

DROPBOX AND GOOGLE DRIVE INVESTIGATION

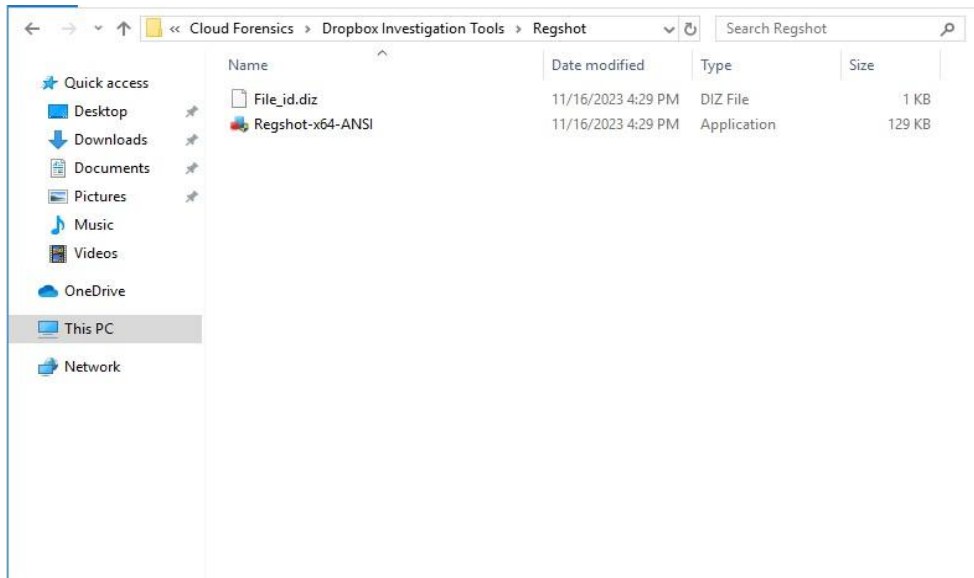
By



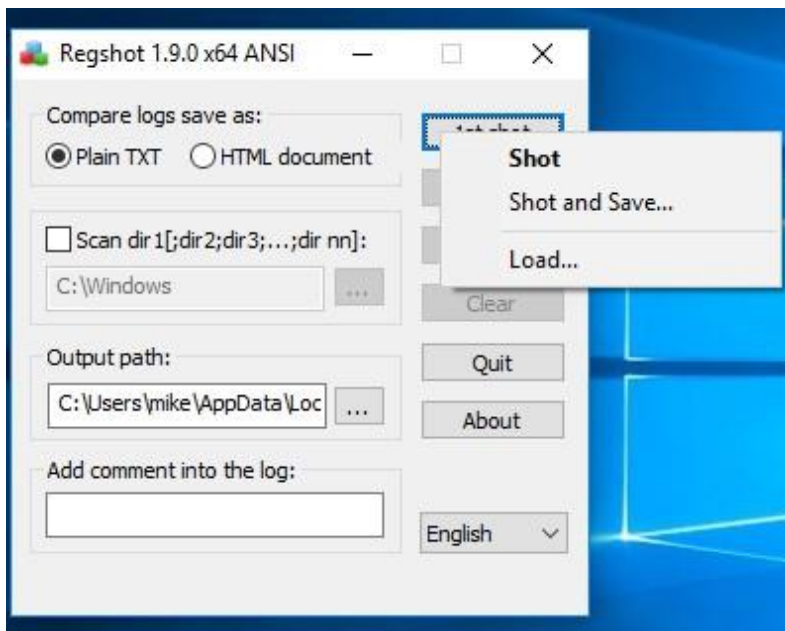
DEWTON KIPROP

DROPBOX INVESTIGATION

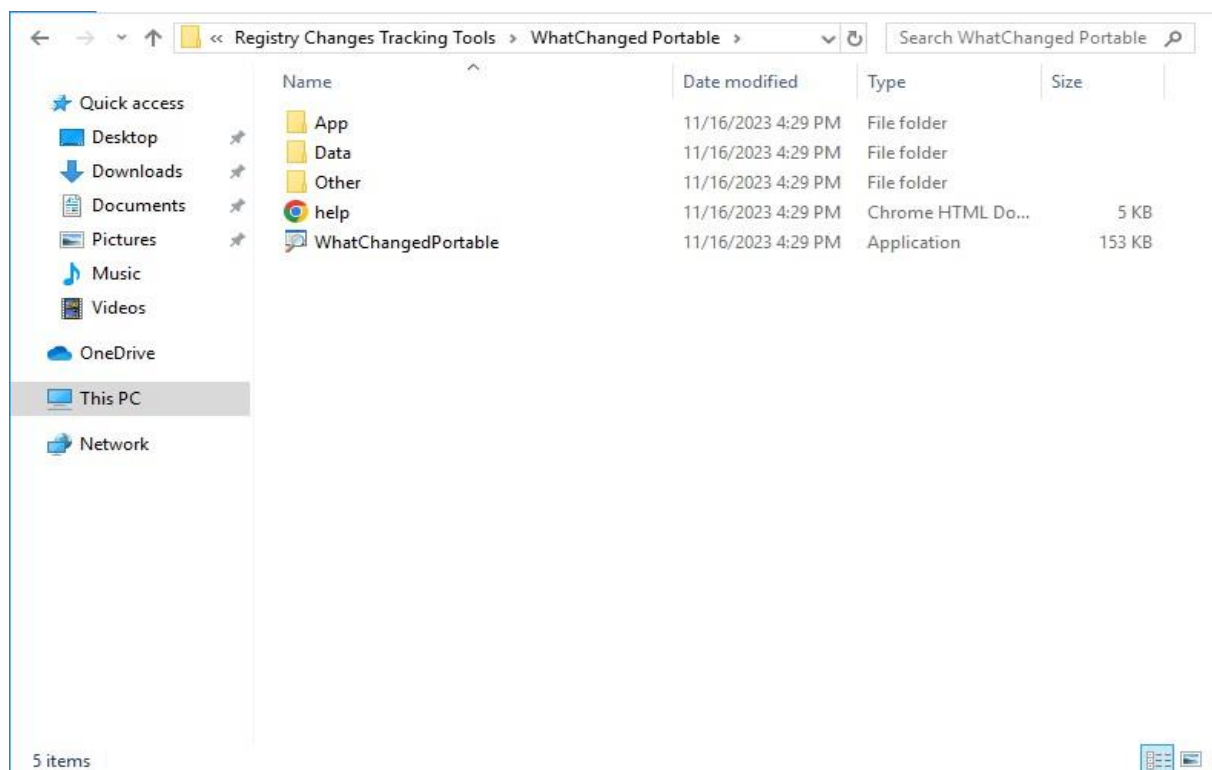
- **Navigate to the folder and double click the .exe file for the Regshot to launch the application.**



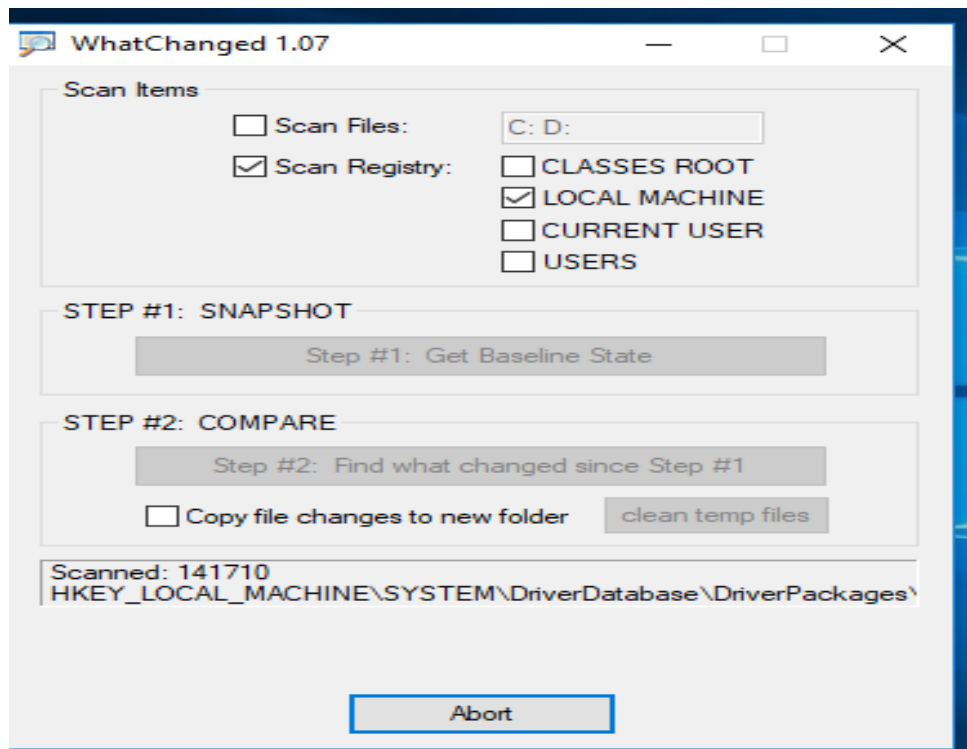
- **Once launched the window below is displayed, click on 1st shot then from the drop down click on shot.**



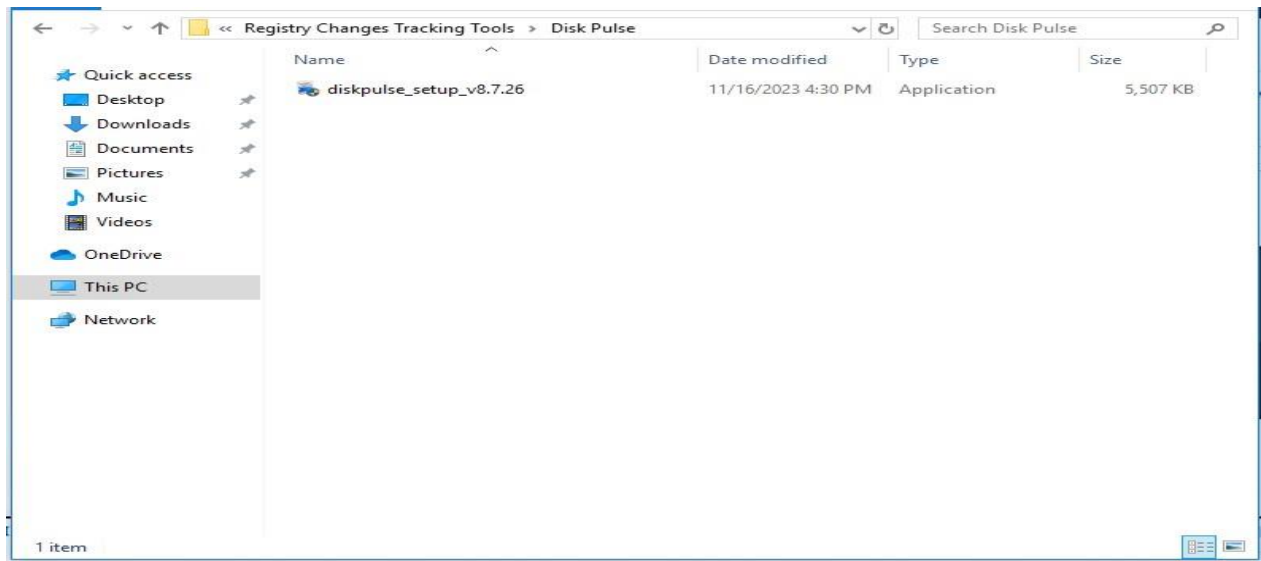
- **Navigate to the folder containing the WhatChangedPortable and double click the .exe file to launch it.**



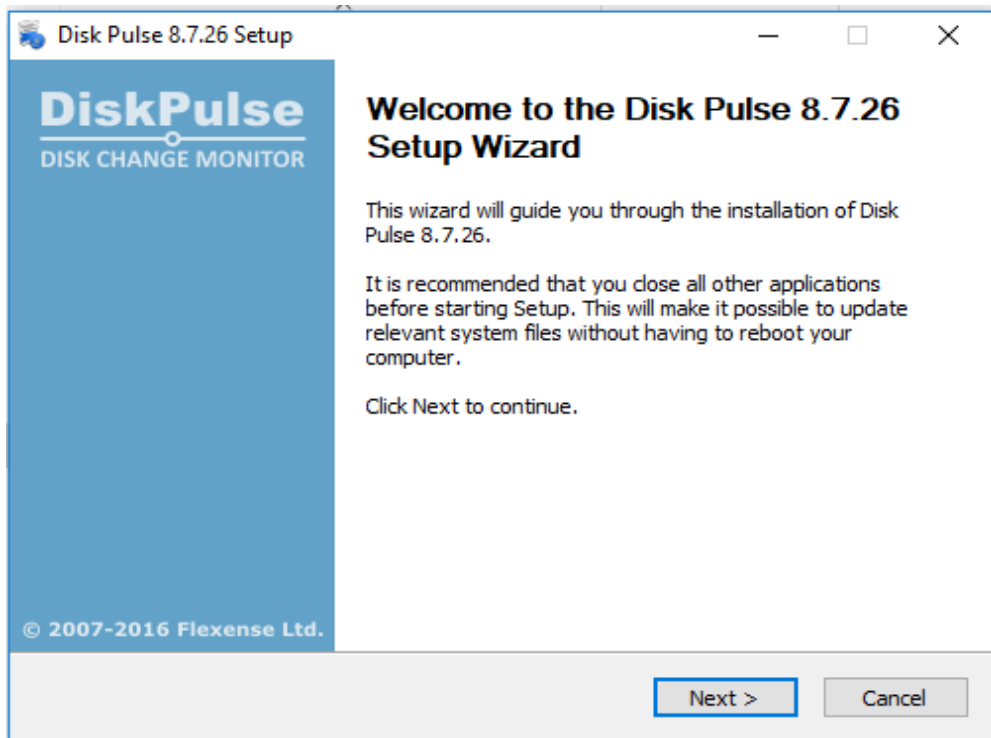
- Once *WhatChangedPortable* has launched as below, check the boxes for *scan registry* and *LOCAL MACHINE*. Click on *step #1: SNAPSHOT*.



- Navigate to the folder containing the Disk pulse executable, double click to launch it.

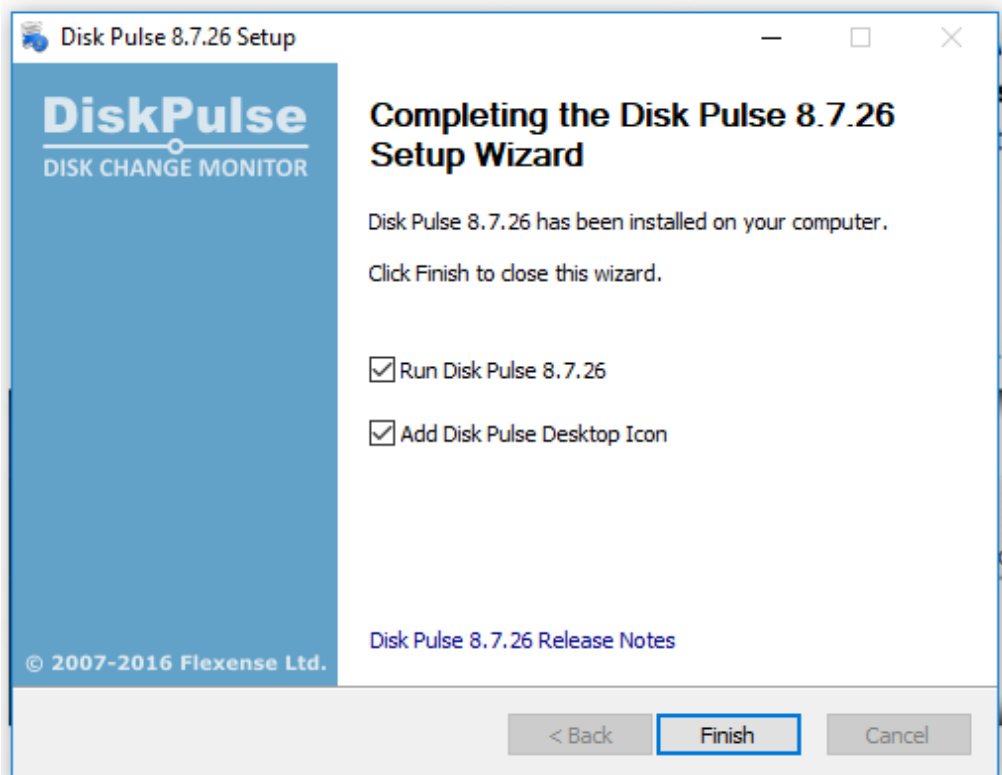


- The following wizard is displayed.

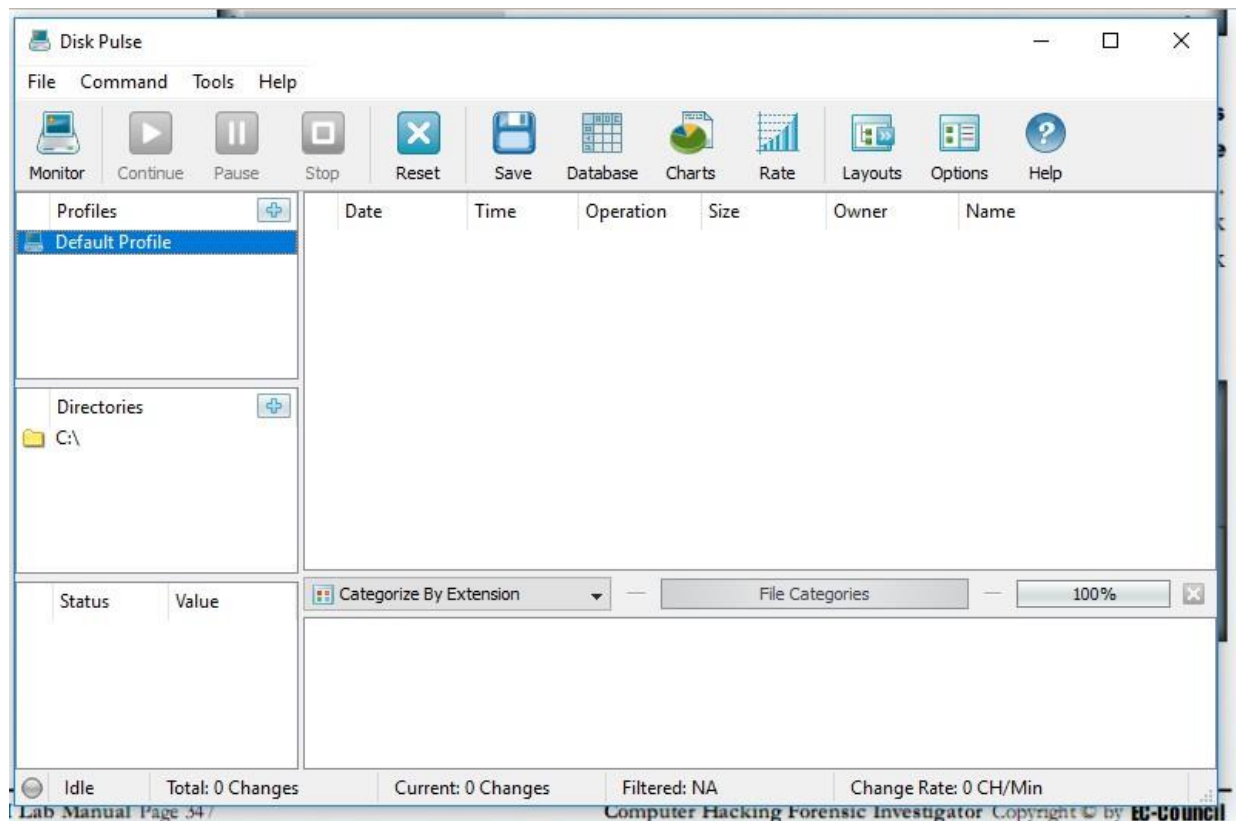


- Check the boxes for the *Run Disk Pulse* and *Add Disk Pulse Desktop icon* before clicking on the finish.

