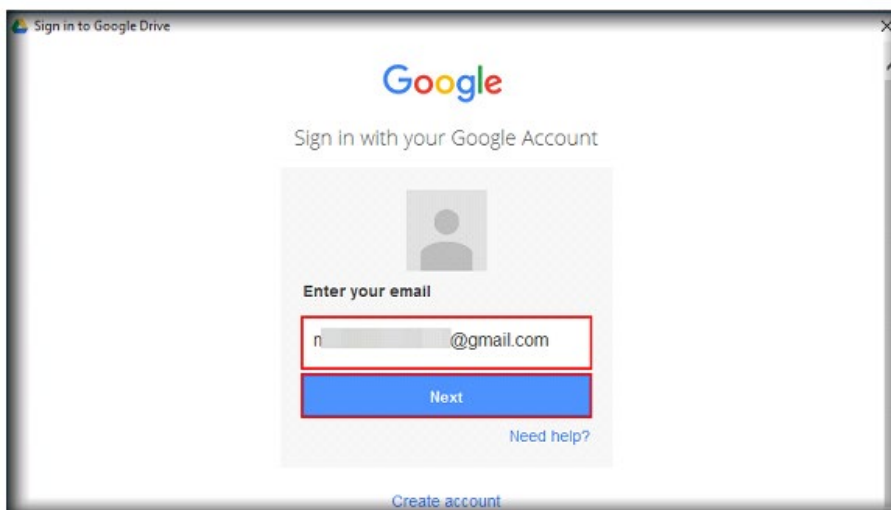
8. Navigate to https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1ggPPWOiezg?e=2vg308 for Google Drive Client, double-click

googledrivesync.exe and follow the wizard driven installation steps to install the application. On completing the installation, click **Close** in the **Installation Complete** window.

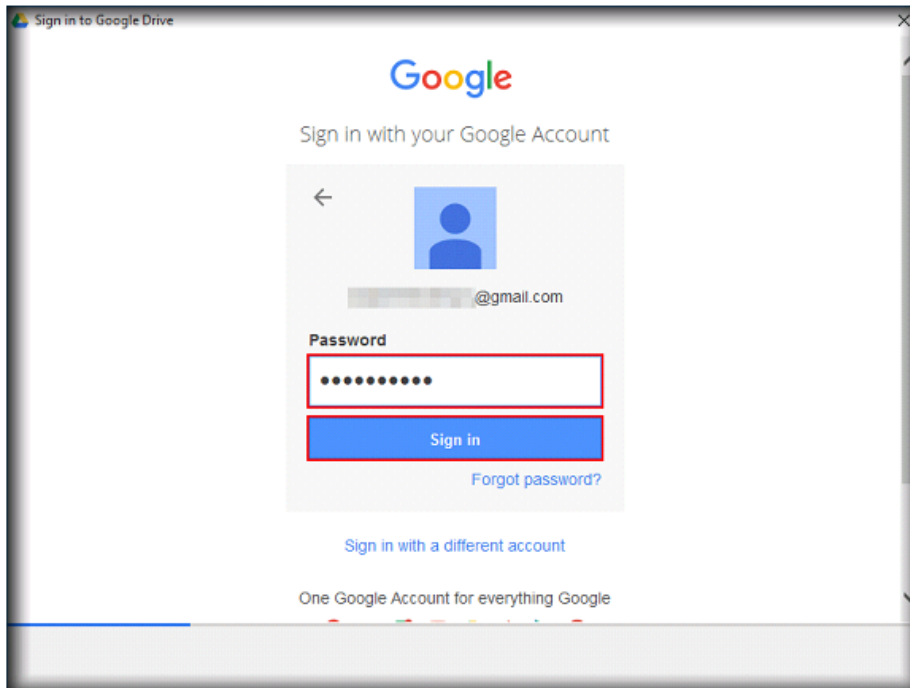
9. Click **Google Drive** icon in the **Apps** screen to run the Google Drive client, and click on **Get Started** to start using the client.



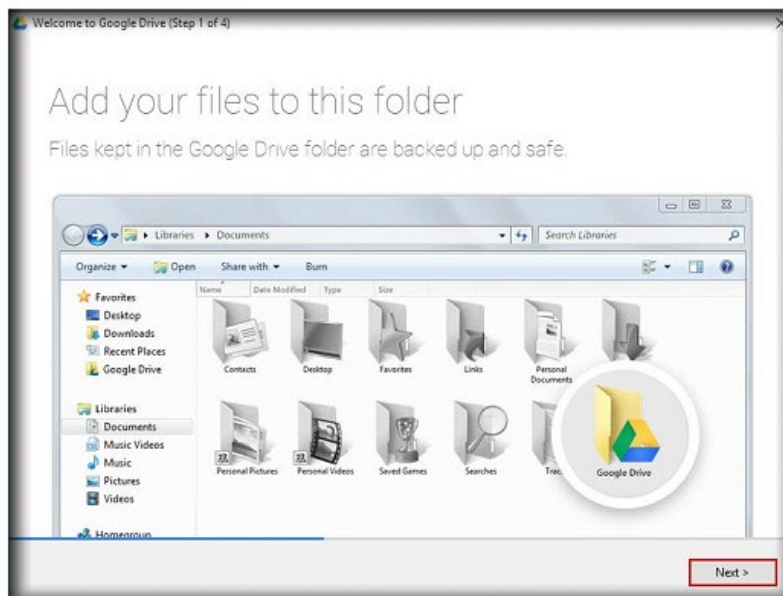
10. Enter the email address of the Google Drive Account and click the **Next** button.



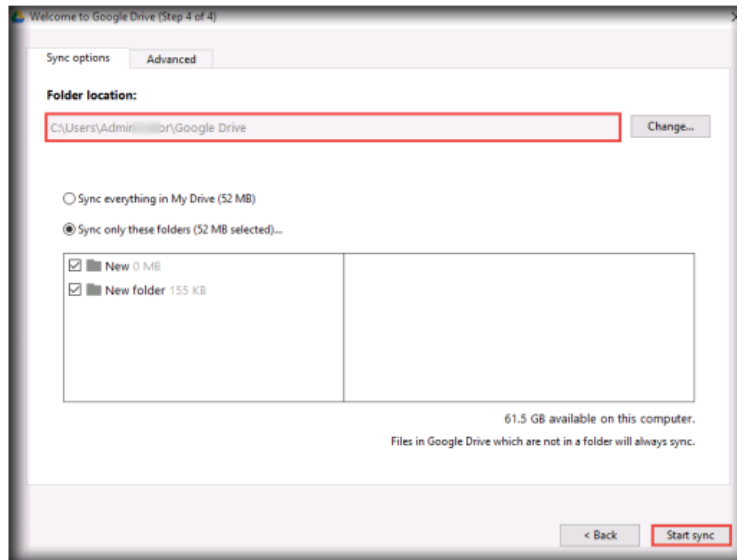
11. Enter the password of the account and click the **Sign In** button.



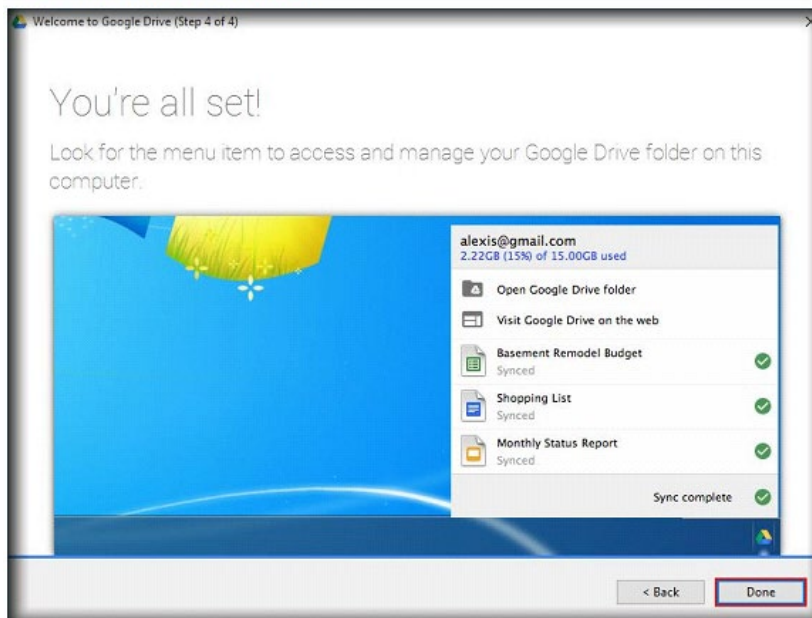
12. The Drive client will take you through the installation information. Note this information because it will help you know about the places where the client stores information on the system. Click the **Next** button.