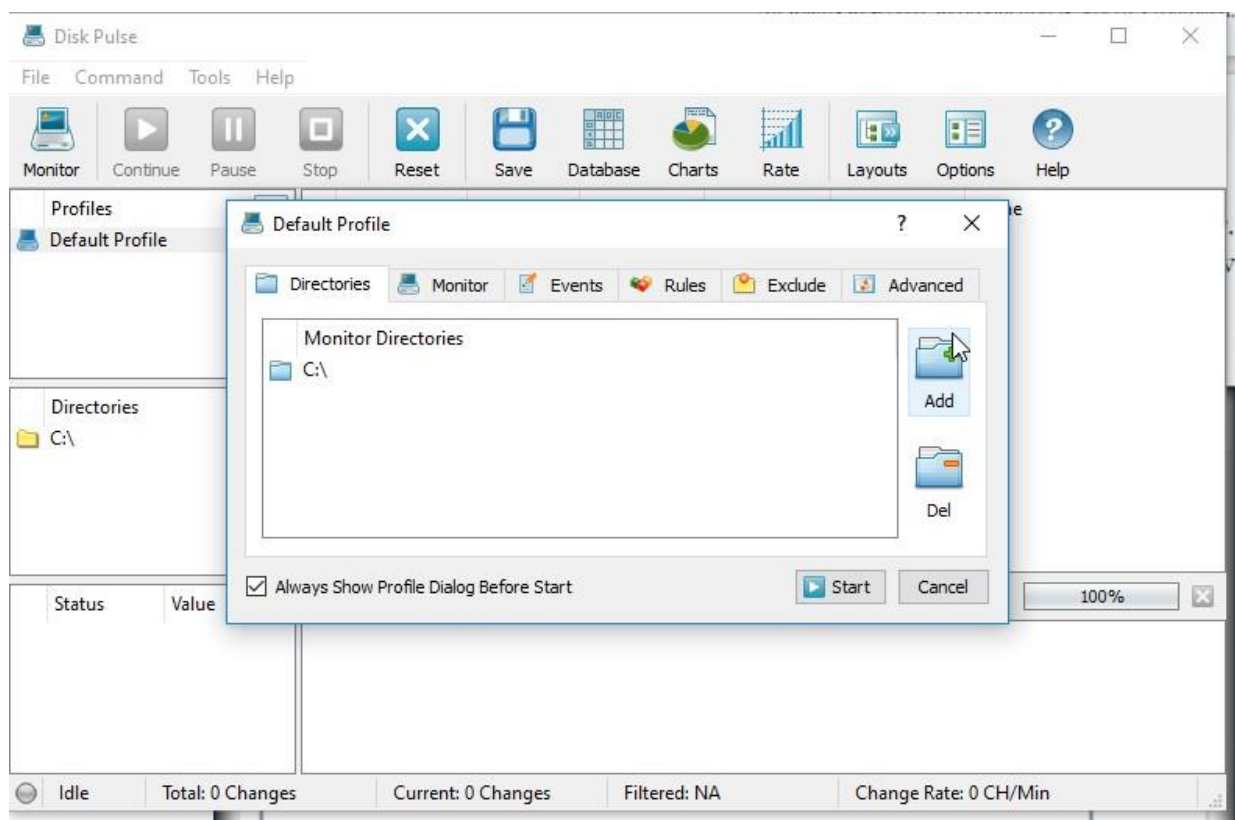
FIGURE 1.3: Notepad file containing all the local machine addresses



- Disk Pulse graphical user interface is displayed as below once launched.



- Click on the monitor tab and click on Add to add a directory. Otherwise C:\ is added by default. Select start.



- Once the start button is clicked, the following is displayed.

The screenshot displays the Disk Pulse application window. The interface includes a menu bar (File, Home, Share, View, Manage), a toolbar with buttons for Monitor, Continue, Pause, Stop, Reset, Save, Database, Charts, Rate, Layouts, Options, and Help. The main area is divided into three sections: Profiles, Directories, and a central table of file operations.

Profiles: Default Profile

Directories: C:\

Date	Time	Operation	Size	Owner	Name
17-Nov-2023	10:41:34	Modified	0 Bytes	mike	C:\Users\mike\AppData\...
17-Nov-2023	10:41:35	Modified	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:35	Created	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:35	Modified	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:35	Created	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:35	Modified	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:36	Modified	973 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:36	Created	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:36	Modified	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:36	Created	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:36	Modified	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:37	Created	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:37	Modified	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...

File Categories:

Category	Size	Count	Percentage
NOEXT Files	30.67 KB	53	75.71 %
TMP Files	30.67 KB	8	11.43 %
PIECESHASH Files	2.16 KB	4	5.71 %
DLL Files	2.55 MB	4	5.71 %
DB Files	12.59 KB	1	1.43 %

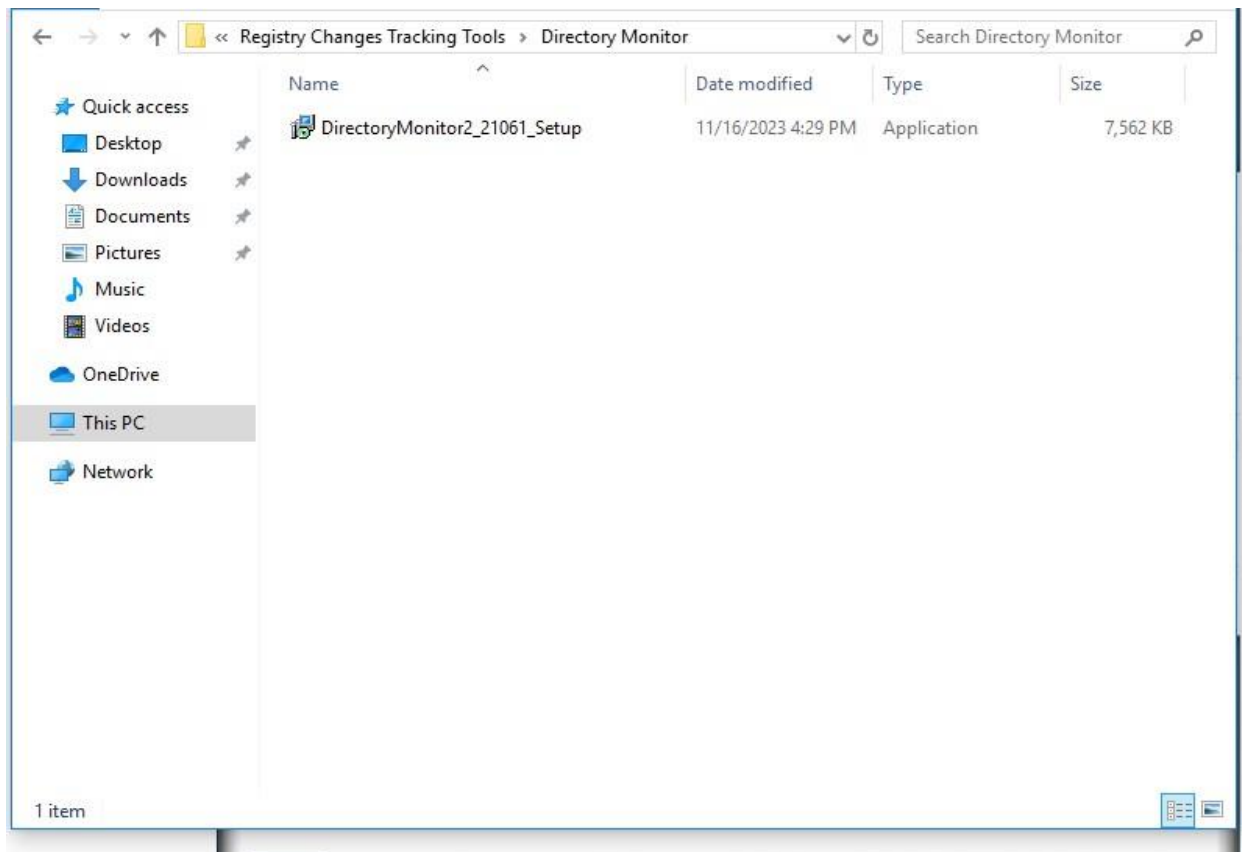
Status Summary:

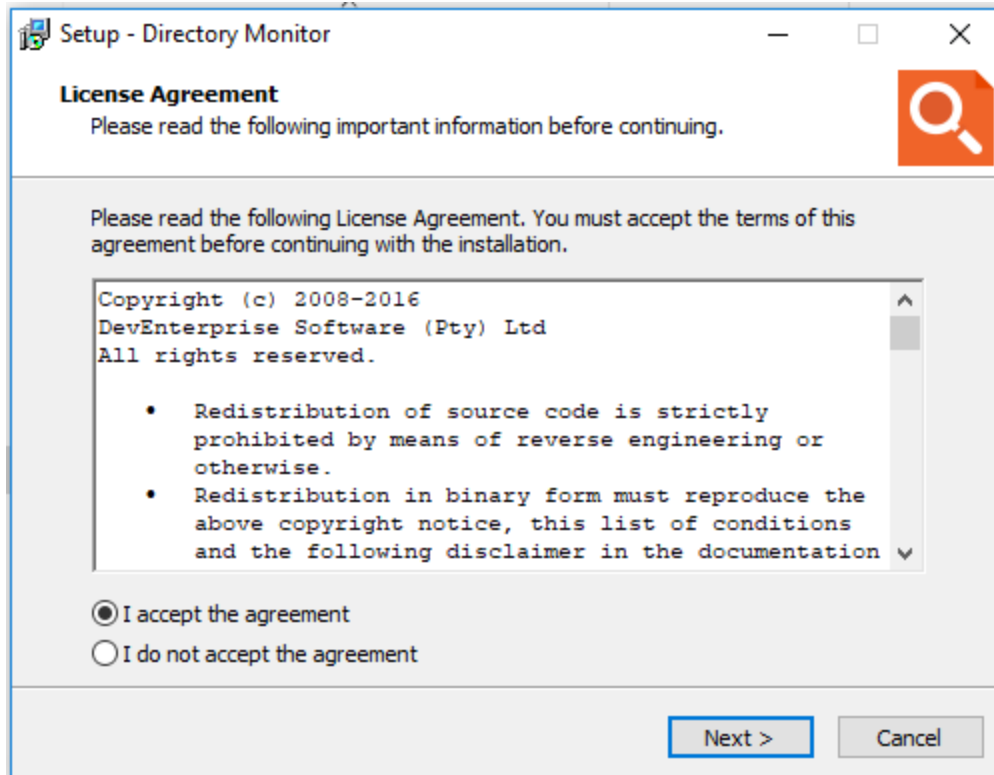
Status	Value
Total Chan...	66
Excluded Fi...	0
Change Rate	474 CH/Min
Process Ti...	8.36 Sec

Bottom Bar: Active | Total: 66 Changes | Current: 66 Changes | Filtered: NA | Change Rate: 474 CH/Min

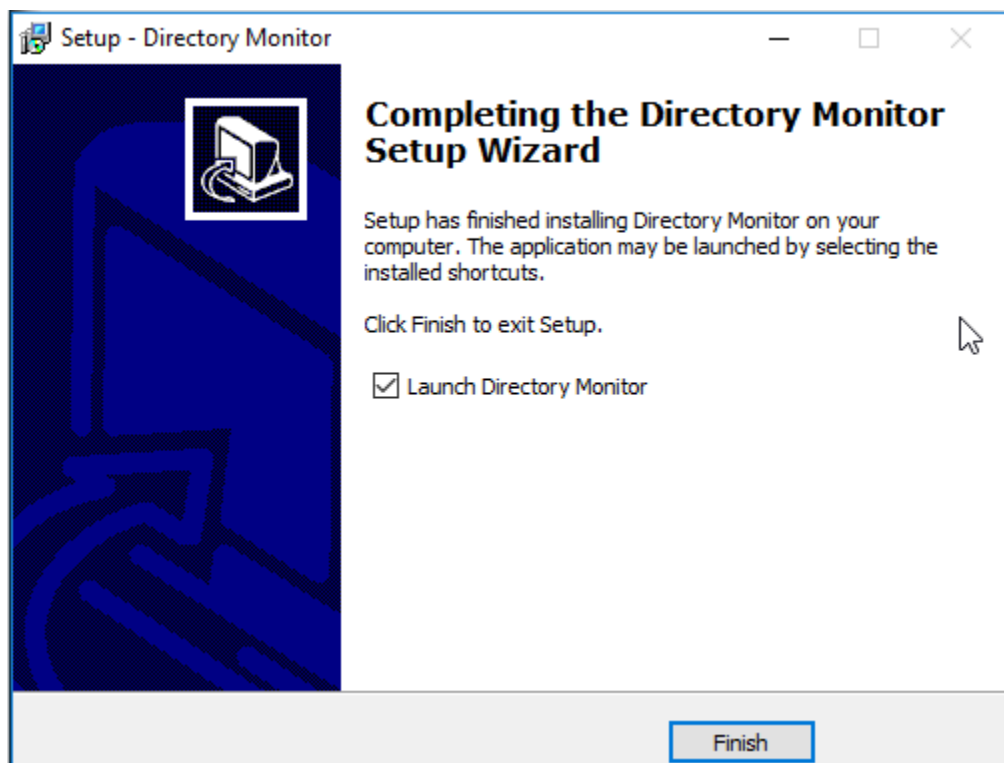
1 item | 1 item selected 5.37 MB

- **Navigate to the folder containing the Directory Monitor set up executable file and double click the file to launch as set up wizard for the Directory monitor tool.**

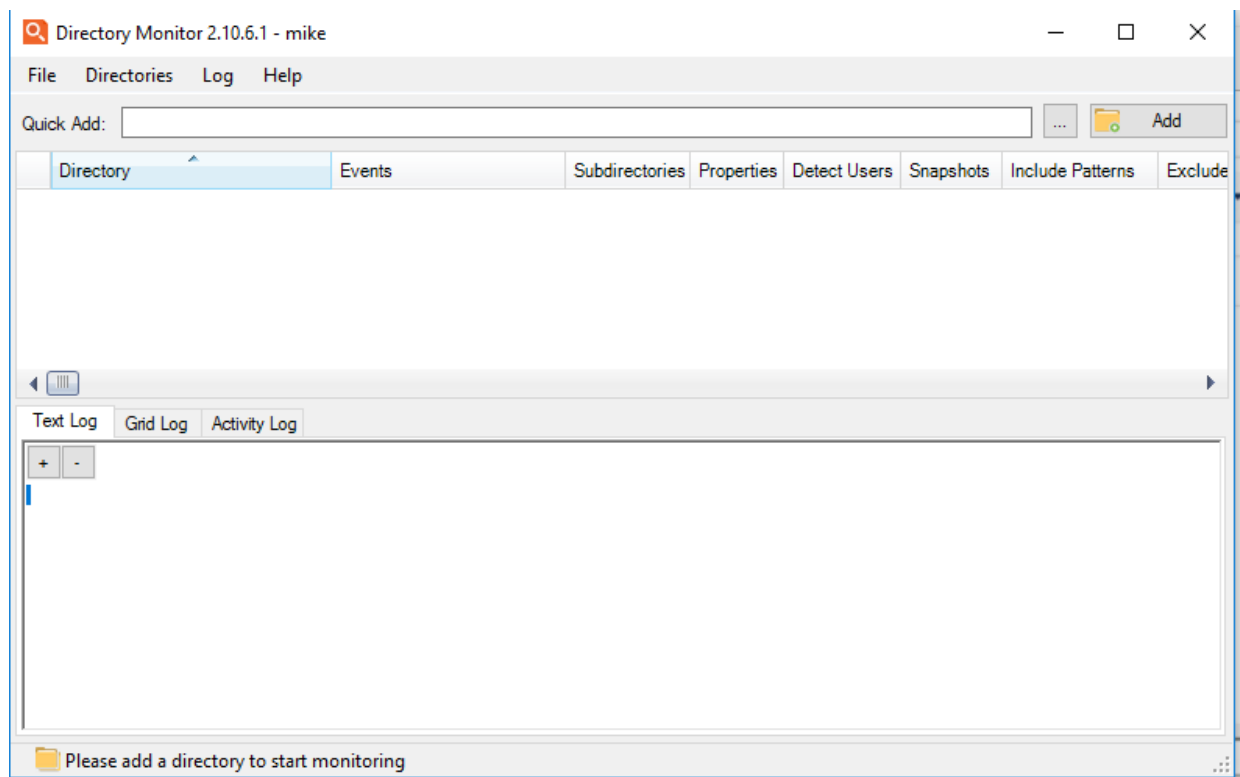




- Follow the wizard below.



- The GUI for the Directory Monitor tool is displayed below.



- The window below is displayed once you click on Add.

The image shows a configuration window for monitoring a directory. It is divided into three main sections: Directory, Options, and Filters.

Directory Section:

- Directory:** A text input field with a browse button (three dots) to its right.
- Username:** A text input field.
- Password:** A text input field.
- Description:** A text area with up and down arrow buttons on the right side.

Options Section:

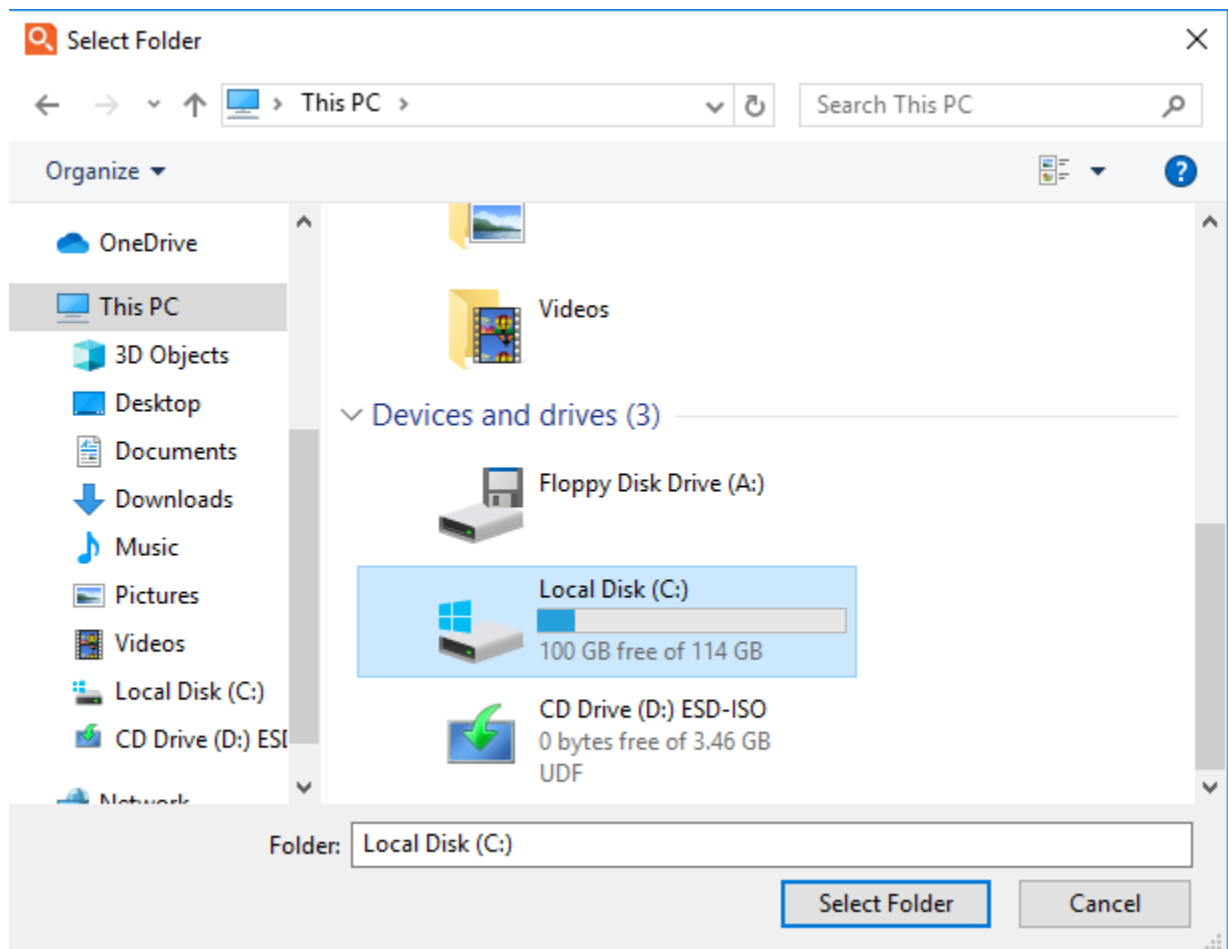
- Events:** A row of checkboxes: ☒ New Files, ☐ Modifications, ☐ Deletions, ☐ Renames, ☐ File Access, and a help icon.
- Options:** ☒ Monitor events of subdirectories, ☐ Monitor changes to attributes and security settings.
- ☒ Try get the user and process information that made the change (with a help icon).
- ☒ Try determine changes while directory was offline using snapshots every minute(s).
- Types:** ☒ Directories and Files, ☐ Files only, ☐ Directories only.