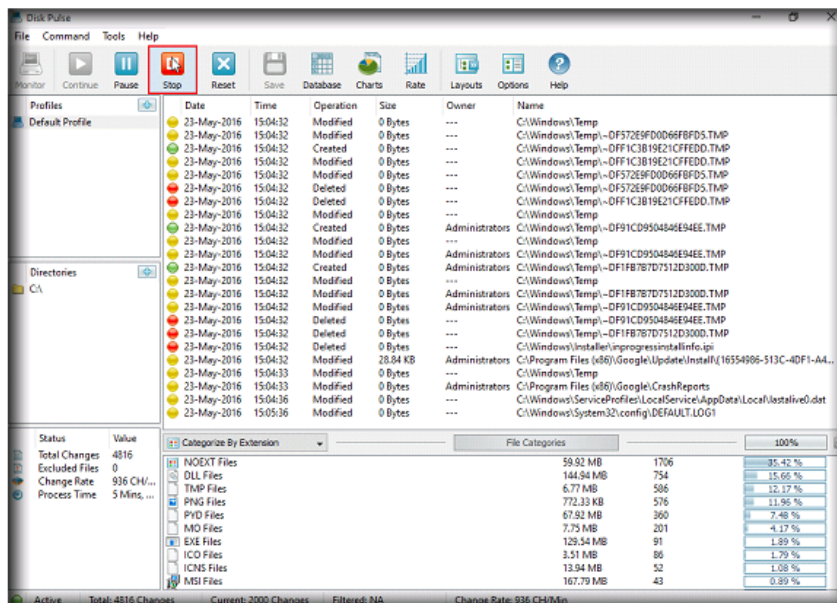
13. Click **Next** button till you go to **Step 4**. Step 4 describes the location which syncs the files on the drive and gives location of a folder that stores the files on the system. In this case, the Google Drive will save a folder at **C:\Users\Administrator\Google Drive** and will sync all the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



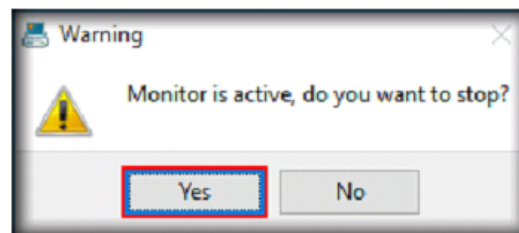
14. Click the **Done** button.



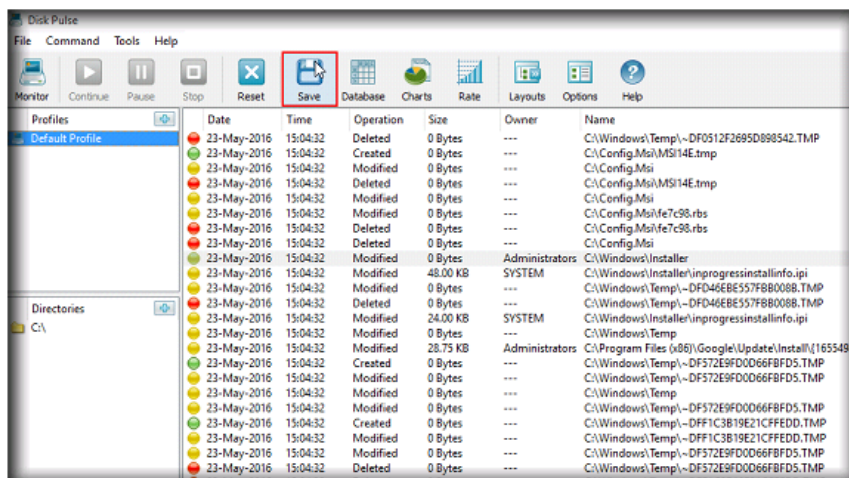
15. After installation is completed, go to the **Disk Pulse** tool and click the **Stop** button to stop monitoring process.



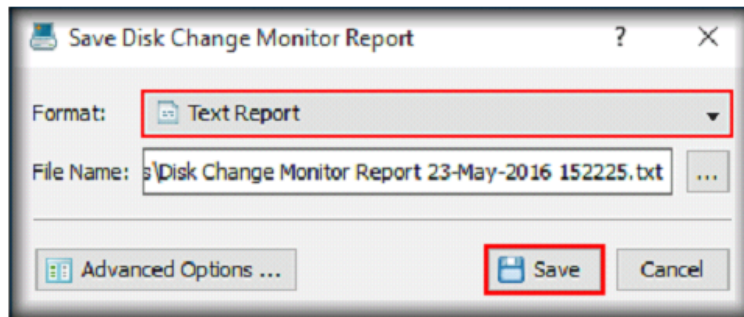
16. The tool will display a **Warning** dialog box, click the **Yes** button to stop the monitoring process.



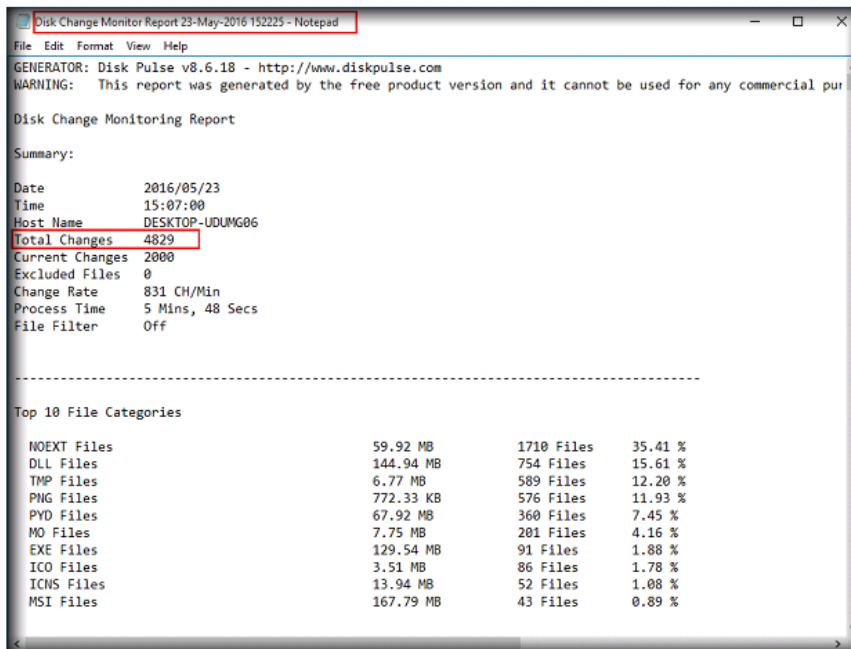
17. Click the Save Record or Save Icon in the tool to save all the entries in the required format.



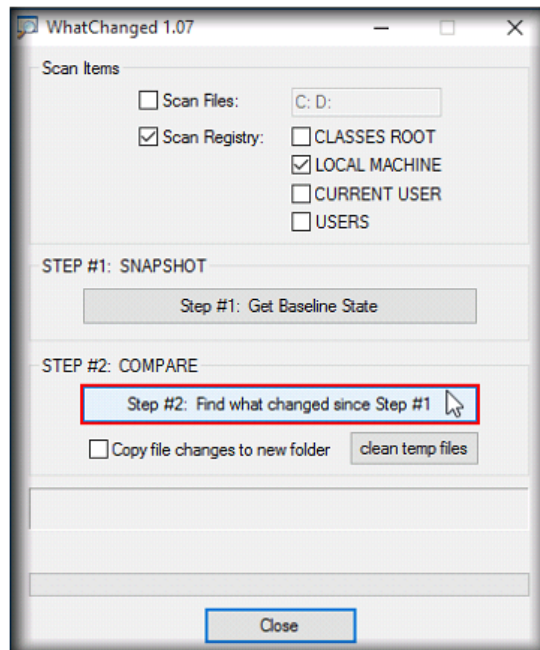
18. The tool will prompt a **Save Disk Change Monitor Report** dialog-box. Click the **Format** option from dropdown list bar and select the required format. Here, you can select **Text format**. Click the **Save** Button.