Filters Section:

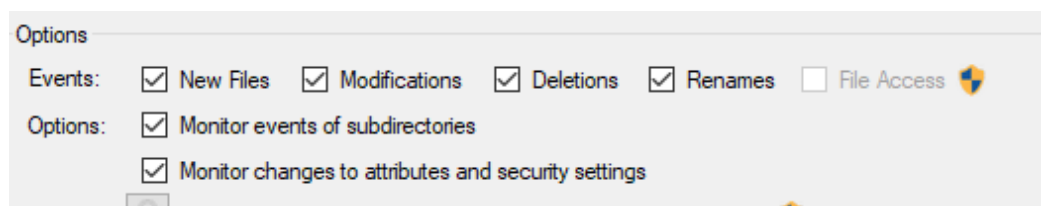
- Exclude patterns:** A large empty text area with a vertical scrollbar and horizontal scroll arrows at the bottom.
- Include patterns:** A large empty text area with a vertical scrollbar and horizontal scroll arrows at the bottom.

Buttons: At the bottom of the window are two buttons: "Save" and "Cancel".

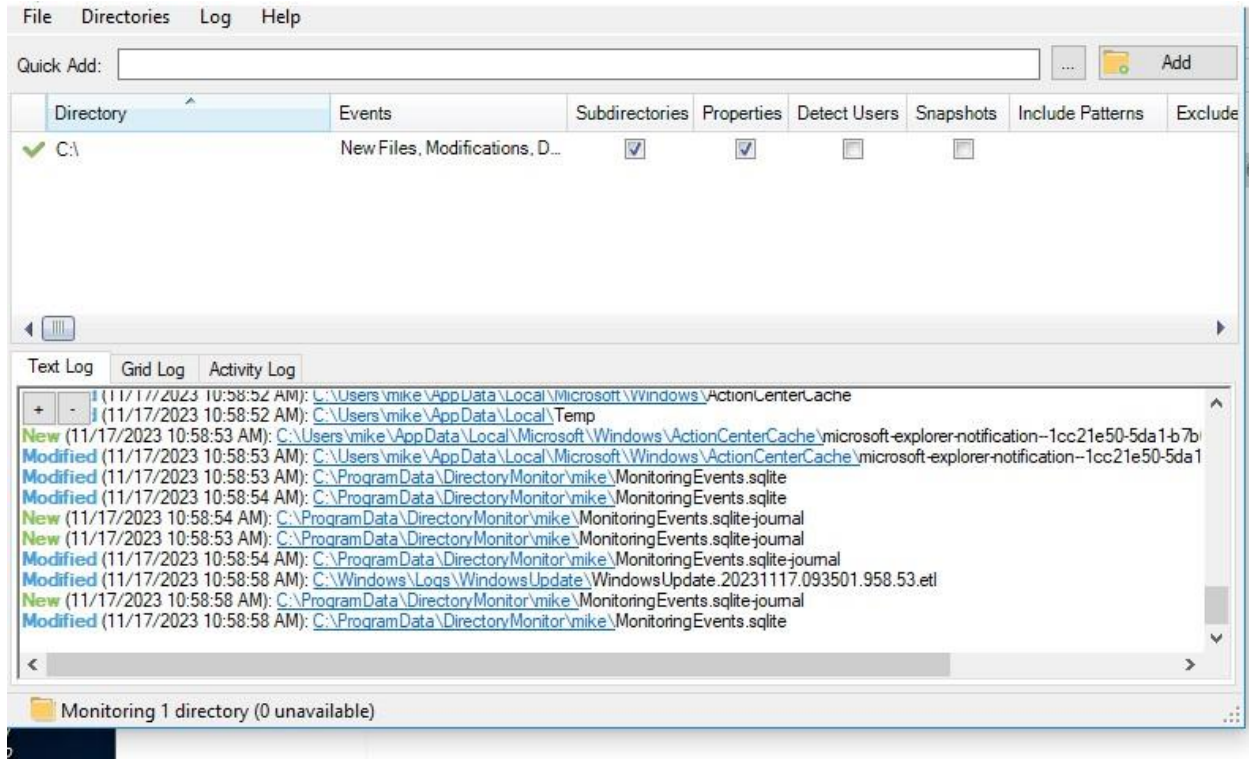
- Select the C:\ and click on select folder.



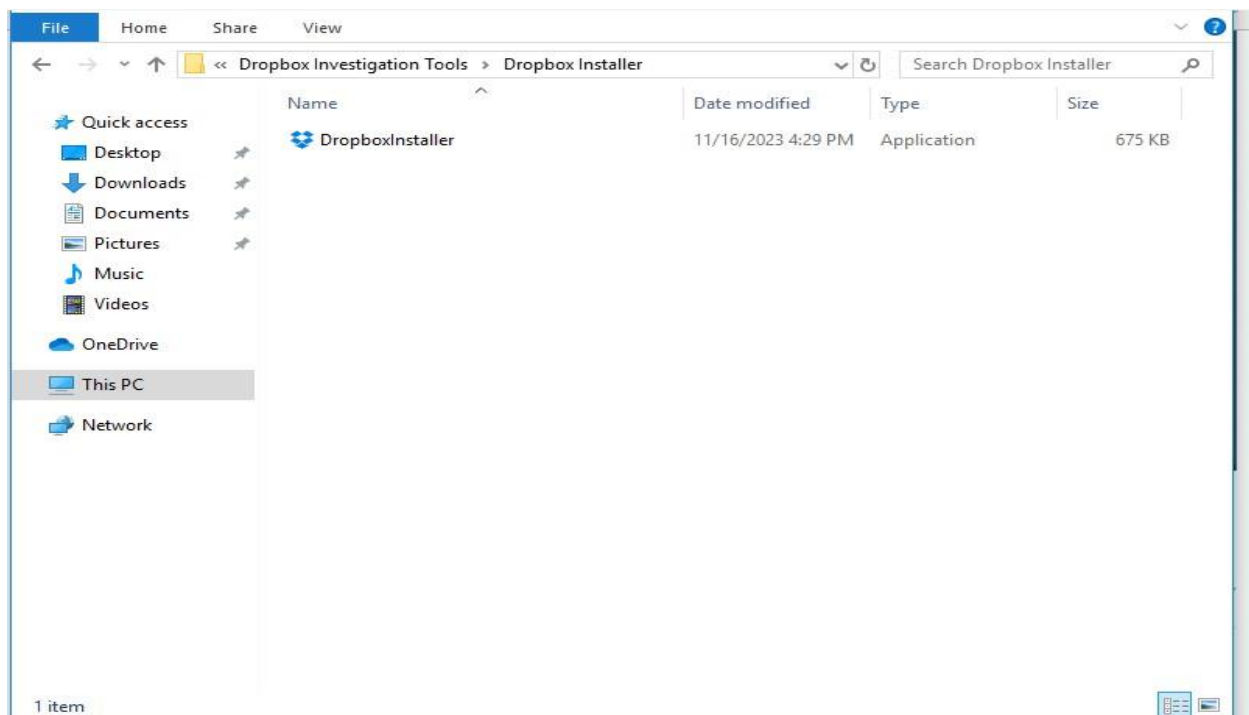
- Check the boxes in the options section for the events and options.

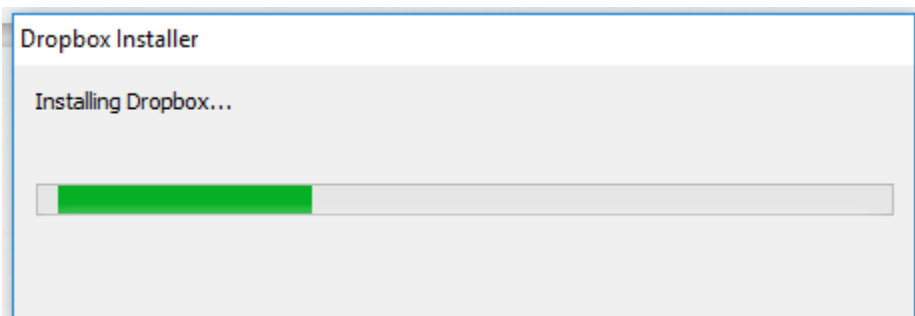


- Once you select the directory, monitoring is initiated as below.

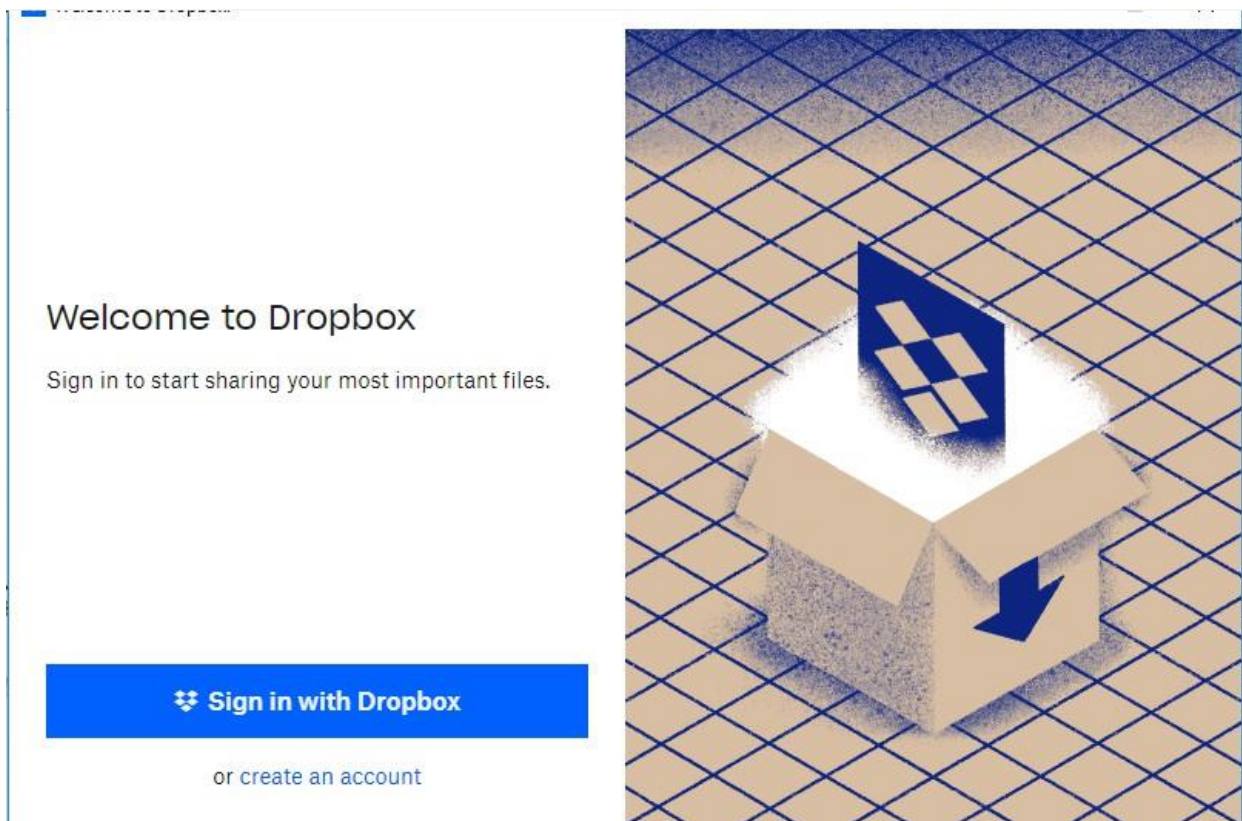


- To install Dropbox, navigate to the folder containing the Dropbox installer.





- **Sign into Dropbox.**



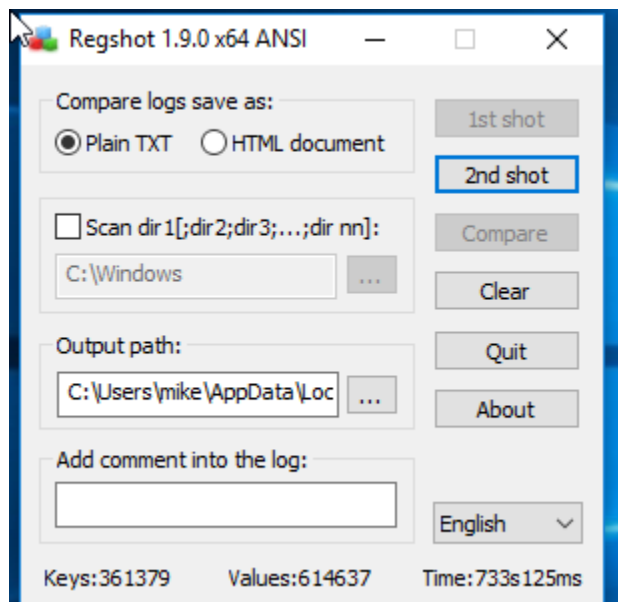
- Once signed in Dropbox, pause the Disk Pulse.

	Pause	Stop	Reset	Save	Database	Charts	Rate	Layouts	Options	Help
	+									
		Date	Time	Operation	Size	Owner	Name			
		17-Nov-2023	12:36:41	Deleted	0 Bytes	---	C:\ProgramData\Directo...			
		17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\ProgramData\Directo...			
		17-Nov-2023	12:36:41	Created	8.52 KB	mike	C:\ProgramData\Directo...			
		17-Nov-2023	12:36:41	Modified	8.52 KB	mike	C:\ProgramData\Directo...			
		17-Nov-2023	12:36:41	Modified	3.00 MB	mike	C:\ProgramData\Directo...			
		17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\Users\mike\AppData\...			
		17-Nov-2023	12:36:41	Modified	245.94 KB	mike	C:\Users\mike\AppData\...			
		17-Nov-2023	12:36:41	Created	0 Bytes	---	C:\Users\mike\AppData\...			
		17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\Users\mike\AppData\...			
		17-Nov-2023	12:36:41	Modified	0 Bytes	---	C:\Users\mike\AppData\...			
		17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\Users\mike\AppData\...			
		17-Nov-2023	12:36:41	Created	0 Bytes	---	C:\Users\mike\AppData\...			
		17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\Users\mike\AppData\...			

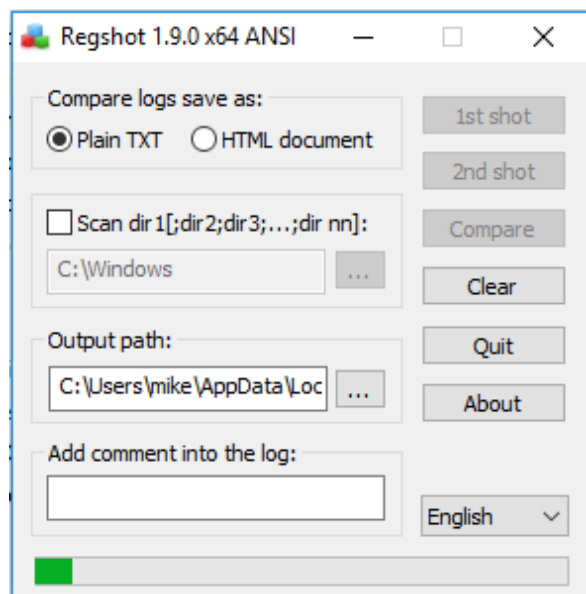
- Select all changes and copy them to a text file for easier analysis.

File	Machine	View	Input	Devices	Help
17-Nov-2023	12:36:30	Modified	3.00 MB	mike	C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite
17-Nov-2023	12:36:30	Modified	0 Bytes	mike	C:\ProgramData\DirectoryMonitor\mike
17-Nov-2023	12:36:30	Modified	0 Bytes	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\
17-Nov-2023	12:36:30	Modified	28.00 KB	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\
17-Nov-2023	12:36:30	Modified	0 Bytes	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\
17-Nov-2023	12:36:30	Modified	323.32 KB	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\
17-Nov-2023	12:36:30	Modified	0 Bytes	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\
17-Nov-2023	12:36:30	Modified	48.00 KB	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\
17-Nov-2023	12:36:30	Modified	0 Bytes	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\
17-Nov-2023	12:36:30	Deleted	0 Bytes	---	C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
17-Nov-2023	12:36:30	Modified	0 Bytes	mike	C:\ProgramData\DirectoryMonitor\mike
17-Nov-2023	12:36:30	Created	8.52 KB	mike	C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
17-Nov-2023	12:36:30	Modified	0 Bytes	---	C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
17-Nov-2023	12:36:30	Modified	0 Bytes	mike	C:\ProgramData\DirectoryMonitor\mike
17-Nov-2023	12:36:30	Created	0 Bytes	---	C:\Users\mike\AppData\Local\Temp\{73454A84-0C5C-4BB3-8AE0-A883599D443}
17-Nov-2023	12:36:30	Modified	0 Bytes	---	C:\Users\mike\AppData\Local\Temp\{73454A84-0C5C-4BB3-8AE0-A88}
17-Nov-2023	12:36:39	Created	2.01 KB	mike	C:\Users\mike\AppData\Local\Microsoft\OneDrive\logs\Personal\FileCoAu
17-Nov-2023	12:36:41	Modified	2.01 KB	mike	C:\Users\mike\AppData\Local\Microsoft\OneDrive\logs\Personal\
17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\Users\mike\AppData\Local\Microsoft\OneDrive\logs\Personal\
17-Nov-2023	12:36:41	Modified	8.52 KB	mike	C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
17-Nov-2023	12:36:41	Deleted	0 Bytes	---	C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\ProgramData\DirectoryMonitor\mike
17-Nov-2023	12:36:41	Created	8.52 KB	mike	C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
17-Nov-2023	12:36:41	Modified	8.52 KB	mike	C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
17-Nov-2023	12:36:41	Modified	3.00 MB	mike	C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\H
17-Nov-2023	12:36:41	Modified	245.94 KB	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\H
17-Nov-2023	12:36:41	Created	0 Bytes	---	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\Network\4
17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\Network\4
17-Nov-2023	12:36:41	Modified	0 Bytes	---	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\Network\4
17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\Network\4
17-Nov-2023	12:36:41	Created	0 Bytes	---	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\Network\4
17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\Network\4

- Launch the already running Regshot and take a 2nd shot.



- Click on compare.



WhatChanged 1.07

Scan Items

☐ Scan Files: C: D:

☒ Scan Registry: ☐ CLASSES ROOT

☒ LOCAL MACHINE

☐ CURRENT USER

☐ USERS

STEP #1: SNAPSHOT

Step #1: Get Baseline State

STEP #2: COMPARE

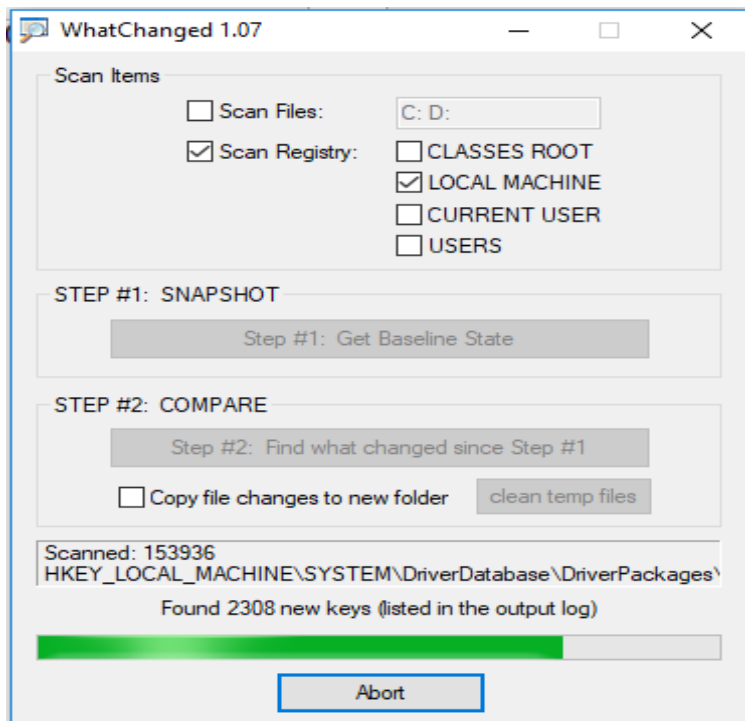
Step #2: Find what changed since Step #1

☐ Copy file changes to new folder clean temp files

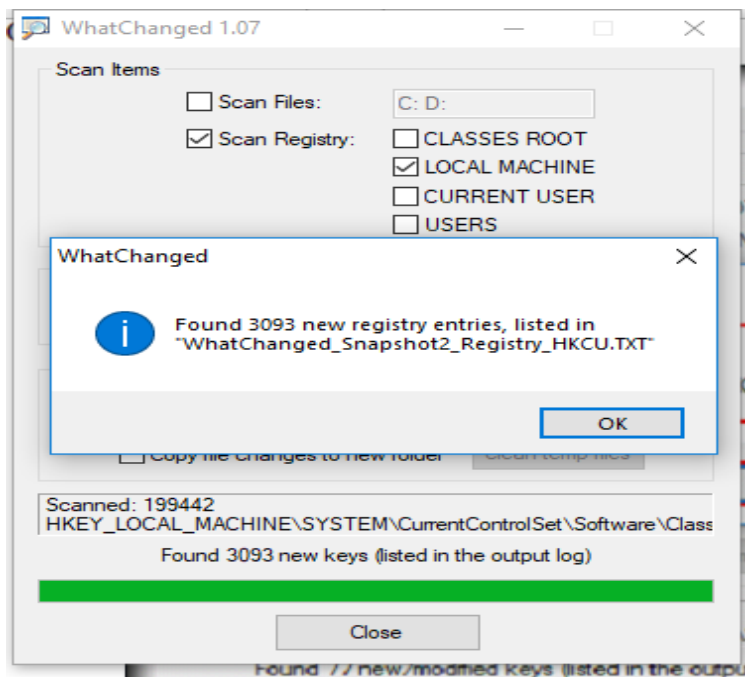
Scanned: 248
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Usage

Found 82 new/modified keys (listed in the output log)

Abort



- Number of changes observed.



- WhatChanged shot1

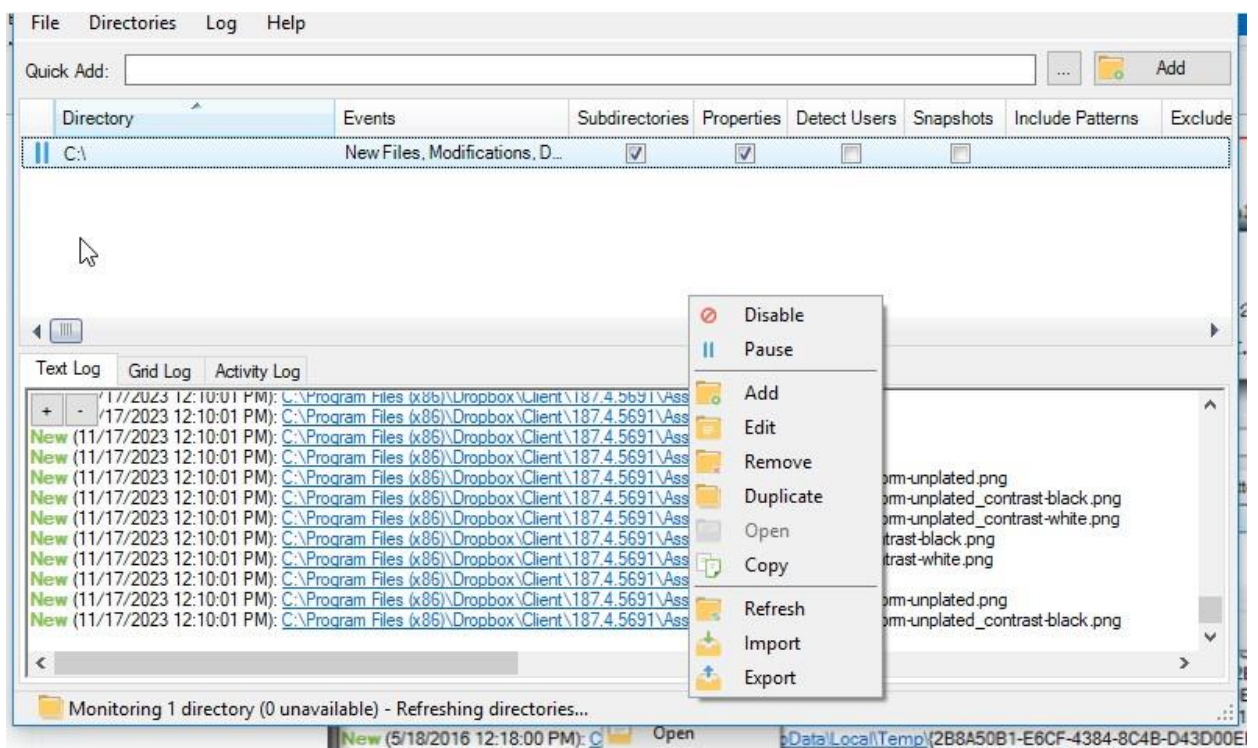
```

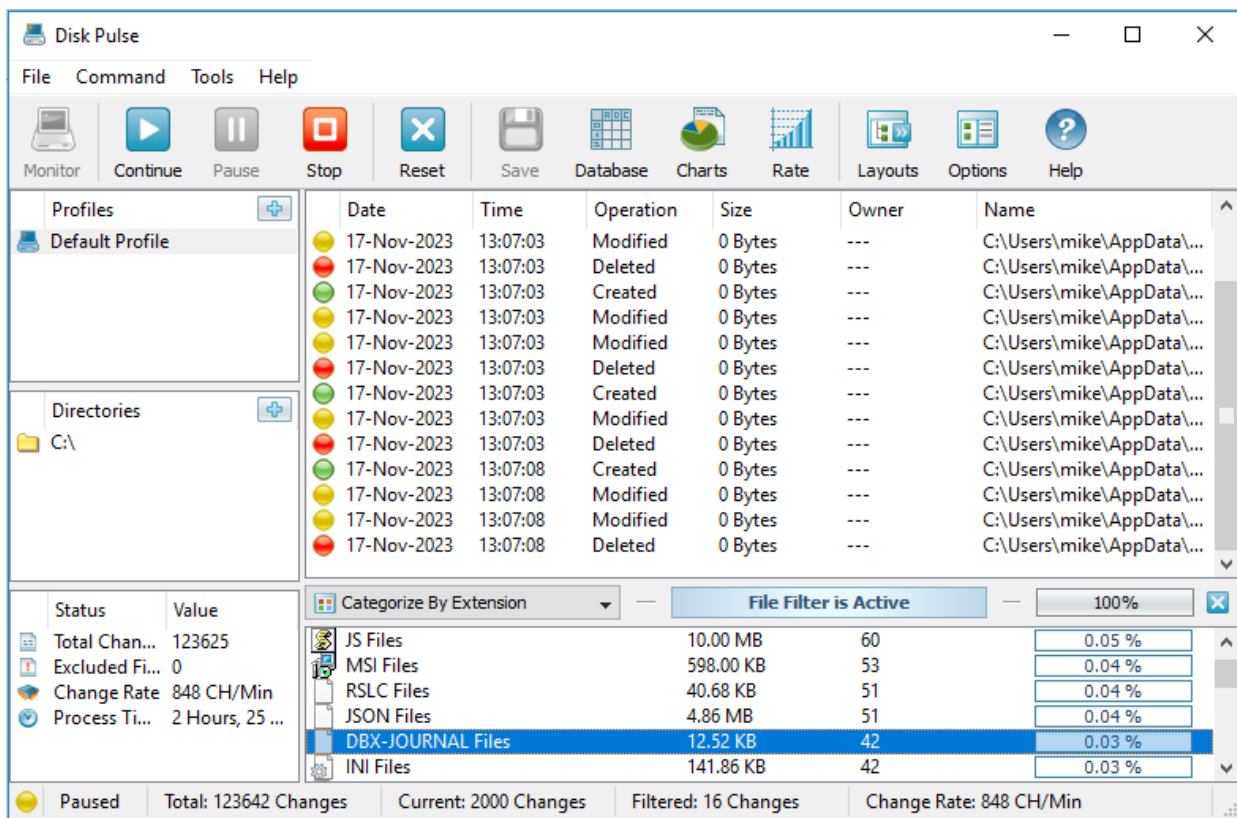
WhatChanged_Snapshot1_Registry_HKLM - Notepad
File Edit Format View Help
HKEY_LOCAL_MACHINE\BCD00000000
HKEY_LOCAL_MACHINE\HARDWARE
HKEY_LOCAL_MACHINE\HARDWARE\ACPI
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX_
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX_\VBOXBIOS
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX_\VBOXBIOS\00000002
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX_\VBOXBIOS\00000002\00000000=DSDTs#
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\FACS
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\FACS\00000000=FACS@
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\FADT
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\FADT\VBOX_
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\FADT\VBOX_\VBOXFACP
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\FADT\VBOX_\VBOXFACP\00000001
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\FADT\VBOX_\VBOXFACP\00000001\00000000=FACP0
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\RSMT
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\RSMT\VBOX_
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\RSMT\VBOX_\VBOXXSMT
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\RSMT\VBOX_\VBOXXSMT\00000001
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\RSMT\VBOX_\VBOXXSMT\00000001\00000000=XSMt<
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\SSDT
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\SSDT\VBOX_
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\SSDT\VBOX_\VBOXCPUT
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\SSDT\VBOX_\VBOXCPUT\00000002
2 items 1 item selected 24.6 MB

```

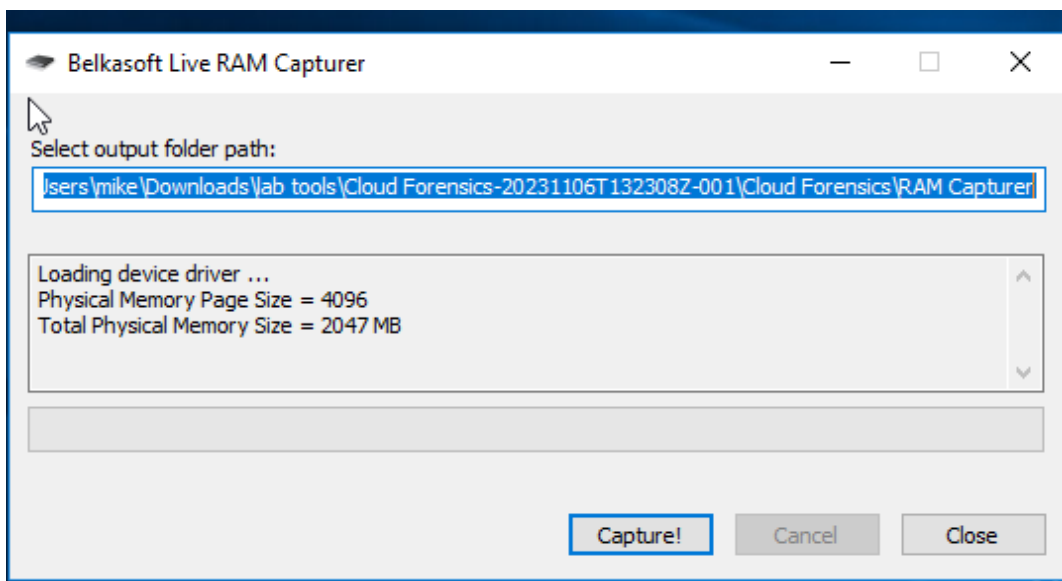
- WhatChanged shot 2

```
WhatChanged_Snapshot2_Registry_HKLM - Notepad
File Edit Format View Help
HKEY_LOCAL_MACHINE\SOFTWARE\Dropbox
HKEY_LOCAL_MACHINE\SOFTWARE\Dropbox\InstallPath=C:\Program Files (x86)\Dropbox\Client
HKEY_LOCAL_MACHINE\SOFTWARE\Dropbox\Client
HKEY_LOCAL_MACHINE\SOFTWARE\Dropbox\Client\Version=187.4.5691
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\path=C:\Program Files (x86)\Dropbox\Update
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\MsiStubRun=0
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\version=1.3.817.1
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\uid={EB232ED7-26D8-46A4-84CC-94503FFFB216}
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\RequestSequence=2
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\LastErrorTime=1700212088
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\LastInstallerResult=0
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\LastInstallerError=0
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\LastInstallerSuccessLaunchCmdLine="C:\Prog
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\LastChecked=1700215776
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients\{CC46080E-4C33-4981-859A-BBA2F780F
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients\{CC46080E-4C33-4981-859A-BBA2F780F
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients\{CC46080E-4C33-4981-859A-BBA2F780F
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\ClientState
```

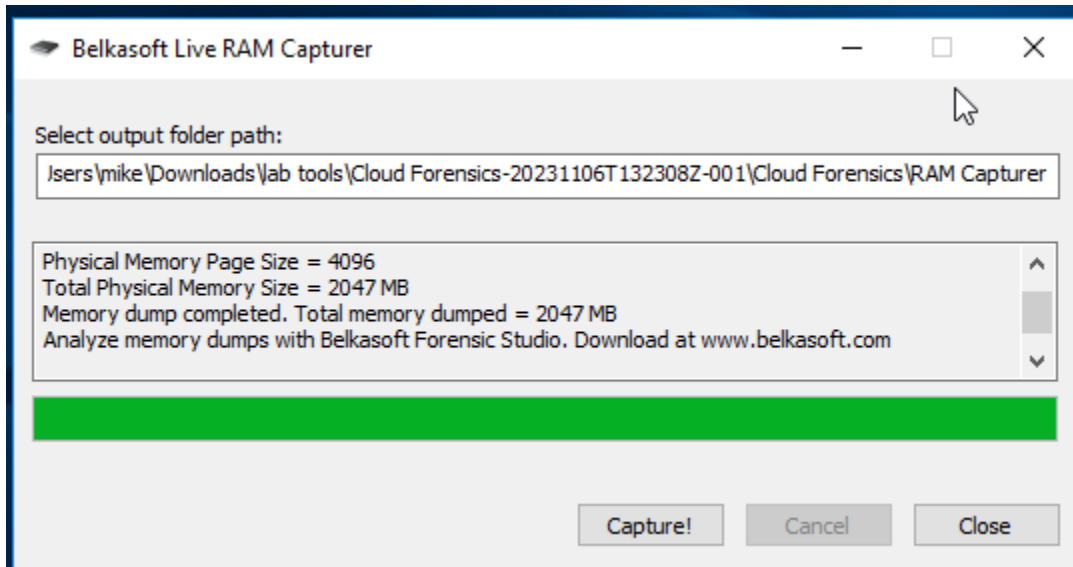




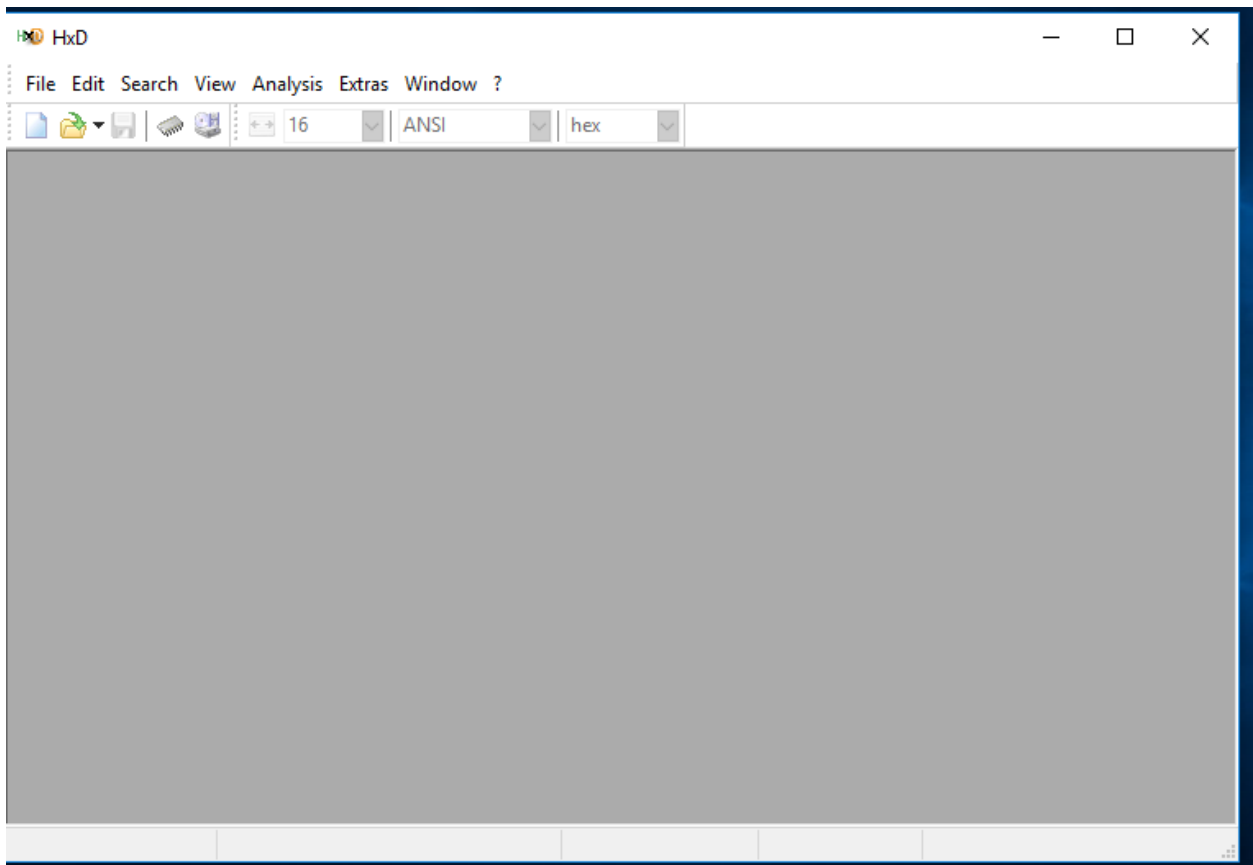
- Launch the RAM capturer and specify the output folder path.