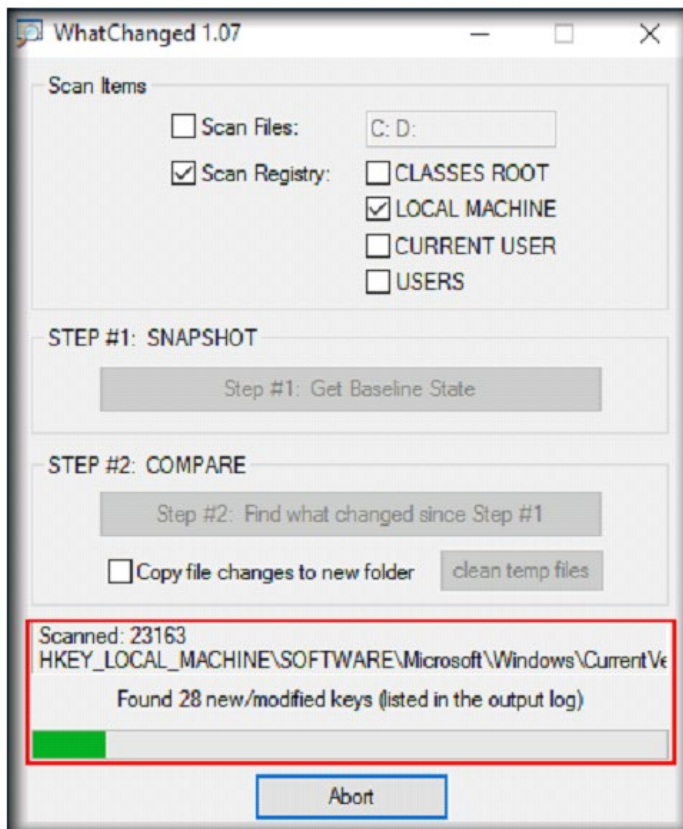
19. The tool will save a Text file with all the changes listed in it.



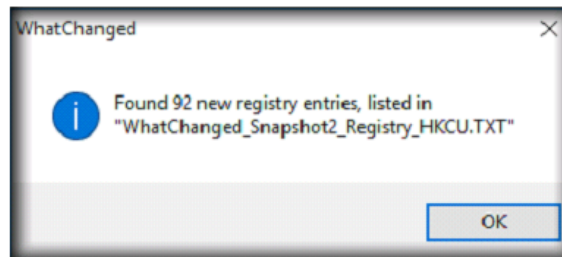
20. Go to the WhatChanged tool and take the second snapshot of the system. Click the **Step #2: Find what changed since Step #1**.



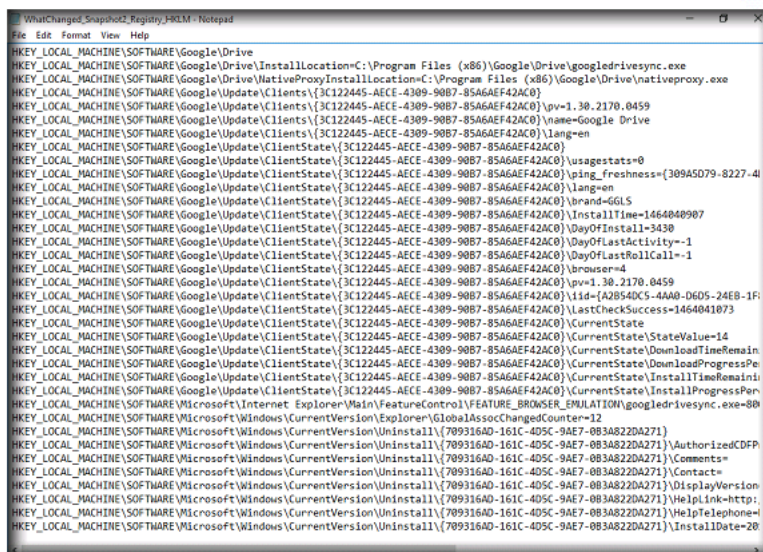
21. The tool will check for the changed entries and re-record all the modified ones. The tool will display the number of changes it has observed across the system and also the progress of scanning.



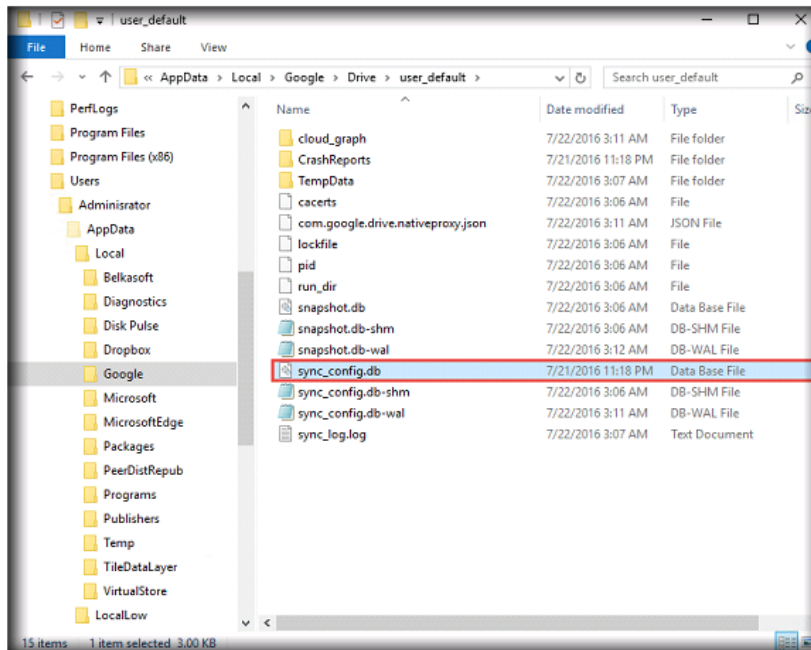
22. On completion of scanning process, the tool will display a dialog box displaying the number of new entries it listed. Click the **OK** button.



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

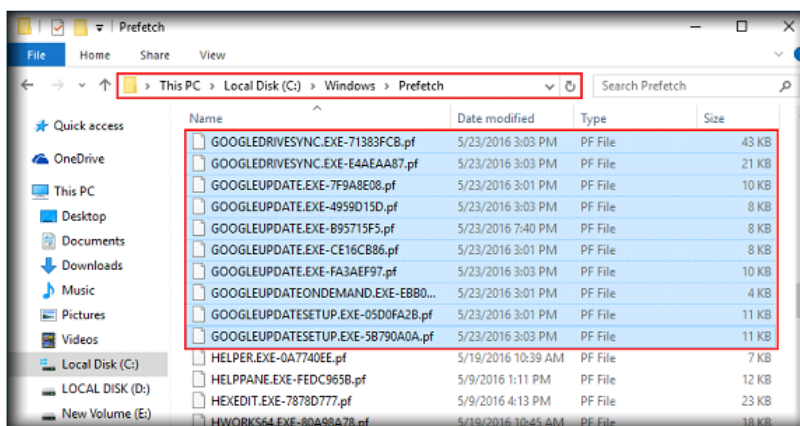


24. The Google Drive client makes many changes in the system such as creation of folders. It stores its configuration files in **C:\Users\<User Name>\AppData\Local\Google\Drive\user_default**.

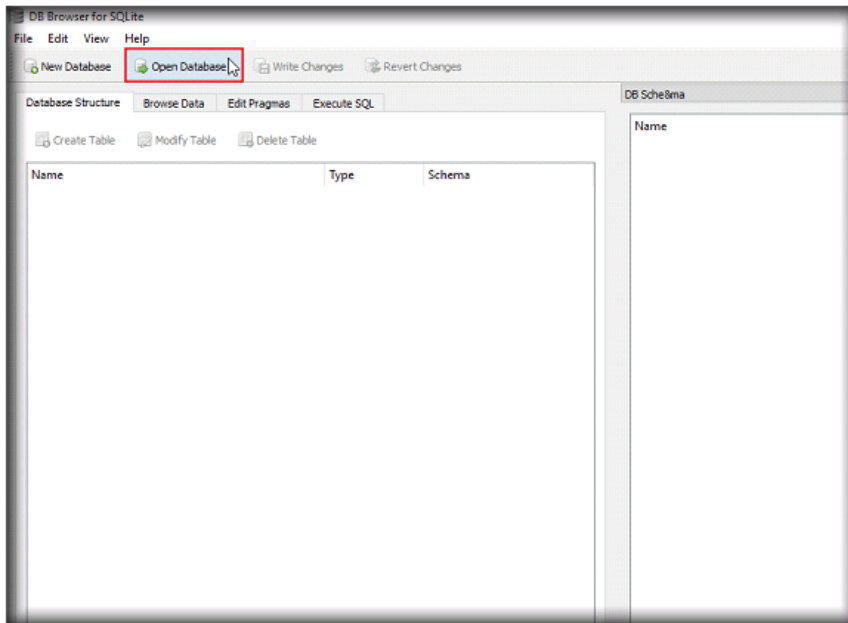


25. Other files created during installation include

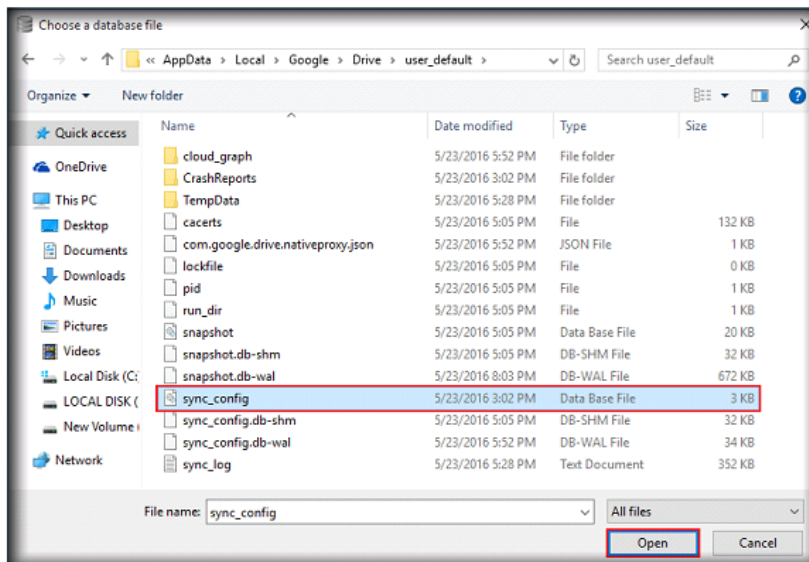
- **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Drive\Google Drive.lnk**
- **C:\Windows\Prefetch\GOOGLEDRIVESYNC.EXE-NNNNNNNN.pf**
- **C:\Windows\Prefetch\GOOGLEUPDATE.EXE-NNNNNNNN.pf**



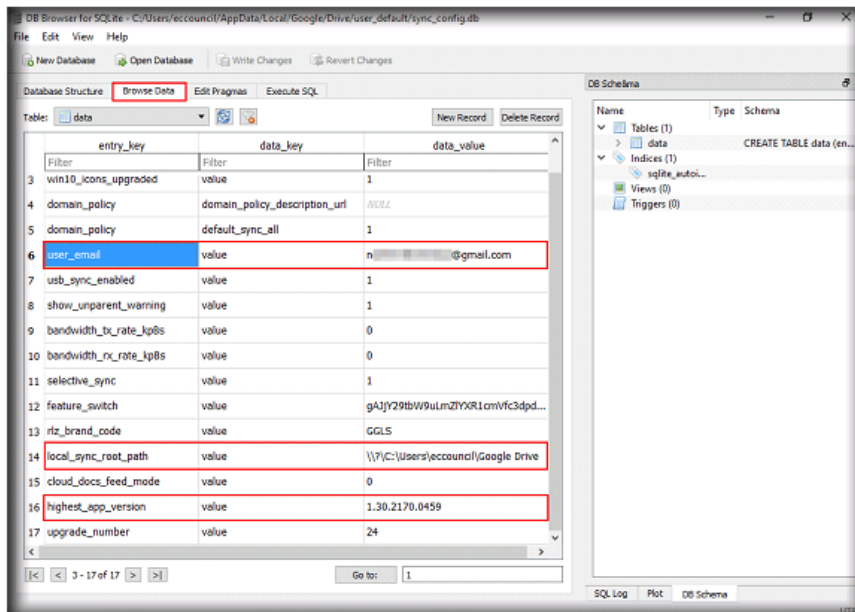
26. Run the **DB Browser for SQLite** tool and click the **Open Database** option.



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.



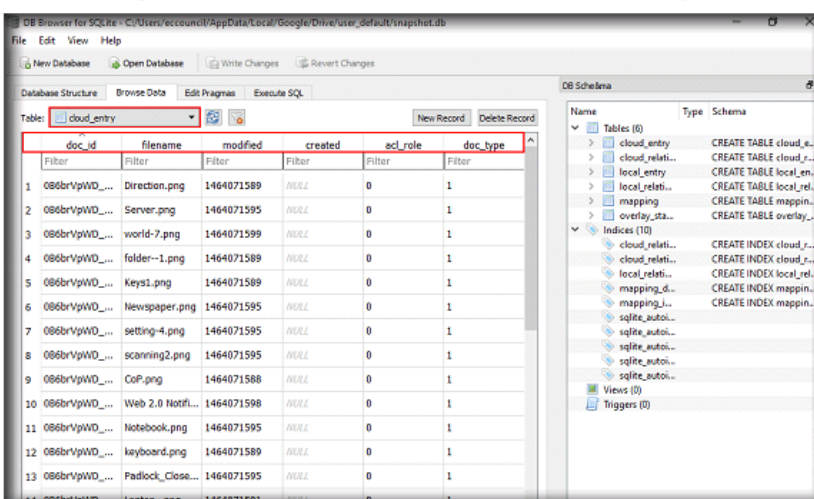
28. Click the **Browse Data** tab to view the details stored in the database file. The file stores data such as user's email address, local sync root path, and highest_app_version.



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.



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

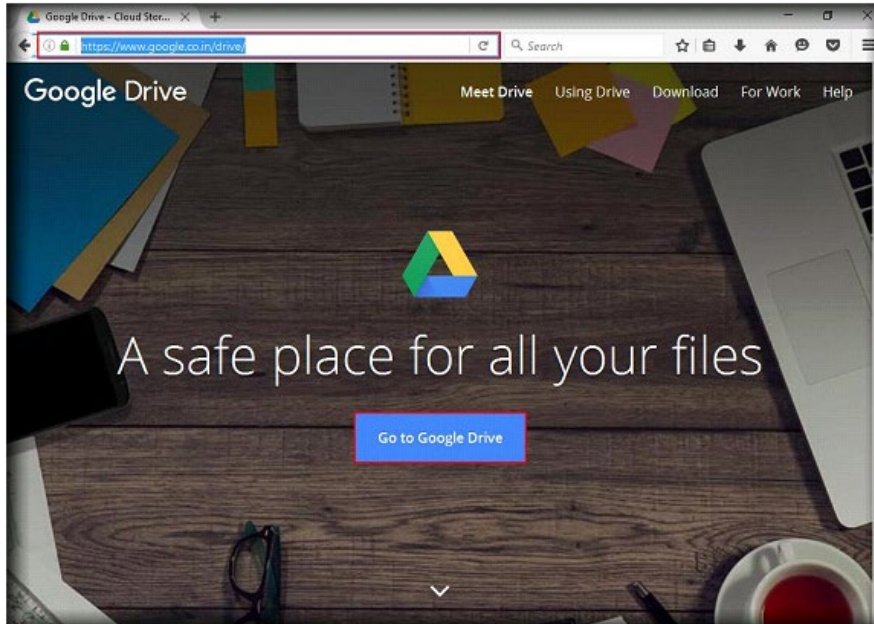
inode_number	filename	modified	checksum	size	is_folder
11258999069...	Getting started	1464004622	df1f432d0c63...	1560010	0
11258999069...	Search.png	1464071595	9641c73a79a...	99613	0
11258999069...	Scissors.png	1464071595	a06dbecb8cb...	90525	0
14073748836...	Laptop.png	1464071591	c81dcbca2f07...	76497	0
14073748836...	keyboard.png	1464071589	4f6494836062...	154729	0
14073748836...	Direction.png	1464071589	17838ef55692...	17136	0
14073748836...	folder-1.png	1464071589	11103c2704b...	2604	0
14073748836...	Whiteboard.png	1464071599	9d0727d6770...	28599	0
14073748836...	world-7.png	1464071599	f49bfa7353ca...	44462	0
14073748836...	Wireless_Sign...	1464071599	feed979d074d...	74403	0
14073748836...	Web 2.0 Notifi...	1464071598	c5c05340b40...	5508	0
14073748836...	Web 2.0 Notifi...	1464071595	3e87766b3ee...	215887	0

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.