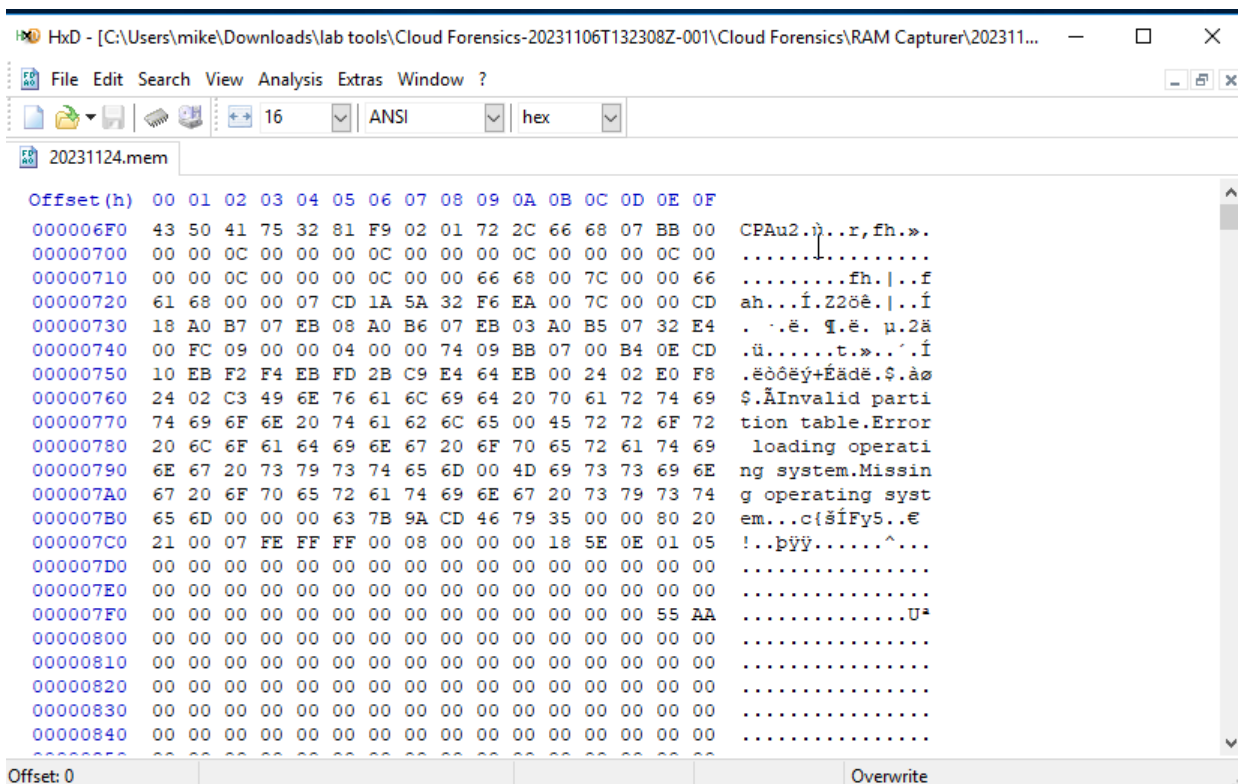
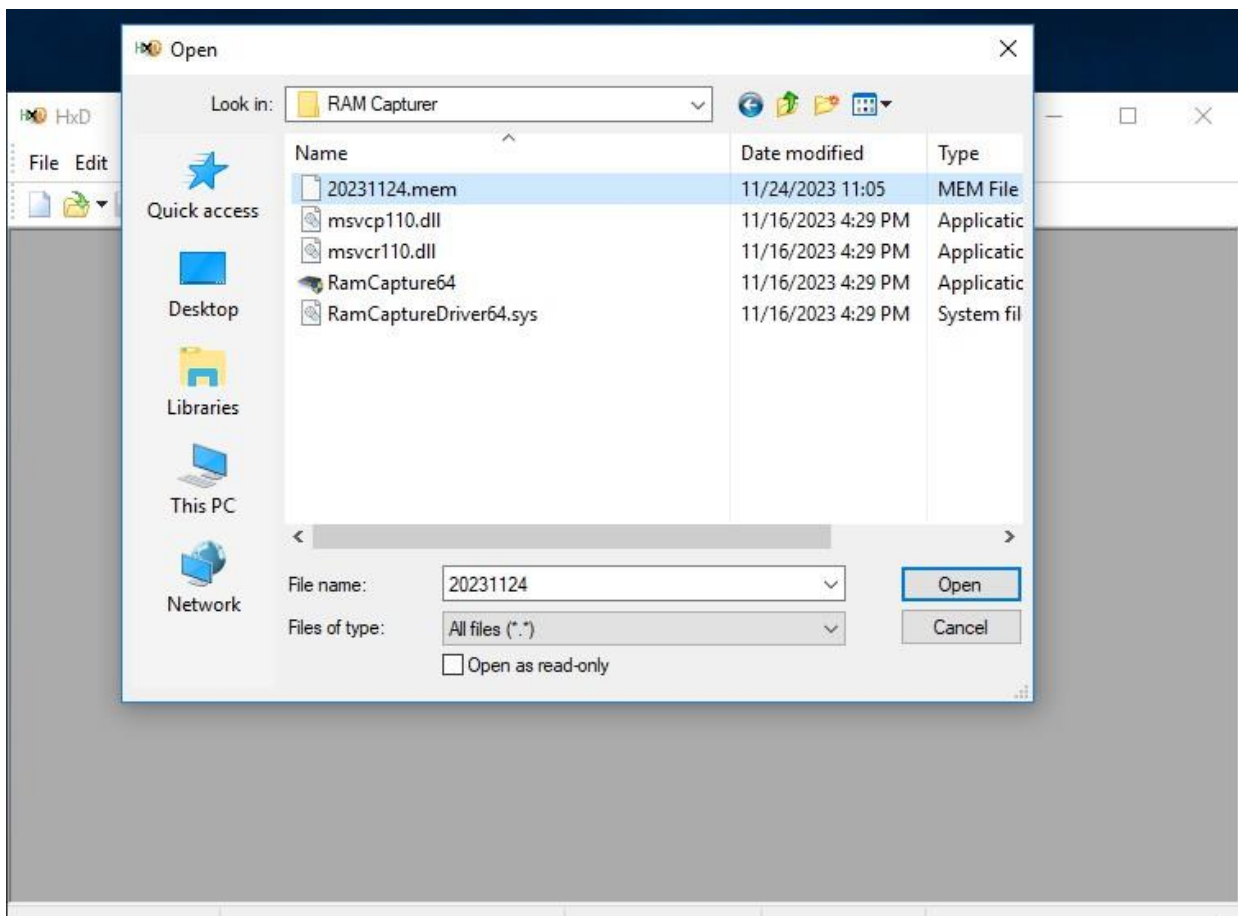


- Once the scan completes click on close.

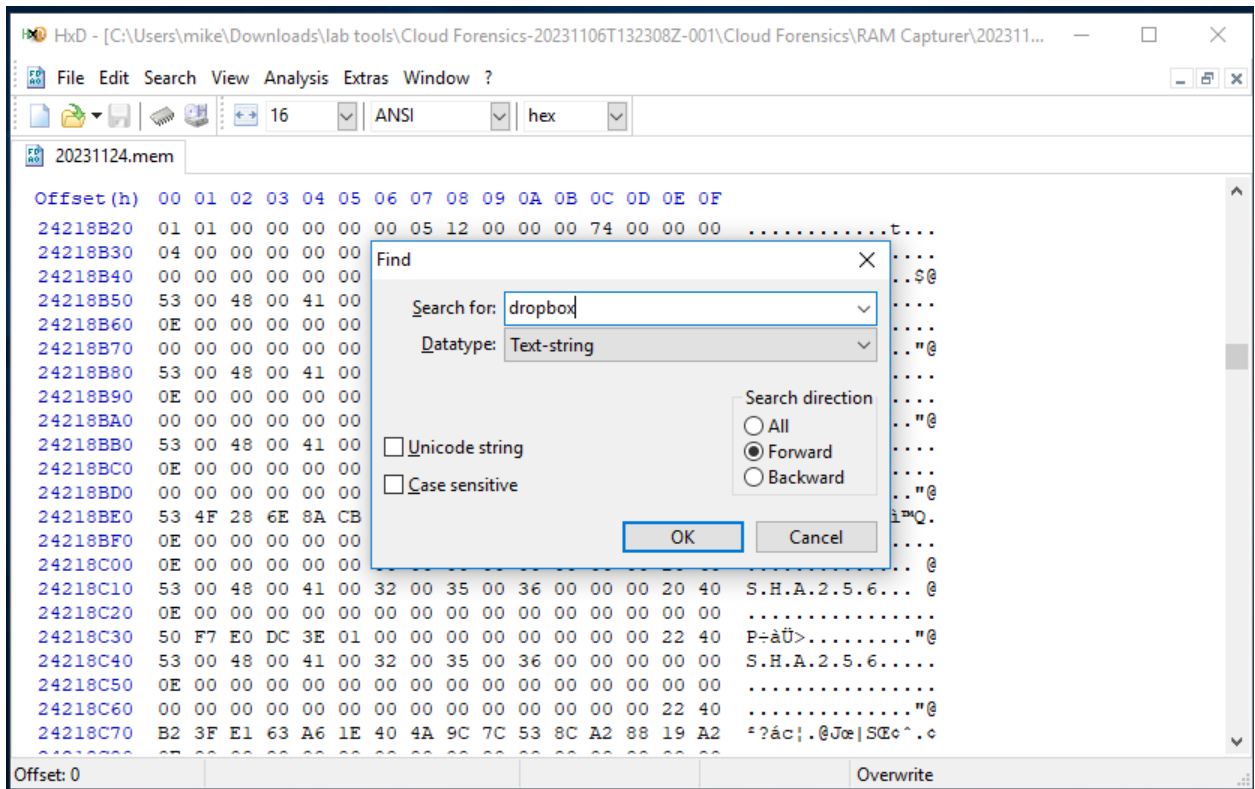


- Once the hex editor is launched, the following GUI is displayed.

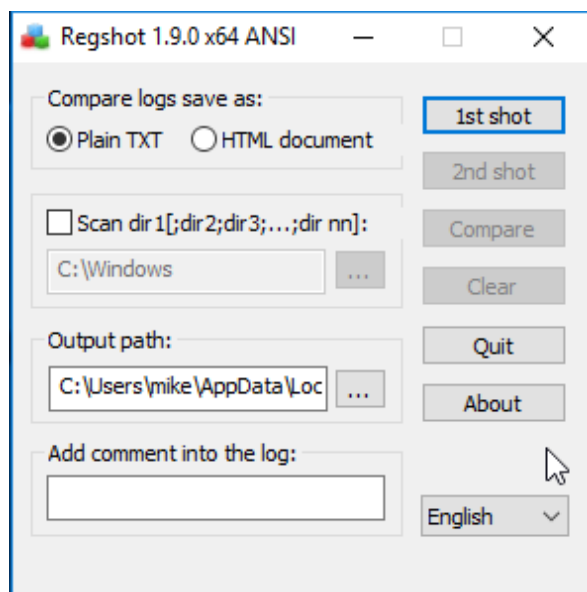
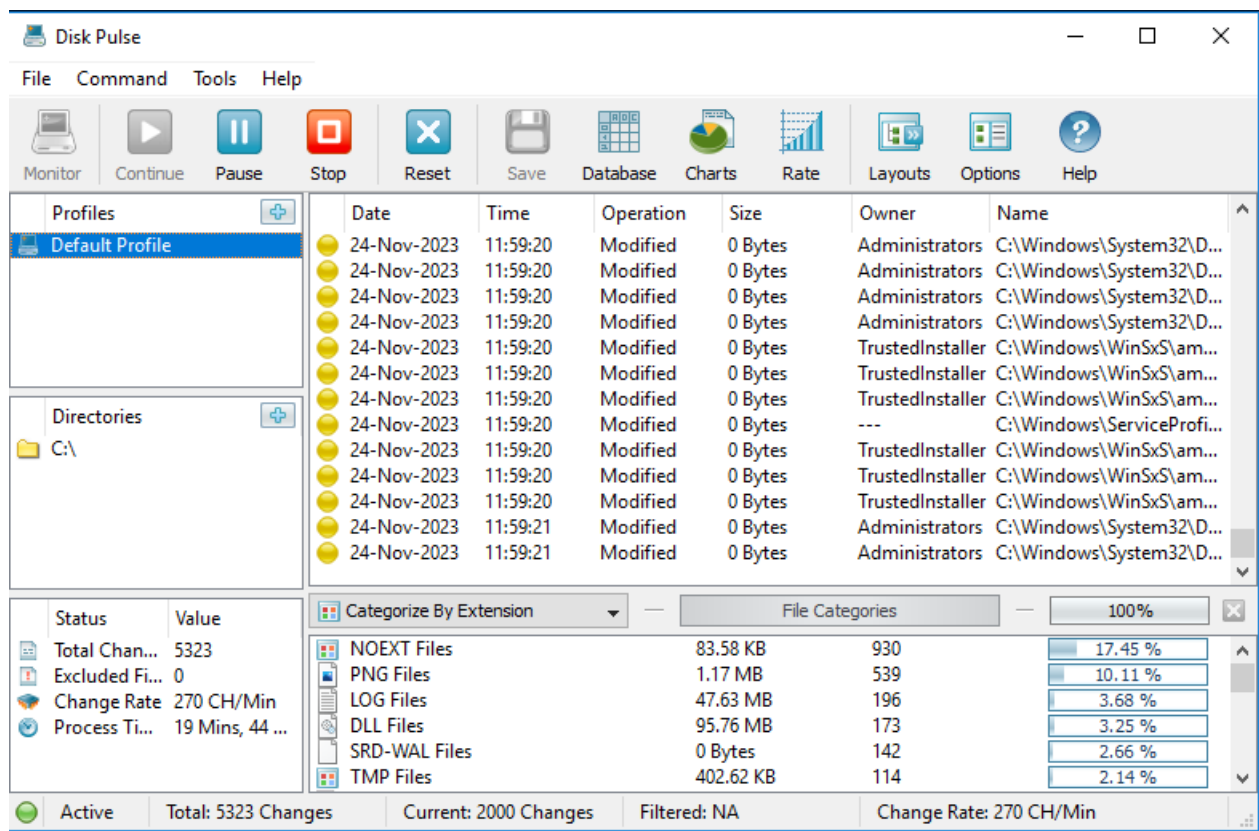




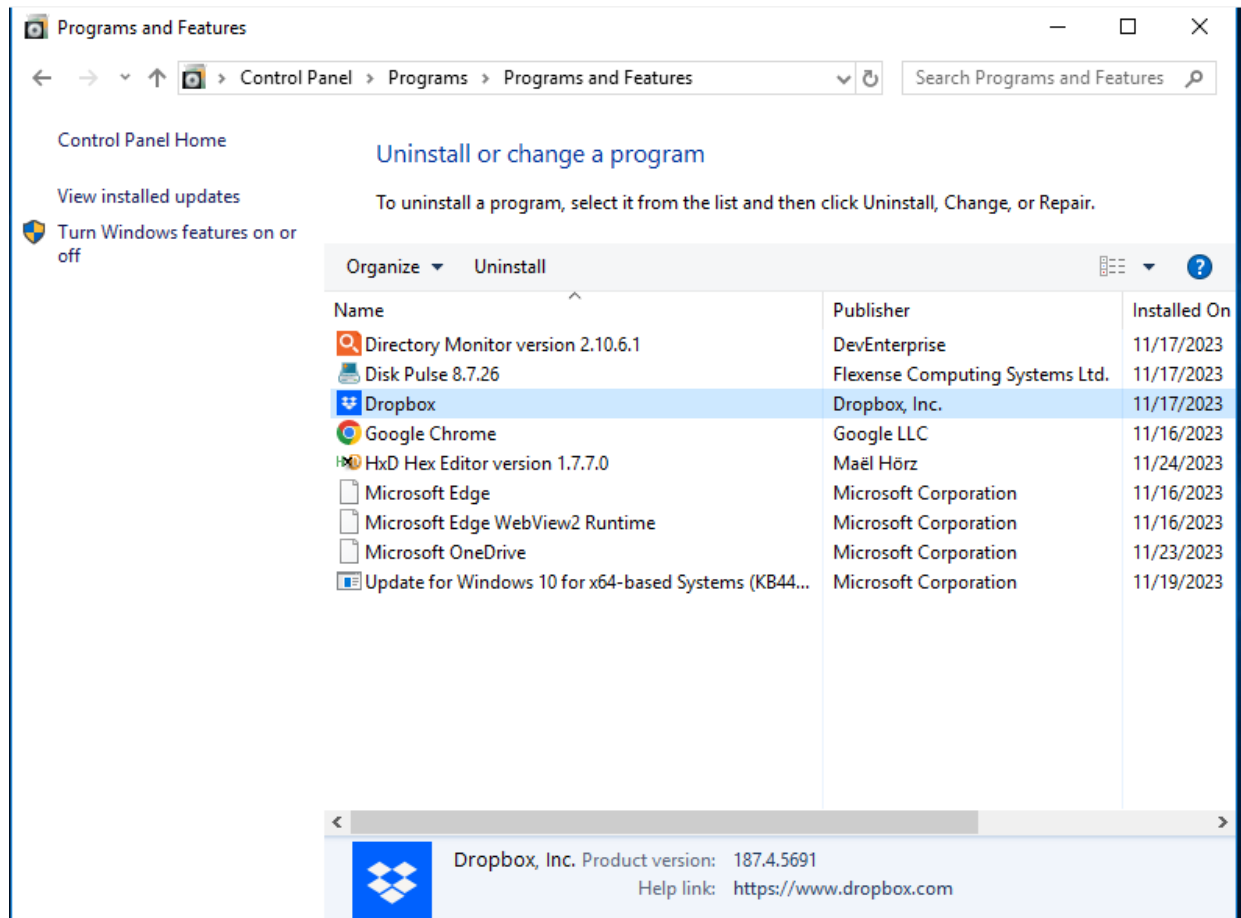
- Using Ctrl + F displays the following pop up window, such for dropbox in the search for section.

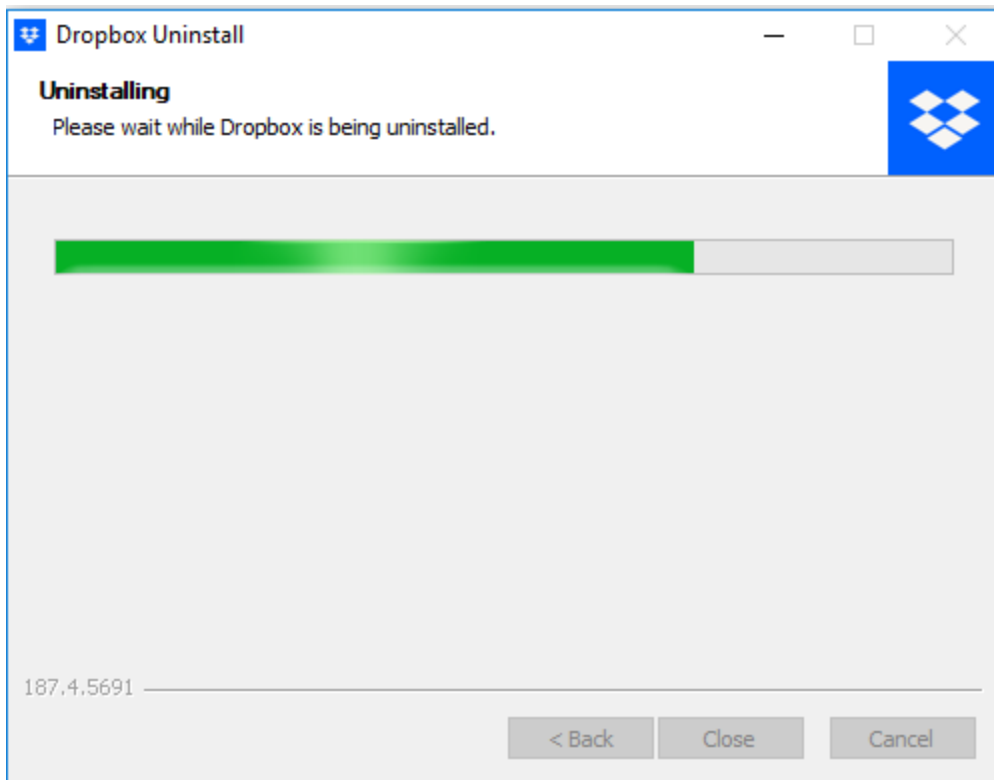


- Launch the Regshot and disk pulse click on 1st shot and monitor respectively.