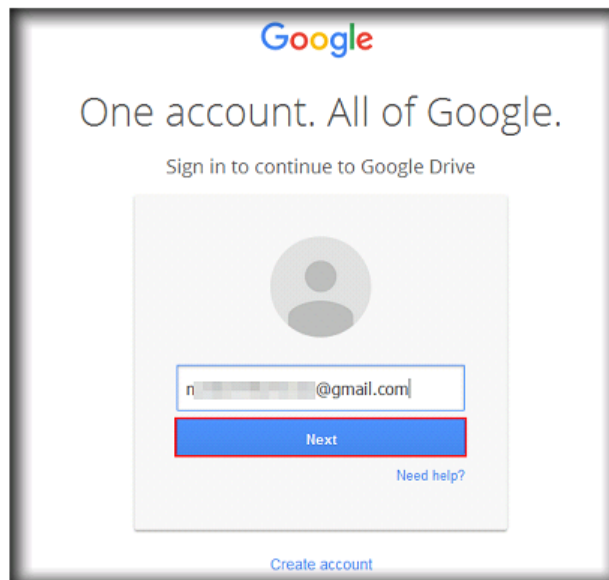
```

(sync_type: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:3ad3fcb3d454d1698f18189fa2d9dc5C:\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:
  
```

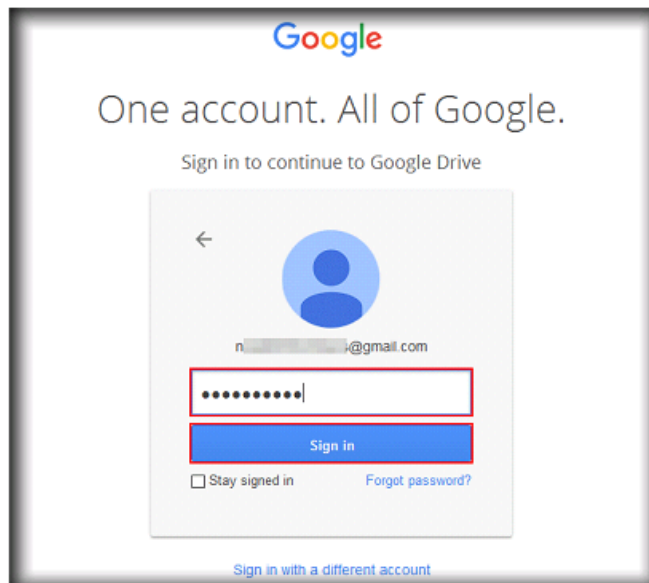
34. Open a web browser and open Google Drive home page by entering the URL **https://www.google.co.in/drive** in the address bar. Google Drive homepage appears, click **Go to Google Drive** button.



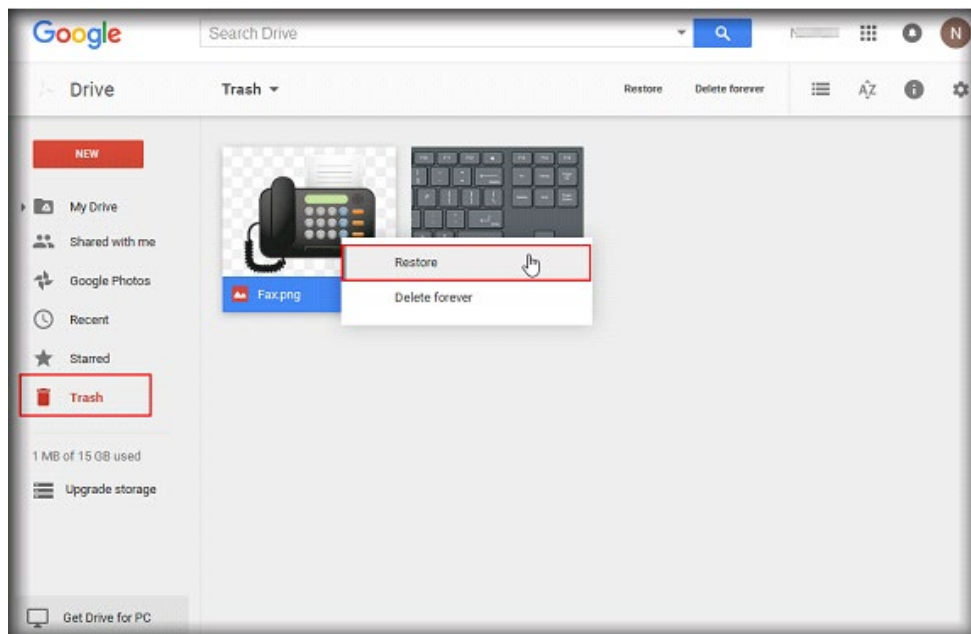
35. Enter the email ID of the Dropbox account in the provided box and click the **Next** button.



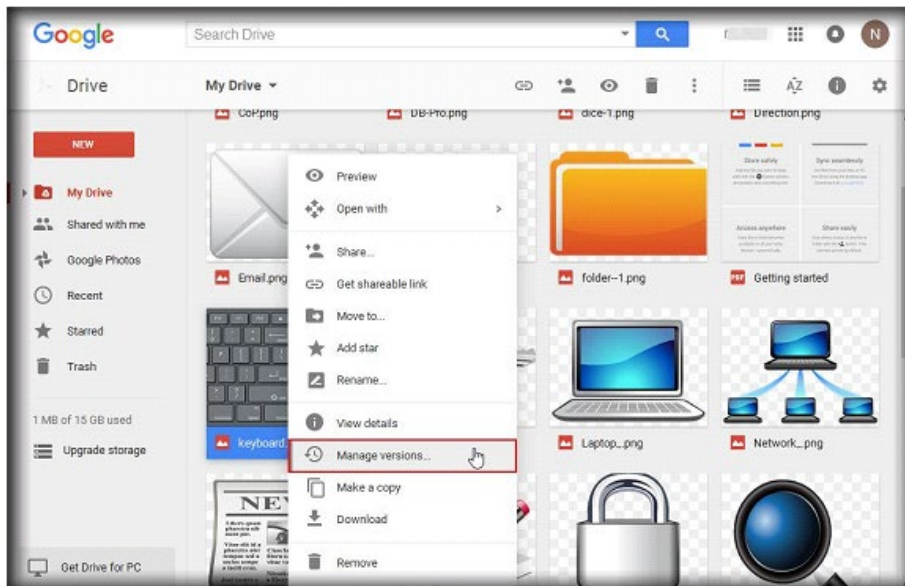
36. Enter password for the account and click the **Sign In** button.



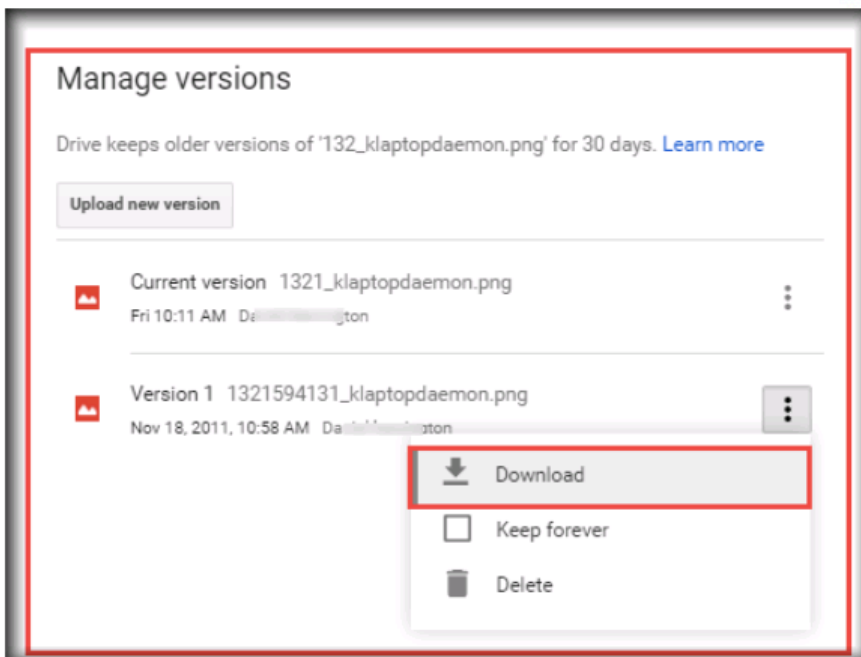
37. The browser access of a Google Drive account will help you to search for deleted files, check and manage versions of a file, view recent activity, as well as review details and activity of any file present.
38. On the homepage of a Google Drive account, click **Trash** in the left pane to view the 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**.



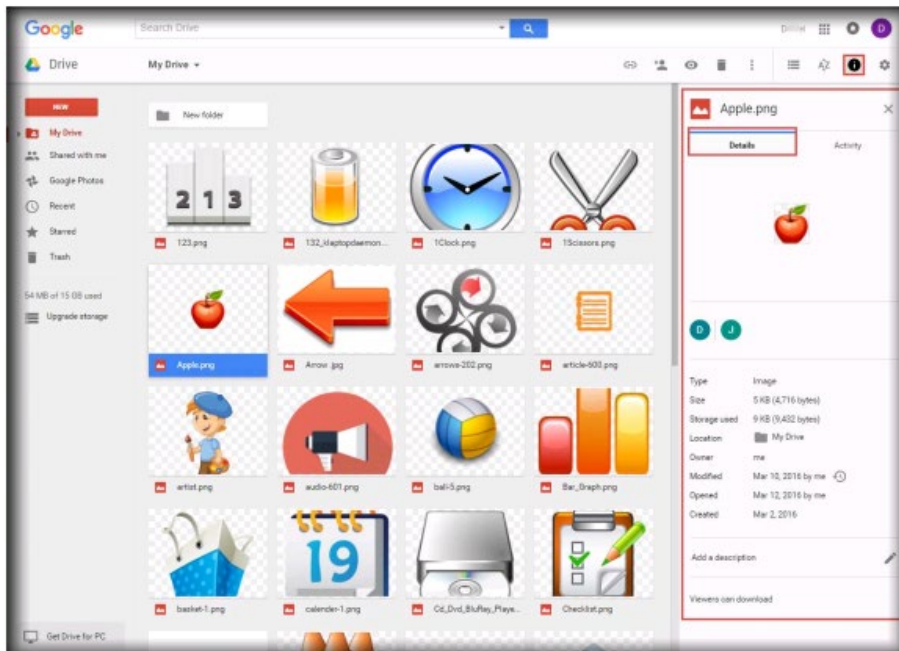
39. In the **My Drive** section, right click any image to get options and click **Manage versions...** option to see its versions.



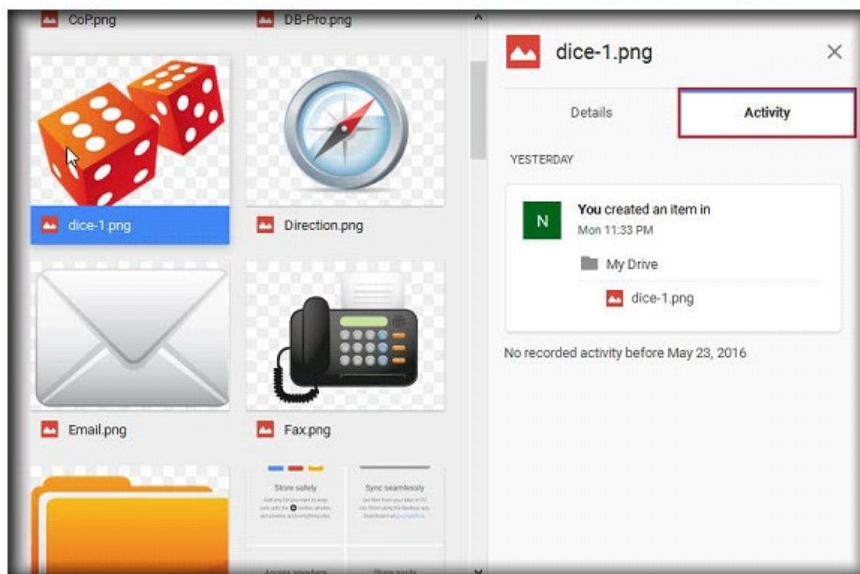
40. In the **Manage Versions** dialog box, you can click the **Ellipsis** (⋮) button related to a file from the extreme right to download the file.



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.



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



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

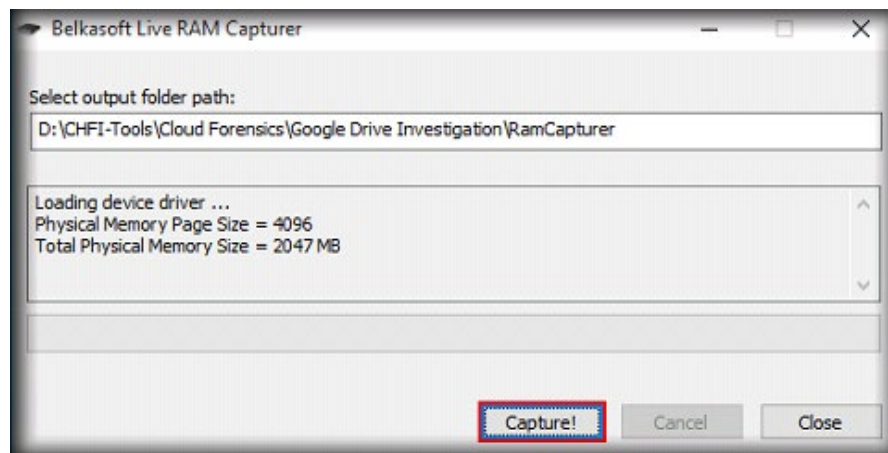


44. Now run the RAM Capturer tool. To run the tool, navigate to the location:

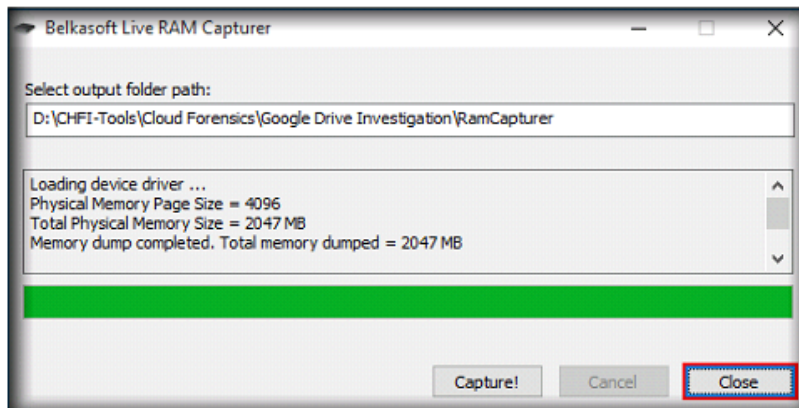
<https://uowtsd->

[my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1ggPPWOiezg?e=2vg308](https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1ggPPWOiezg?e=2vg308) for RAM Capturer and double-click **RamCapture64.exe**. RamCapture window appears, click the **Capture** button.

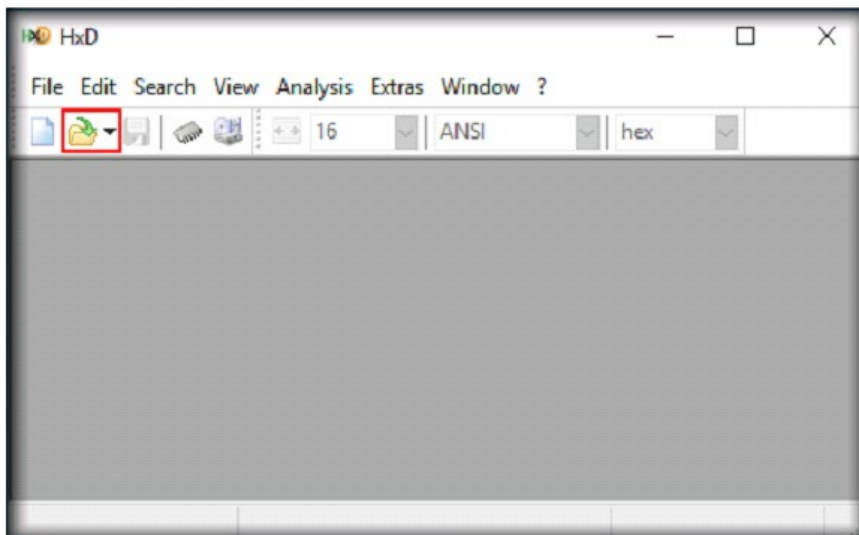
Note: If Ram Capturer displays an error while launching, copy the RAM Capturer folder located at https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1ggPPWOiezg?e=2vg308 to desktop and try running the tool.