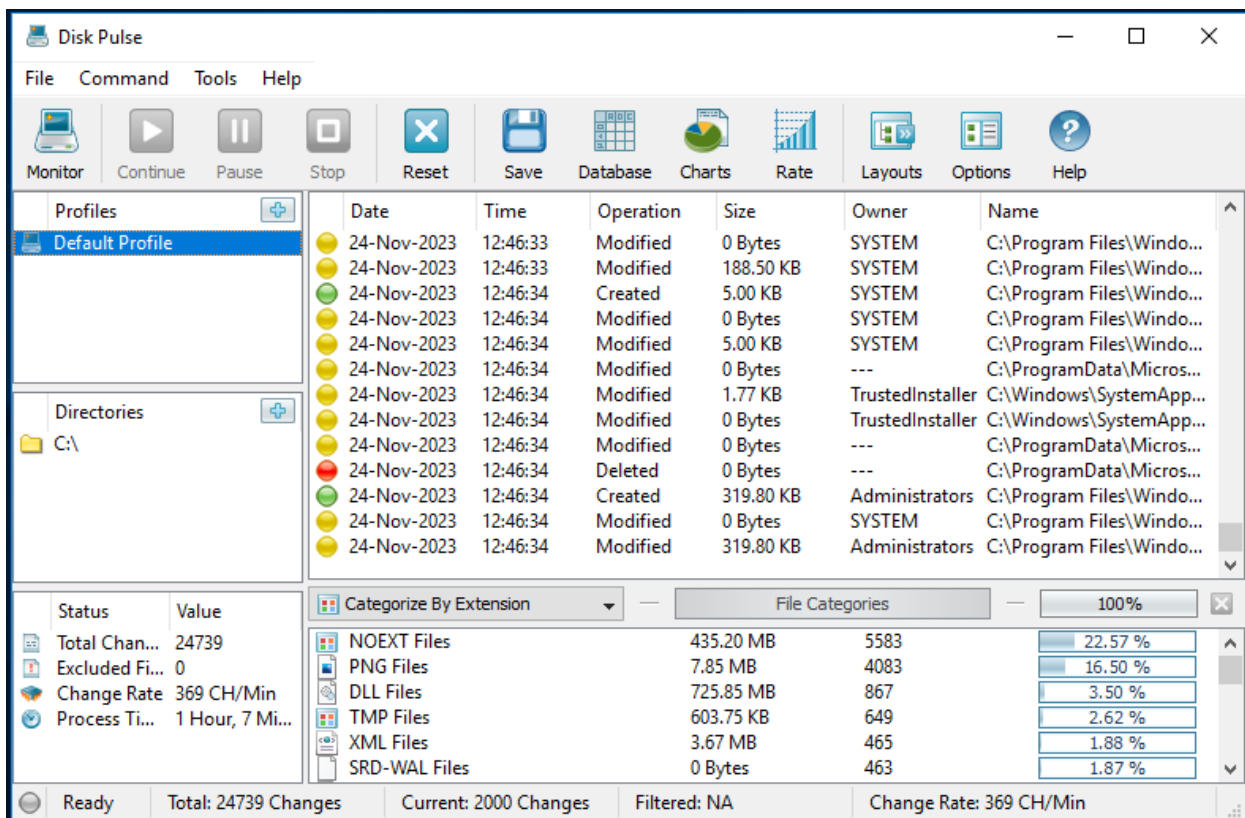


- **Navigate to the control panel, under the programs select the uninstall link and double click on Dropbox to uninstall.**





- On the already running Disk pulse, click on stop



- Select all changes and right click and copy the changes to clipboard.

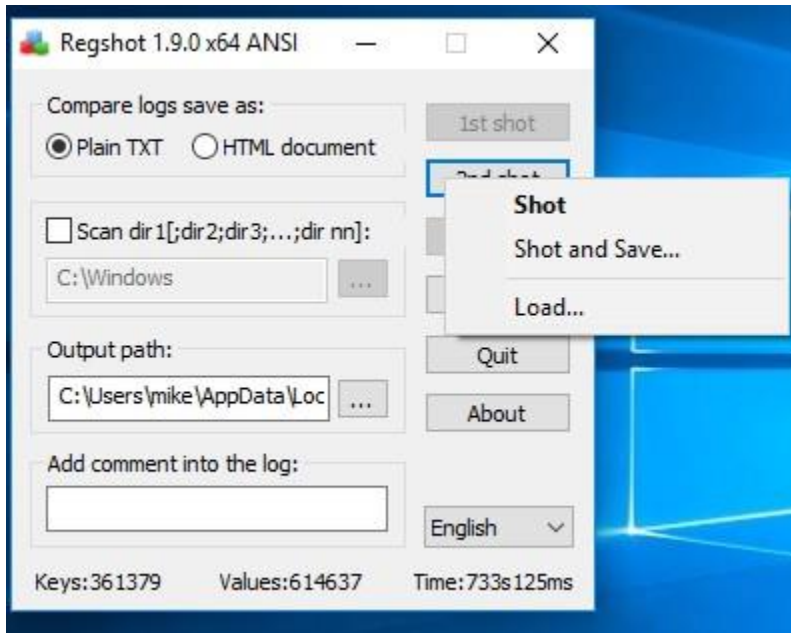
	Date	Time	Operation	Size	Owner	Name
	24-Nov-2023	12:46:33	Modified	0 Bytes	SYSTEM	C:\Program Files\Windo...
	24-Nov-2023	12:46:33	Modified	188.50 KB	SYSTEM	C:\Program Files\Windo...
	24-Nov-2023	12:46:34	Created	5.00 KB	SYSTEM	C:\Program Files\Windo...
	24-Nov-2023	12:46:34	Modified	0 Bytes	SYSTEM	C:\Program Files\Windo...
	24-Nov-2023	12:46:34	Modified	5.00 KB	SYSTEM	C:\Program Files\Windo...
	24-Nov-2023	12:46:34	Modified	0 Bytes	---	C:\ProgramData\Micros...
	24-Nov-2023	12:46:34	Modified	1.77 KB	TrustedInstaller	C:\Windows\SystemApp...
	24-Nov-2023	12:46:34	Modified	0 Bytes	TrustedInstaller	C:\Windows\SystemApp...
	24-Nov-2023	12:46:34	Modified	0 Bytes	---	C:\ProgramData\Micros...
	24-Nov-2023	12:46:34	Deleted	0 Bytes	---	C:\ProgramData\Micros...
	24-Nov-2023	12:46:34	Created	319.80 KB	Administrators	C:\Program Files\Windo...
	24-Nov-2023	12:46:34	Modified	0 Bytes	SYSTEM	C:\Program Files\Windo...
	24-Nov-2023	12:46:34	Modified	319.80 KB	Administrators	C:\Program Files\Windo...

- Paste the changes to a text file for easy analysis.

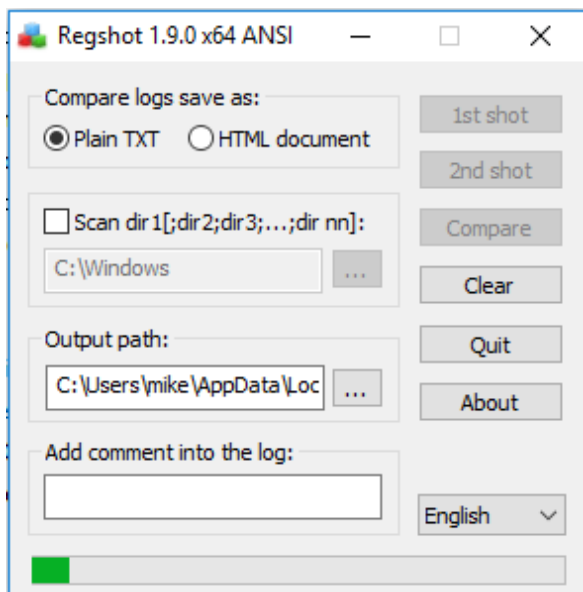
Untitled - Notepad

File	Edit	Format	View	Help
24-Nov-2023	12:46:21	Modified	0 Bytes	SYSTEM C:\Program Files\WindowsApp
24-Nov-2023	12:46:22	Modified	6.72 KB	Administrators C:\Program Files\Wi
24-Nov-2023	12:46:22	Created 4.75 KB	Administrators	C:\Program Files\WindowsApp
24-Nov-2023	12:46:22	Modified	0 Bytes	SYSTEM C:\Program Files\WindowsApp
24-Nov-2023	12:46:22	Modified	4.75 KB	Administrators C:\Program Files\Wi
24-Nov-2023	12:46:22	Modified	2.90 KB	TrustedInstaller C:\Windows\
24-Nov-2023	12:46:22	Modified	0 Bytes	TrustedInstaller C:\Windows\
24-Nov-2023	12:46:23	Created 3.77 KB	Administrators	C:\Program Files\WindowsApp
24-Nov-2023	12:46:23	Modified	0 Bytes	SYSTEM C:\Program Files\WindowsApp
24-Nov-2023	12:46:23	Modified	3.77 KB	Administrators C:\Program Files\Wi
24-Nov-2023	12:46:23	Created 4.15 KB	Administrators	C:\Program Files\WindowsApp
24-Nov-2023	12:46:23	Modified	0 Bytes	SYSTEM C:\Program Files\WindowsApp
24-Nov-2023	12:46:24	Modified	4.15 KB	Administrators C:\Program Files\Wi
24-Nov-2023	12:46:25	Created 5.40 KB	Administrators	C:\Program Files\WindowsApp
24-Nov-2023	12:46:25	Modified	0 Bytes	SYSTEM C:\Program Files\WindowsApp
24-Nov-2023	12:46:25	Modified	5.40 KB	Administrators C:\Program Files\Wi
24-Nov-2023	12:46:25	Created 5.72 KB	Administrators	C:\Program Files\WindowsApp
24-Nov-2023	12:46:25	Modified	0 Bytes	SYSTEM C:\Program Files\WindowsApp
24-Nov-2023	12:46:26	Modified	5.72 KB	Administrators C:\Program Files\Wi
24-Nov-2023	12:46:26	Modified	3.36 KB	TrustedInstaller C:\Windows\
24-Nov-2023	12:46:26	Created 0 Bytes	SYSTEM	C:\Program Files\WindowsApps\Micros
24-Nov-2023	12:46:26	Modified	0 Bytes	SYSTEM C:\Program Files\WindowsApp
24-Nov-2023	12:46:26	Created 0 Bytes	SYSTEM	C:\Program Files\WindowsApps\Micros
24-Nov-2023	12:46:26	Modified	0 Bytes	SYSTEM C:\Program Files\WindowsApp
24-Nov-2023	12:46:26	Created 9.83 KB	Administrators	C:\Program Files\WindowsApp

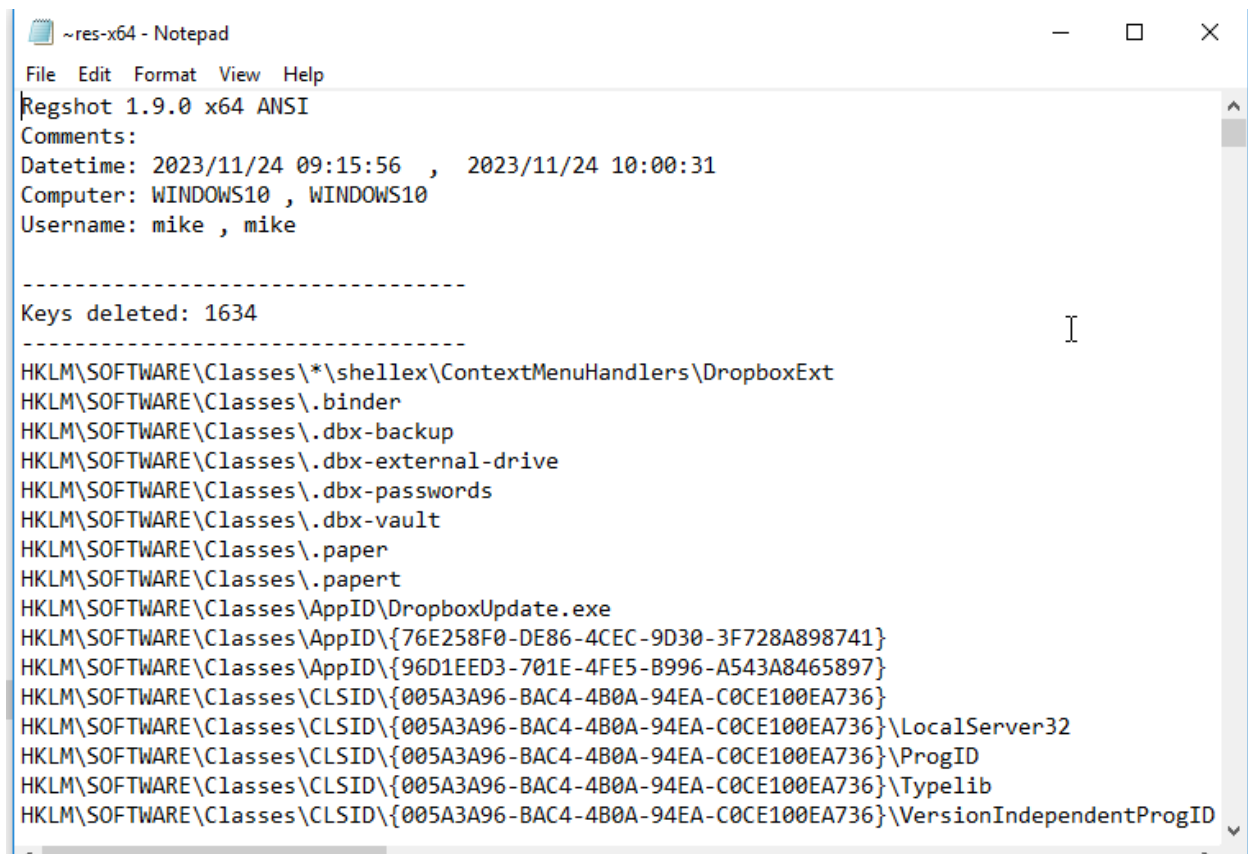
- Launch the Regshot and select 2nd shot, then shot.



- Click on the compare.



- The tool prompts a notepad file after comparing first and second shot.



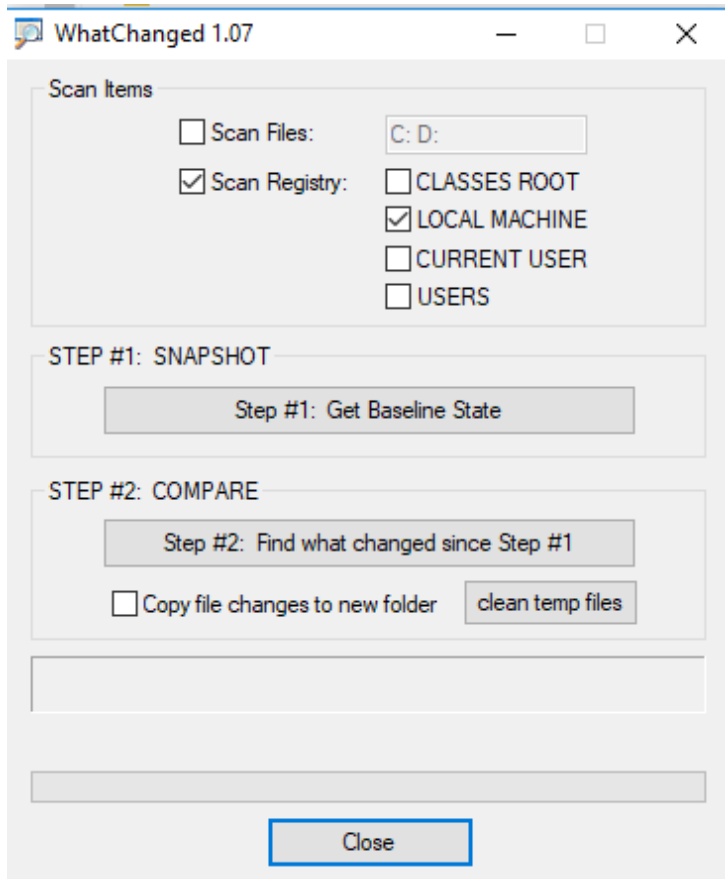
The screenshot shows a Notepad window titled '~res-x64 - Notepad'. The menu bar includes File, Edit, Format, View, and Help. The text content is as follows:

```
Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2023/11/24 09:15:56 , 2023/11/24 10:00:31
Computer: WINDOWS10 , WINDOWS10
Username: mike , mike

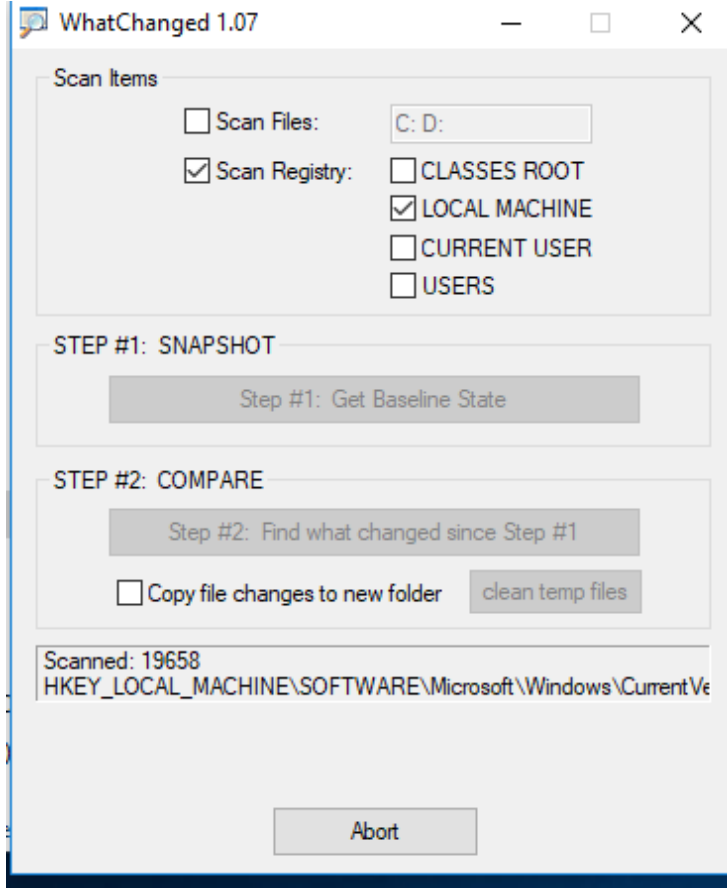
-----
Keys deleted: 1634
-----
HKLM\SOFTWARE\Classes\*\shellex\ContextMenuHandlers\DropboxExt
HKLM\SOFTWARE\Classes\*.binder
HKLM\SOFTWARE\Classes\*.dbx-backup
HKLM\SOFTWARE\Classes\*.dbx-external-drive
HKLM\SOFTWARE\Classes\*.dbx-passwords
HKLM\SOFTWARE\Classes\*.dbx-vault
HKLM\SOFTWARE\Classes\*.paper
HKLM\SOFTWARE\Classes\*.papert
HKLM\SOFTWARE\Classes\AppID\DropboxUpdate.exe
HKLM\SOFTWARE\Classes\AppID\{76E258F0-DE86-4CEC-9D30-3F728A898741}
HKLM\SOFTWARE\Classes\AppID\{96D1EED3-701E-4FE5-B996-A543A8465897}
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}\LocalServer32
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}\ProgID
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}\Typelib
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}\VersionIndependentProgID
```


INVESTIGATION OF GOOGLE DRIVE

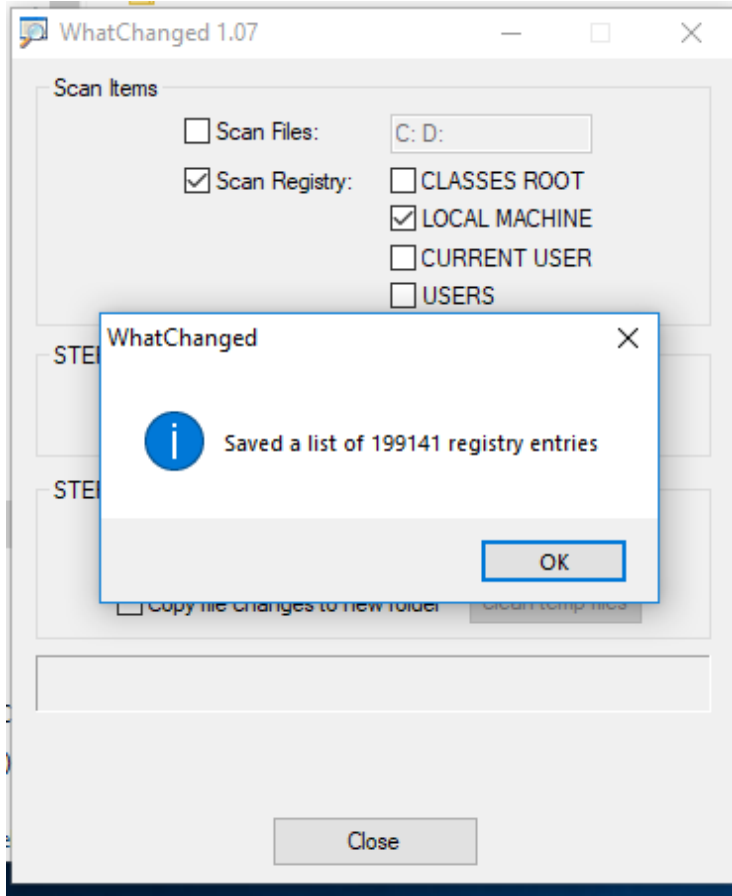
- Launch the WhatChanged and select the *scan Registry* and *LOCAL MACHINE*.



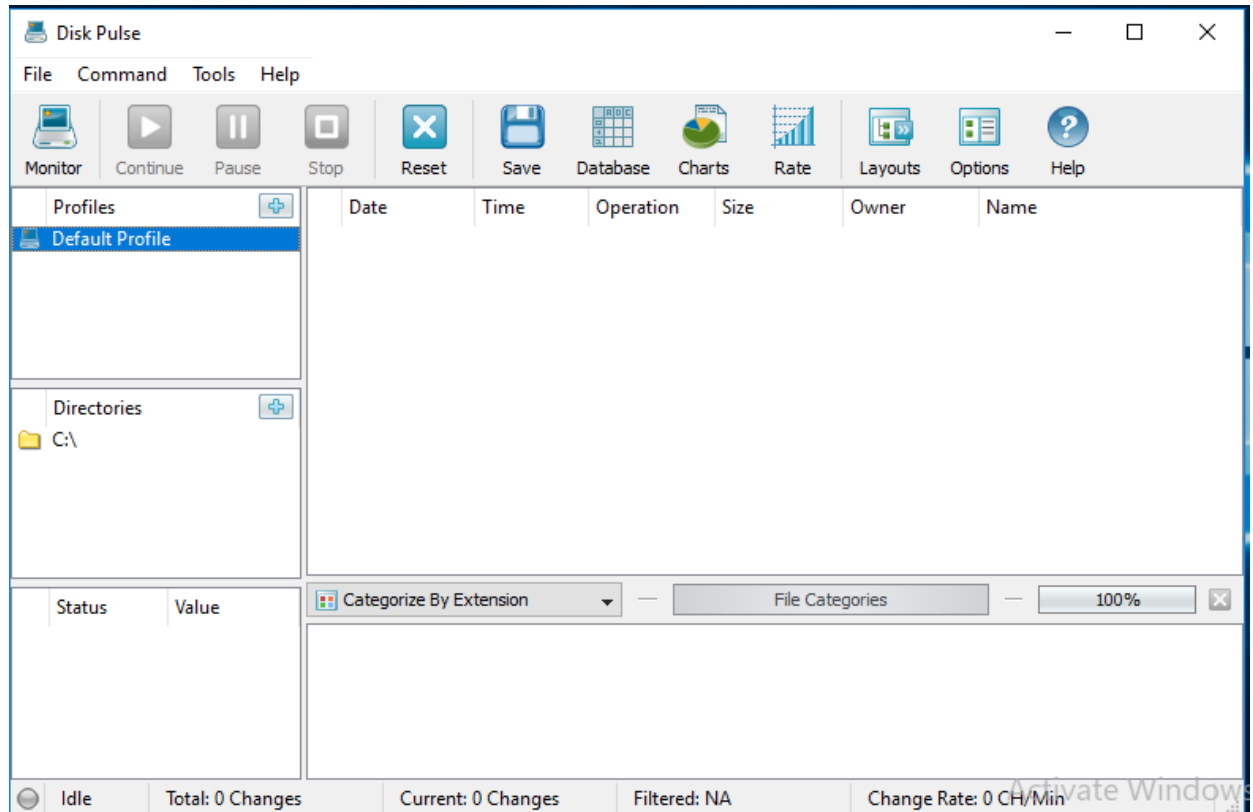
- Click on *step#1: Get Baseline State*.



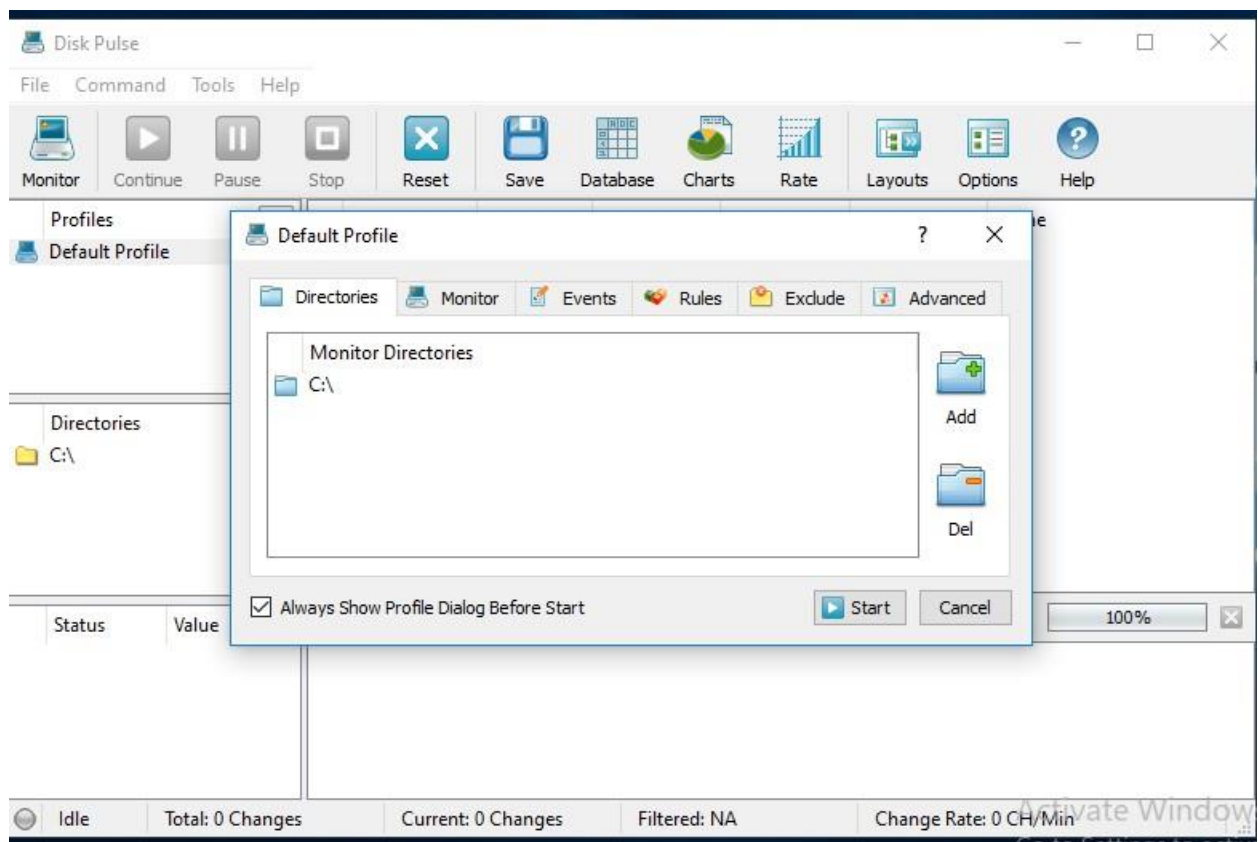
- Dialog box displaying total number of entries recorded.



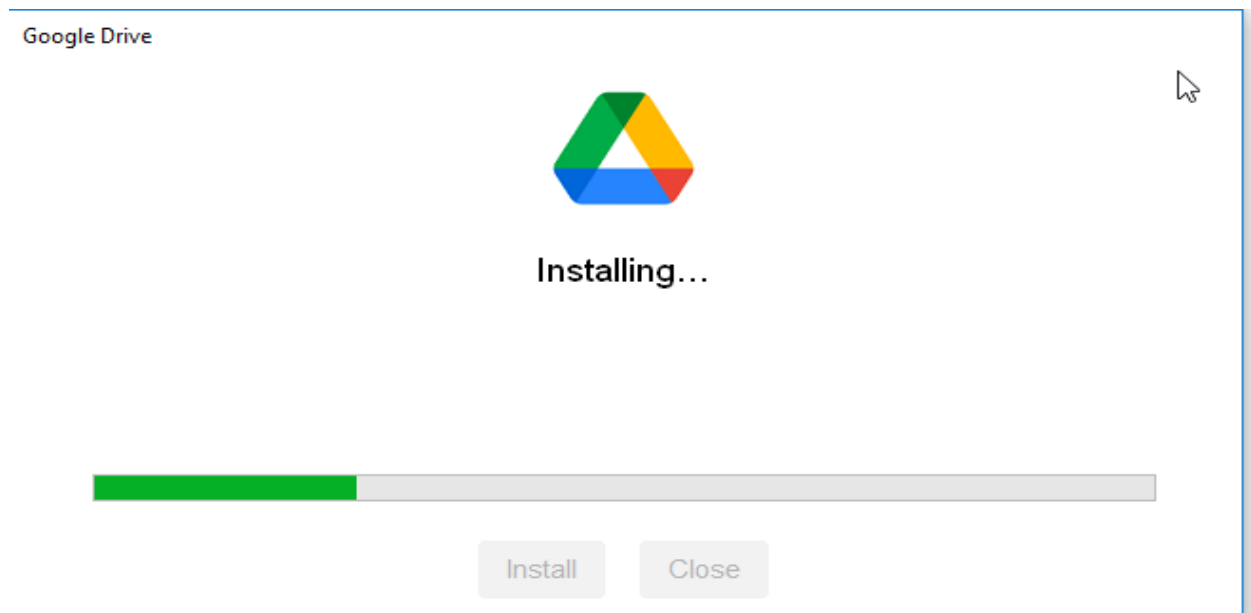
- Launch the Disk Pulse.



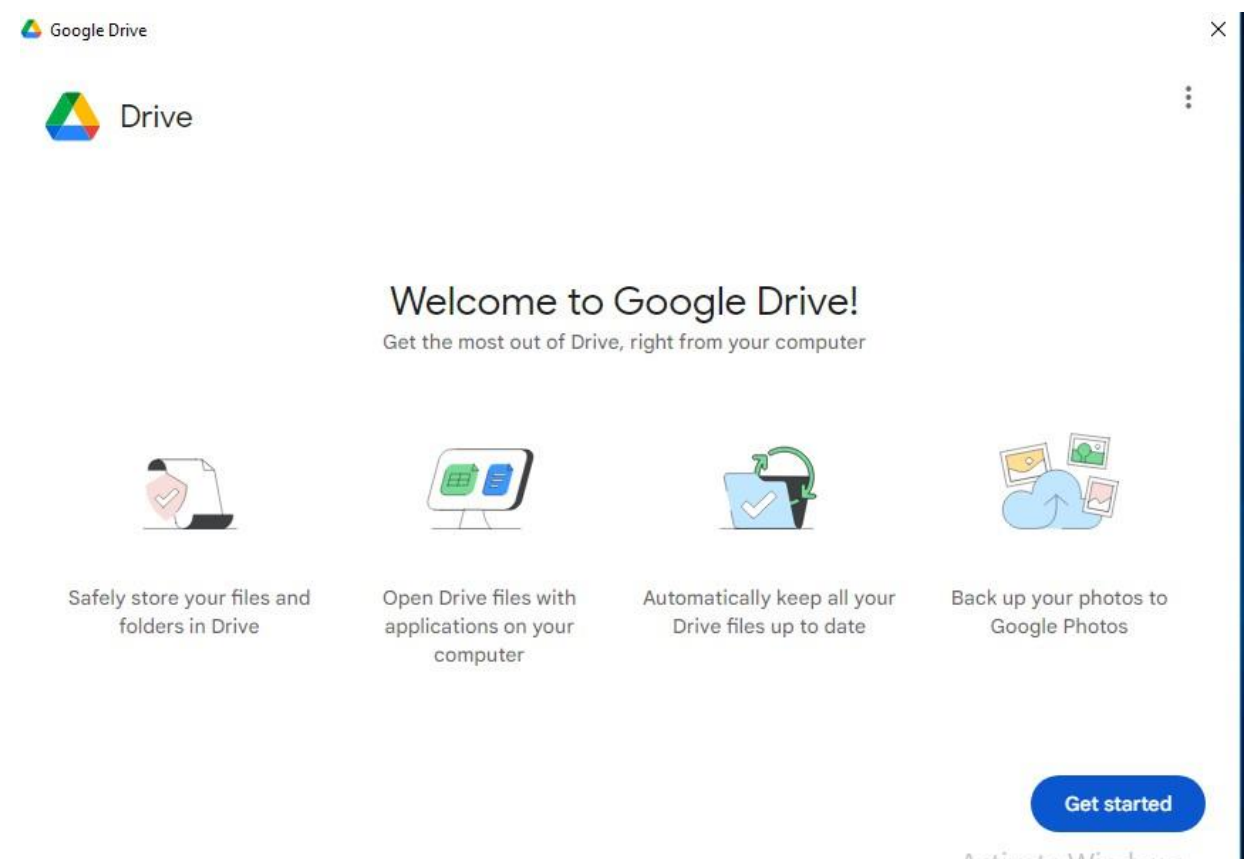
- Click on monitor, the dialog window displays with the C:\ added by default. Click on start.



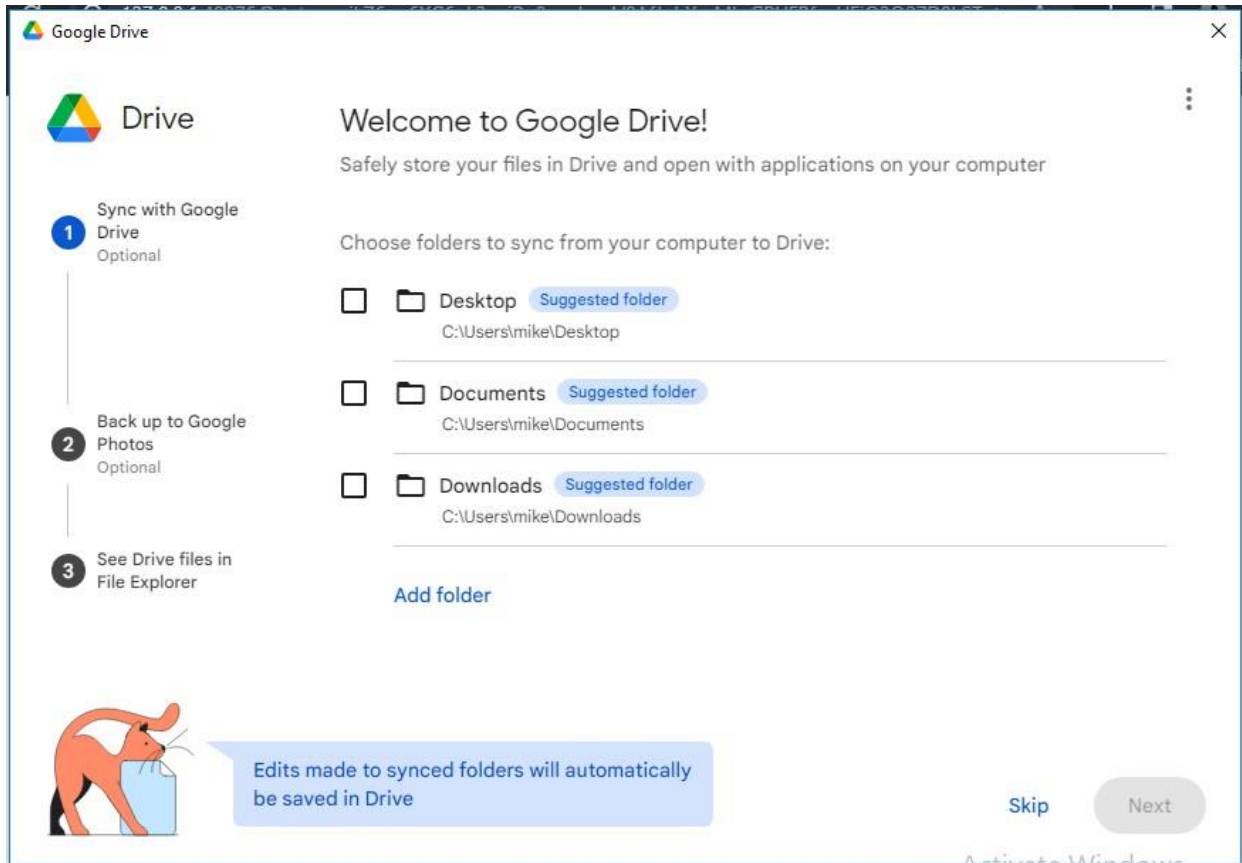
- **Install the google drive client.**



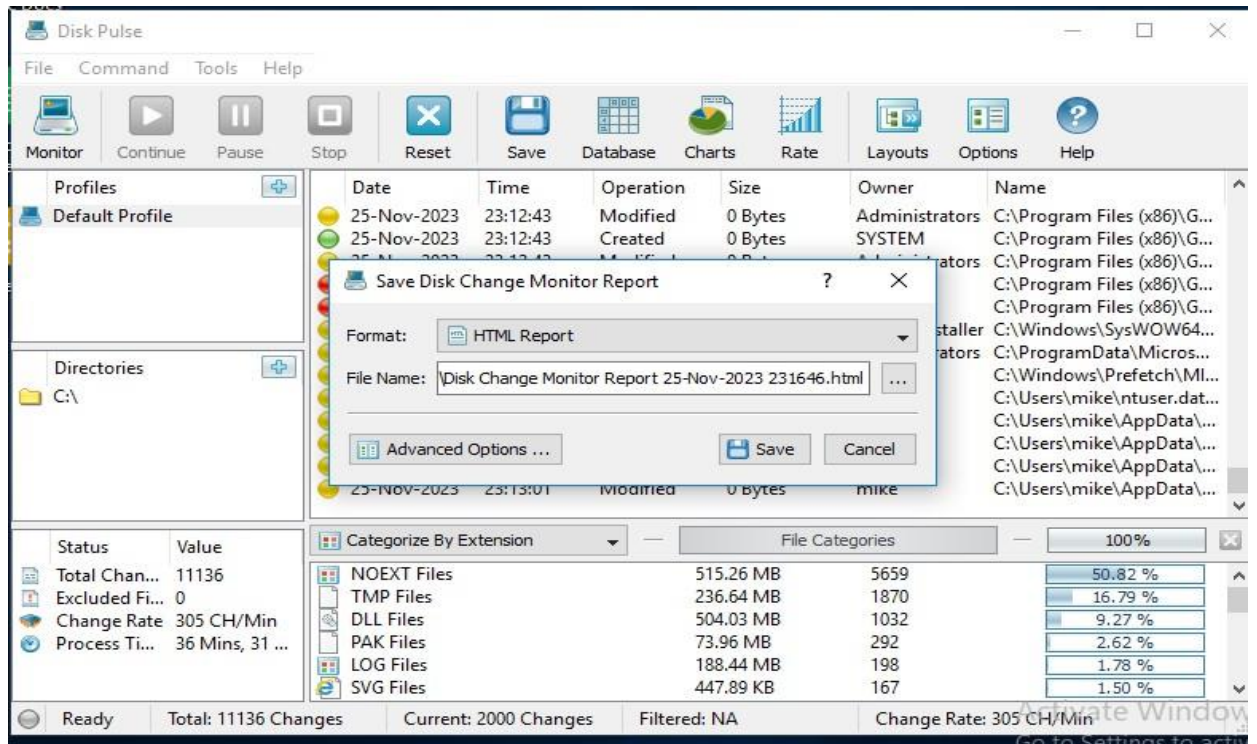
- **Once done, click on the app icon to launch the google drive and click on 'Get started'.**



- Select the folder of choice to sync.



- **Navigate back to the already running disk pulse and click on 'Stop' to stop monitoring the process**



- Click on save icon to save all entries. From the 'save disk change monitor report' prompt, select the text format from the drop-down list and click on save button.

The screenshot shows the Disk Pulse application window. A warning dialog box is displayed in the center, asking "Monitor is active, do you want to stop?". The dialog has a yellow warning icon and two buttons: "Yes" and "No".

The background application window shows a list of file changes with columns: Date, Time, Operation, Size, Owner, and Name. The list includes several entries for file modifications on 25-Nov-2023.