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

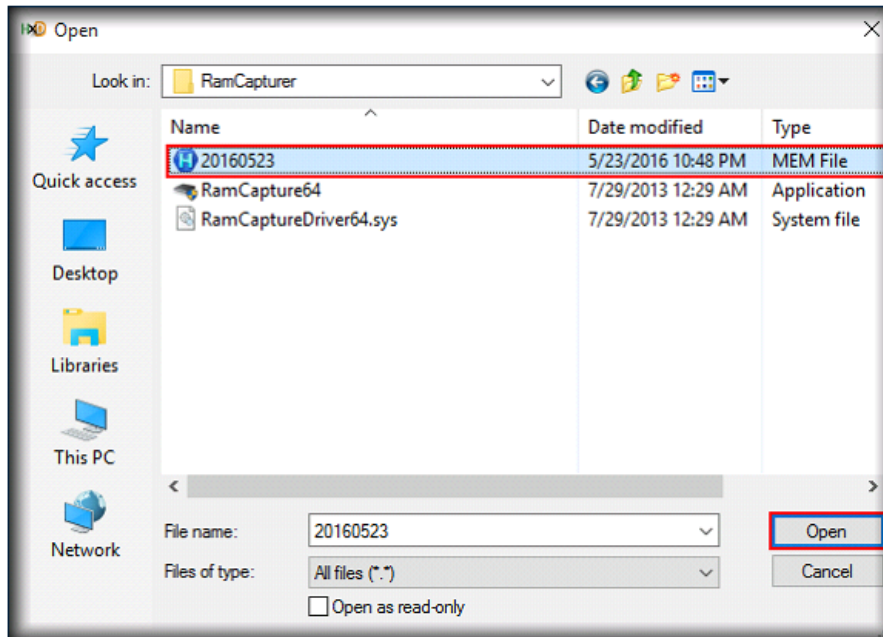


46. Run the **HxD** tool to view the Hex value of capture RAM data. Click the **Open** icon to add a file.

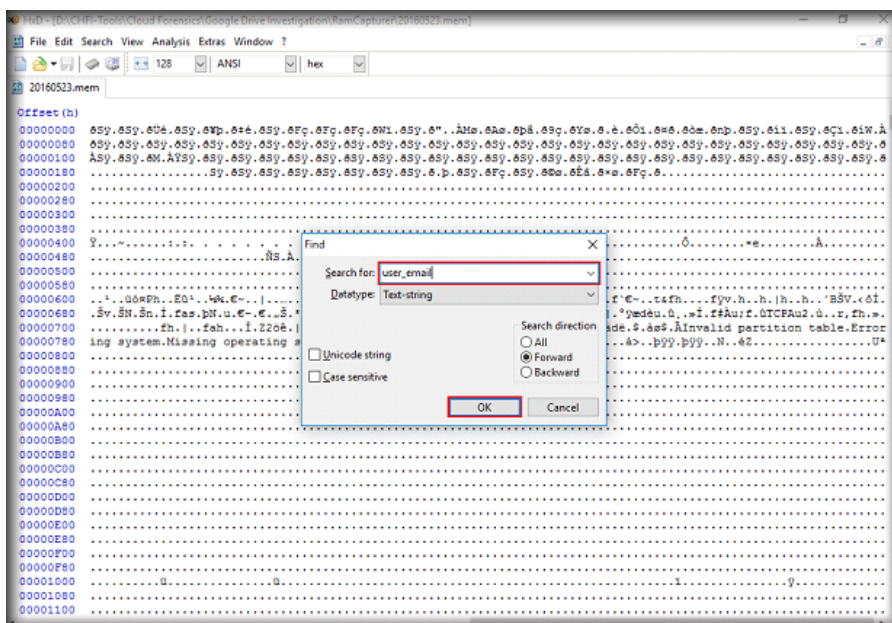


47. Navigate to https://uwotds-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwotds_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308 for RAM Capturer folder, select the captured RAM data file, and click open.

47. Navigate to the **Z:\CHFIv9 Module 10 Cloud Forensics\RAM Capturer** folder, select the captured RAM data file, and click **Open**.



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.



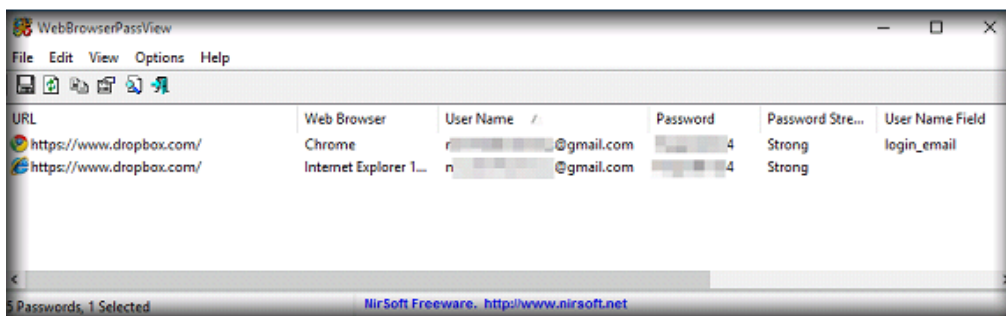
50. The tool will display data with searched string that would be having the email of the Google drive account.

```
.....9..cloud_graph_generationvalue5...5..win10_icons_upgradedvalue1...
domain_policydefault_sync_all1-...!Auser_emailvaluenowhereforensics@gmail.com
ningvalue1 ..9..bandwidth_tx_rate_kpbsvalue0 ..9..bandwidth_rx_rate_kpbsvalue
```

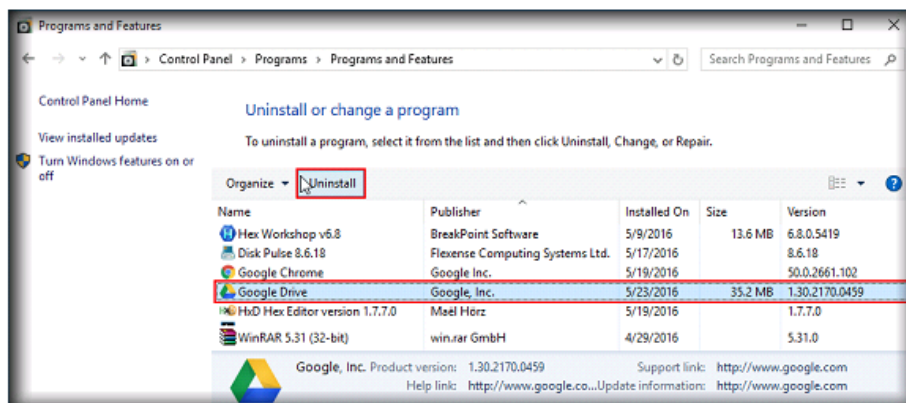
51. Similarly search for other keywords. You can find the password of the account by searching for password-related keywords such as passwd, password, etc.

```
0."8.0..."0.0..."X8,...("X..."0,.H0.h"*.u0.HX.00..x.80.(..h8
.."È..èy0.(.."X.."Y.80."È*..ä0.häx.ä8.ä..æ0.èx.c"...äX.i".è0.i0
...Èx.(i....0..0i.00i.88.Ä8.€X7gmail.comPasswd....=I4ks
ignIn=S0.+in&Persist€.entCookie=yes.Ü:#+«,"6h.t..p.s.:/"
.ÄR..c0.u.n..s...g.o.g.l.eh.cX.m8.Sh.r..ç..v.i.cH.L.i".A.u..h
qR..+...^0.ñ.0Tú0RE ..X.'æPg.0..Ä..0.Qg'*X.Ä[..X.04..X.p.».T0cT
X.....X.0.»..X..JOš.7Y.+û.8X.Pš[E².L..FX.'žVpZ¥».GX..™[.HX. 4.
I..|.JX.à4.K².4.LÜ.~Ü.Mù..[.N9.\.OÜqZÖY.ü.PX.€|.QY. {.9Y.4.<y.Y»
```

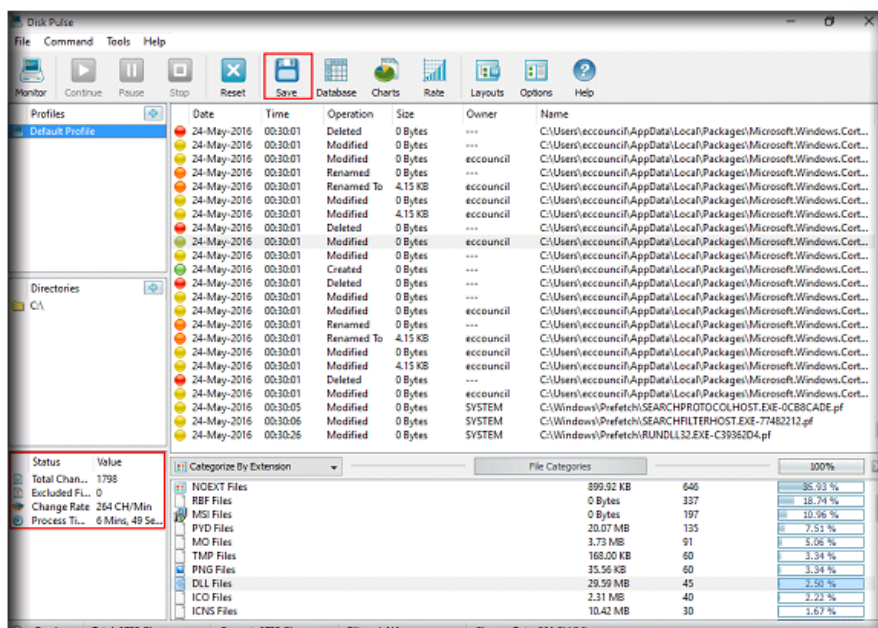
52. Run the **WebBrowserPassView** tool from https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uwtsd_ac_uk/EvUyFob-Qy9EqUxZzPha7dsBa2gnZvPs0qv1qgPPWOiezg?e=2vg308 to view the passwords when a user accesses the Google Drive account through a browser.



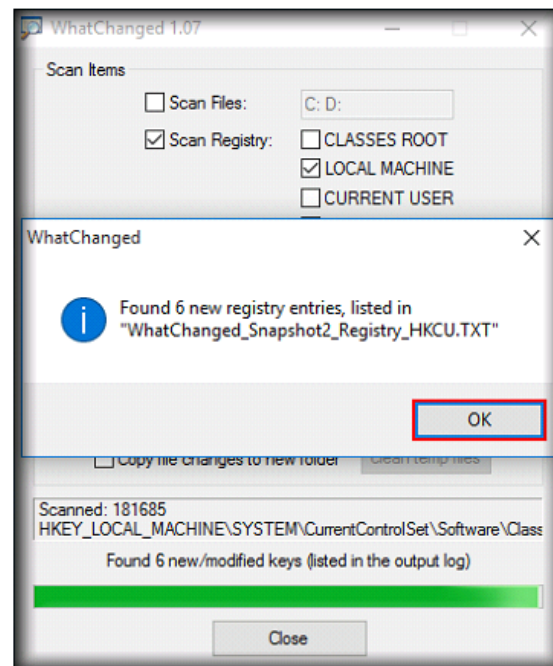
53. Run the **Disk Pulse** and **WhatChanged** tools similar to the steps above. Start the monitoring process and capture the first system snapshot.
54. Uninstall the Google Drive client to observe the artifacts it leaves behind that could help in investigation of an attack.
55. Go to **Control Panel** → 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.



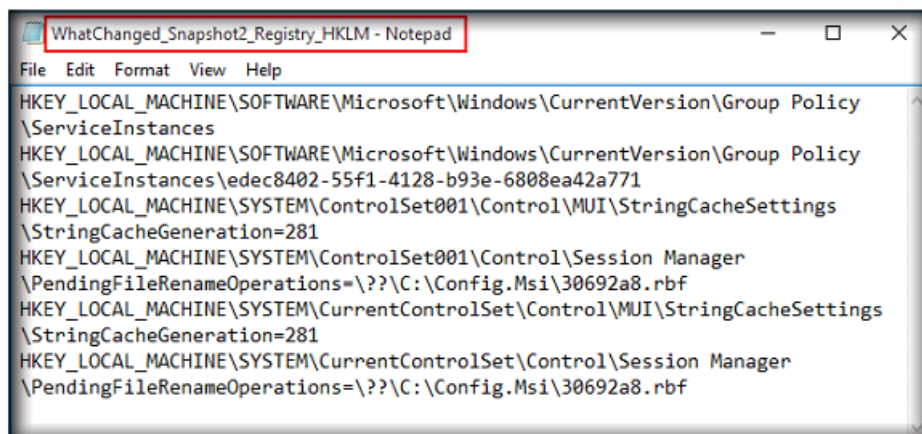
57. After uninstalling the **Google Drive** client from the system, go to the **Disk Pulse** tool and stop the process. Click the **Save** button to save the report.
58. The report will contain the list of all the files modified during the uninstallation process.



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.



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



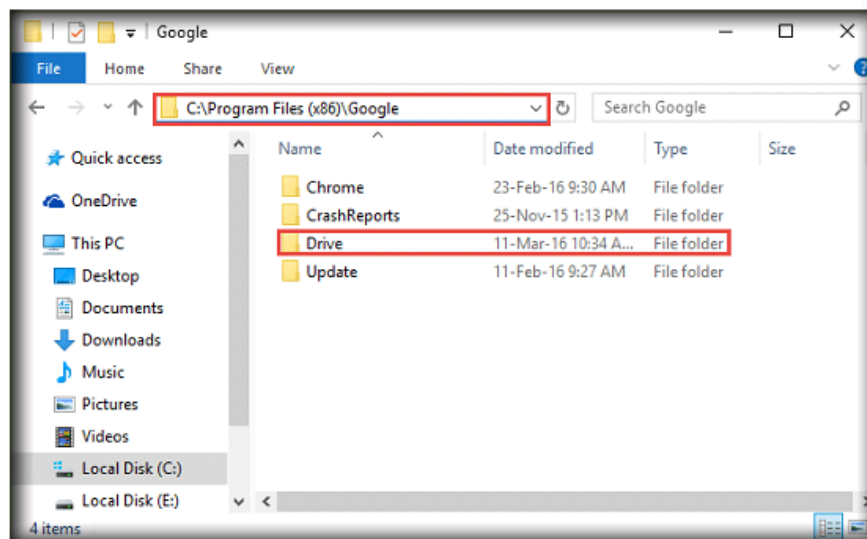
61. Uninstalling the client will result in

- Deletion of the client config folder (sync_config.db)
- Preservation of a local copy of the file as well as the Prefetch files

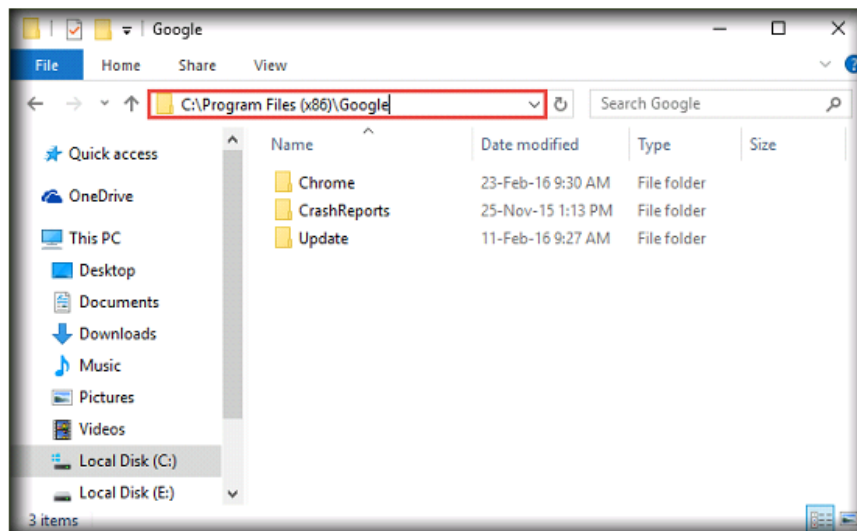
62. Other files that can help you in recovering traces or evidences of the cloud storage service include

- 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:



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



Lab Analysis

Analyze and document the results related to the lab exercise.