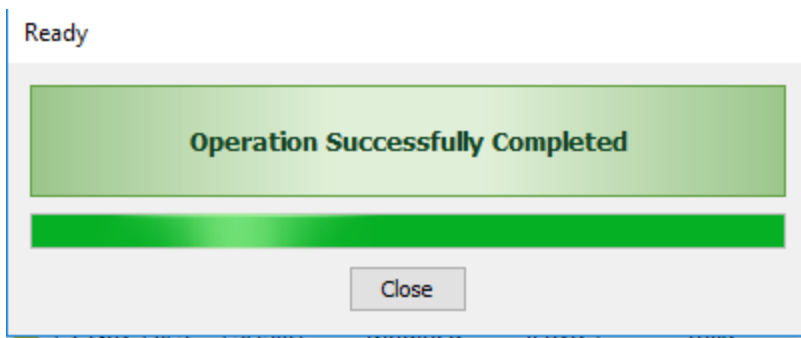
Below the file list, there is a section for "File Categories" showing the distribution of file types:

File Category	Size	Count	Percentage
NOEXT Files	515.10 MB	5636	50.81 %
TMP Files	236.60 MB	1859	16.76 %
DLL Files	500.86 MB	1029	9.28 %
PAK Files	73.96 MB	292	2.63 %
LOG Files	187.46 MB	197	1.78 %
SVG Files	447.89 KB	167	1.51 %

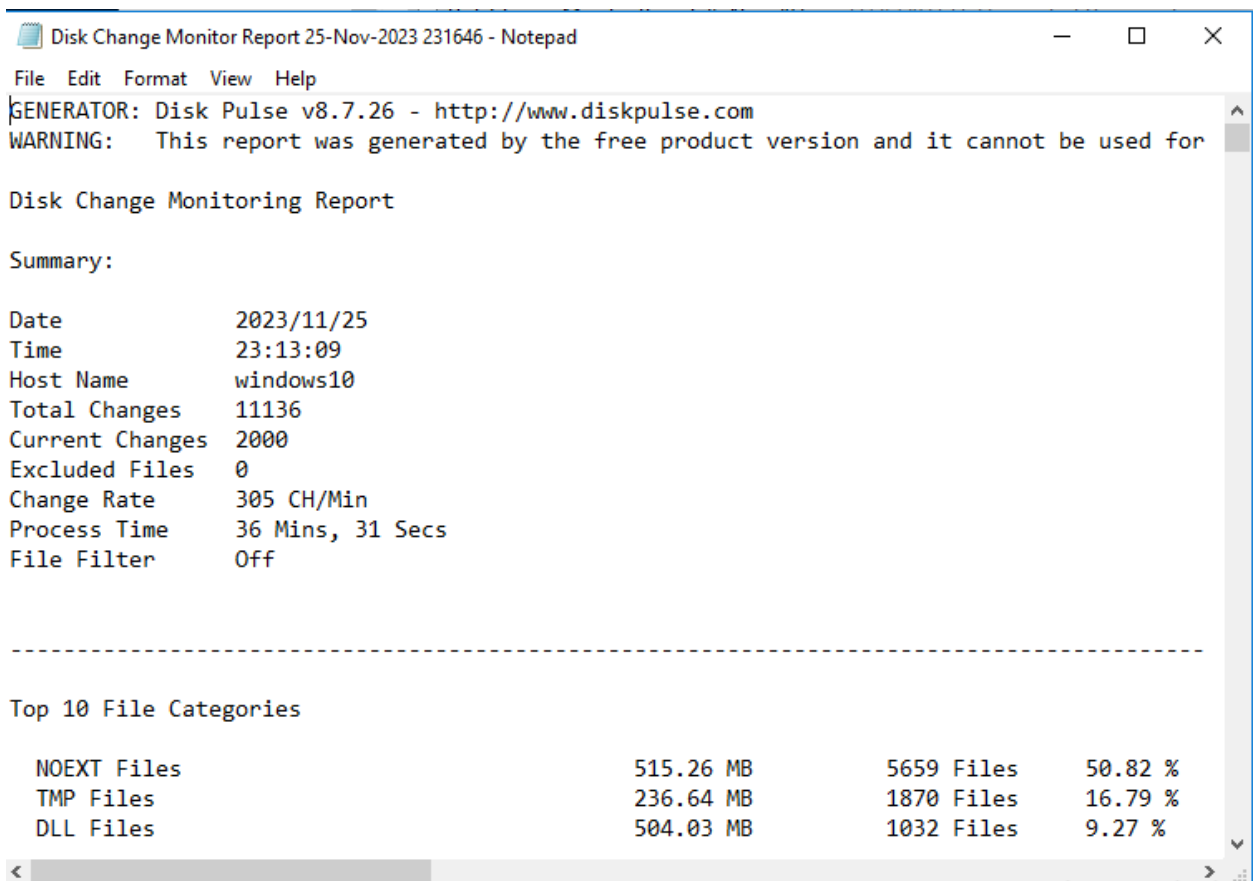
At the bottom of the window, a status bar shows: Active, Total: 11093 Changes, Current: 2000 Changes, Filtered: NA, Change Rate: 309 CH/Min.

The screenshot shows a dropdown menu for selecting the report format. The options are:

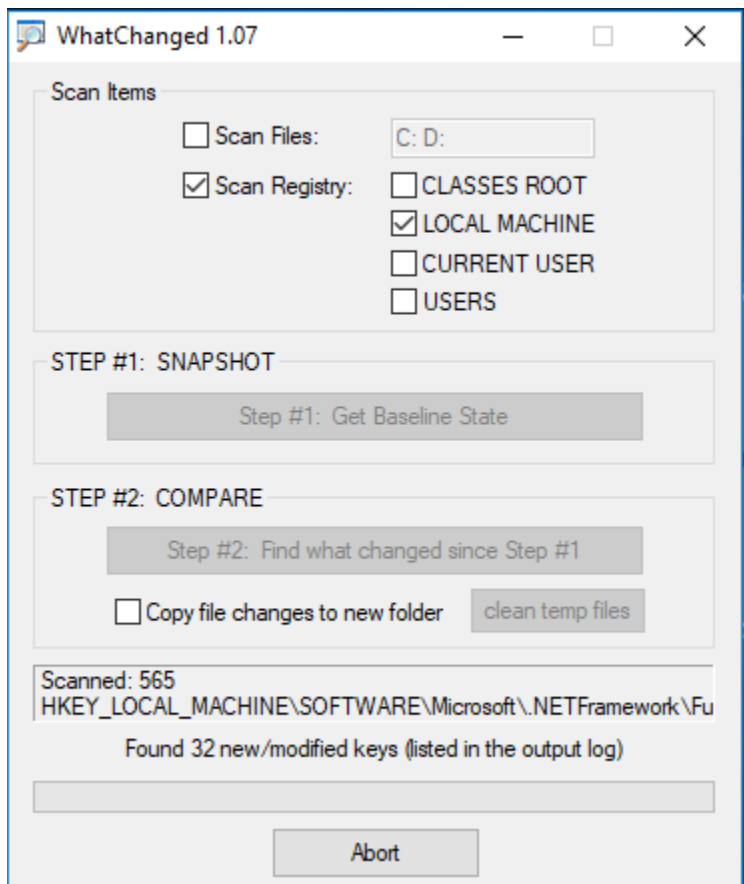
- Text Report
- HTML Report
- HTML Summary
- PDF Report
- PDF Summary
- Text Report
- Text Summary
- CSV Report
- CSV Summary
- XML Report
- XML Summary



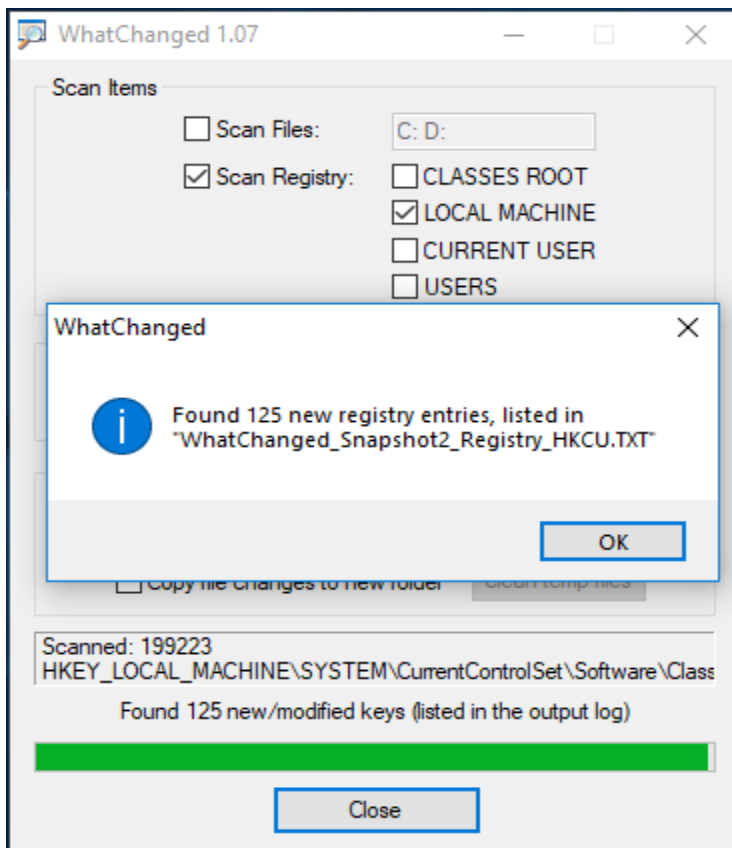
- A text file with all changes listed on it generated by disk pulse.



- **Navigate back to WhatChanged and click on 'step#2: find what changed since step#1'.**



- After the scanning, WhatChanged tools displays a dialog box listing new entries.



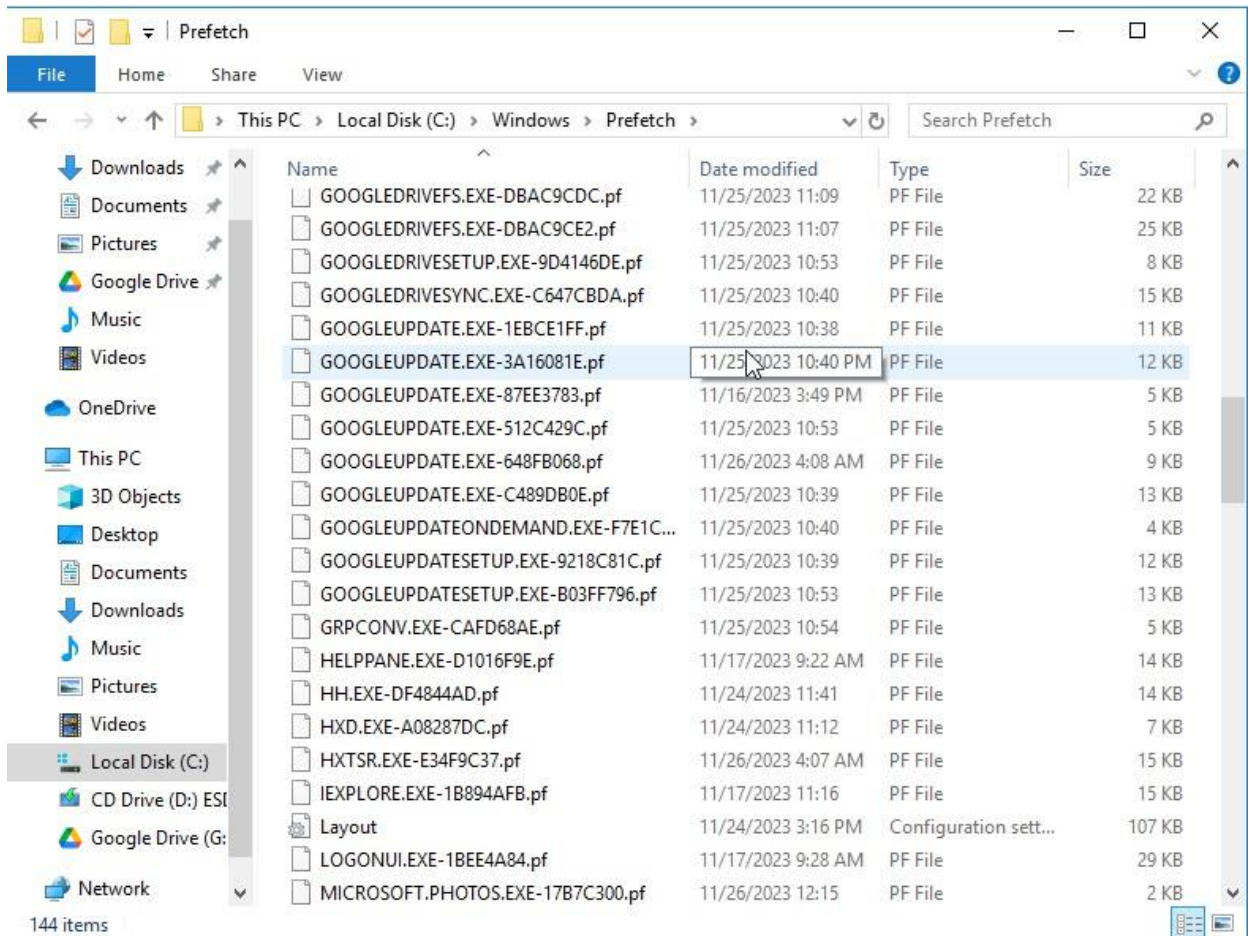
- List of all entries changed saved on a text file by WhatChanged.

```

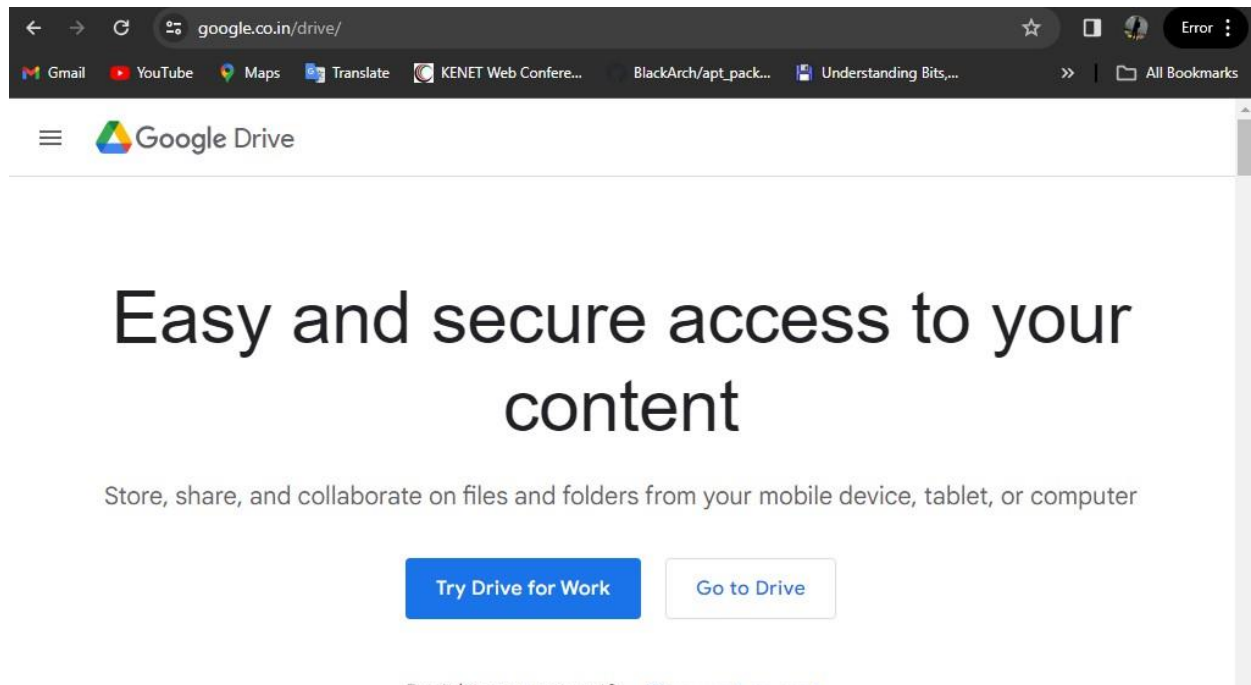
WhatChanged_Snapshot2_Registry_HKLM - Notepad
File Edit Format View Help
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-206309030-24
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-206309030-24
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-206309030-24
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-206309030-24
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-206309030-24
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-206309030-24
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-206309030-24
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\googledrivefs31357
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\googledrivefs31357\Eve
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\googledrivefs31357\Typ
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googledrivefs31357
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googledrivefs31357\Type=2
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googledrivefs31357\Start=1
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googledrivefs31357>ErrorControl=1
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googledrivefs31357\Tag=1
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googledrivefs31357\ImagePath=system32\
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googledrivefs31357\DisplayName=googled
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googledrivefs31357\Group=File System
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googledrivefs31357>Description=Google
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NcbService\NCB\KapiNlmCache\2\Timestam
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeEst
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeHig
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeLow
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime\Secur
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime\Secur
2 items 1 item selected 13.9 KB

```

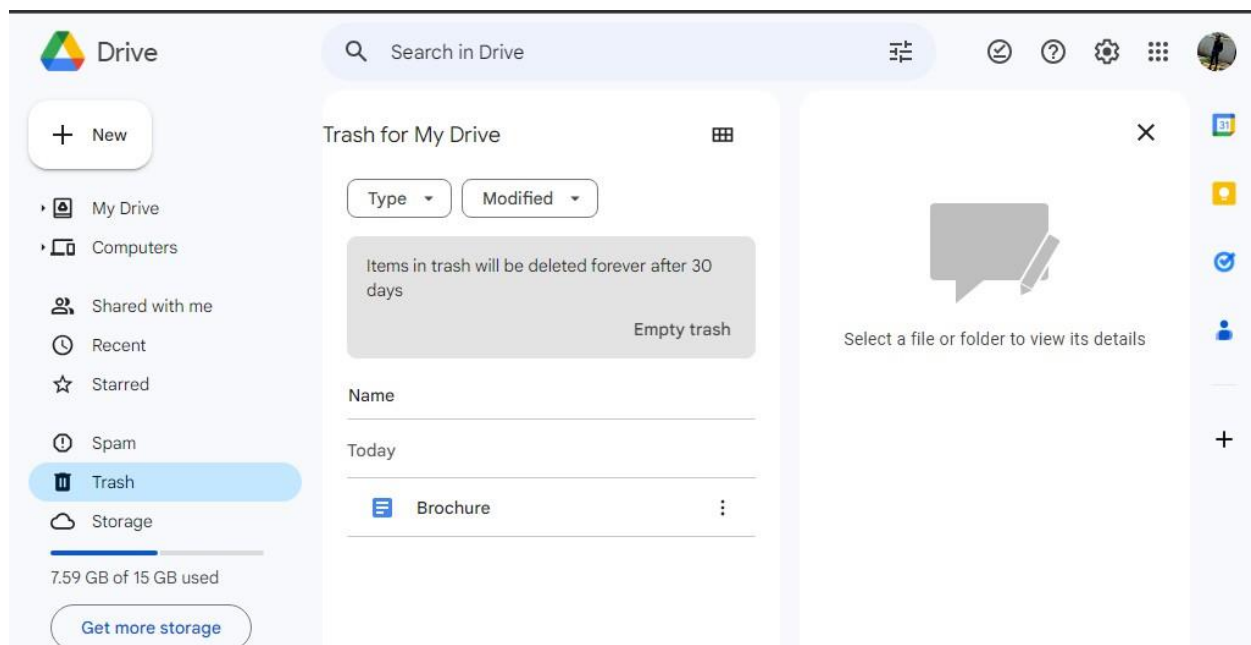
- Other files created during installation by google drive.



- In the URL address bar, enter ; <https://www.google.co.in/drive> once the homepage appears, click on go to drive.

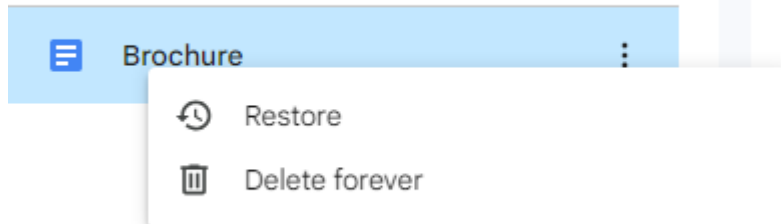


- Click on trash on the left pane to view deleted files.

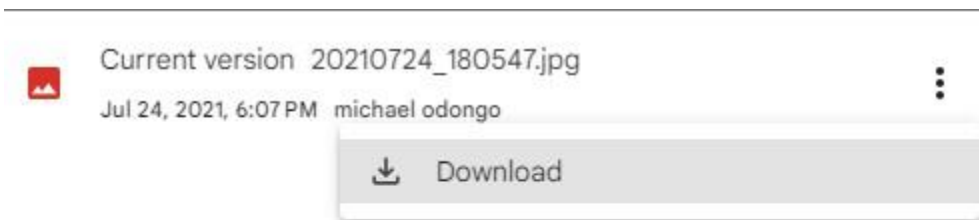


- In the trash section, right click on any image to see options such as: Restore and Delete Forever.

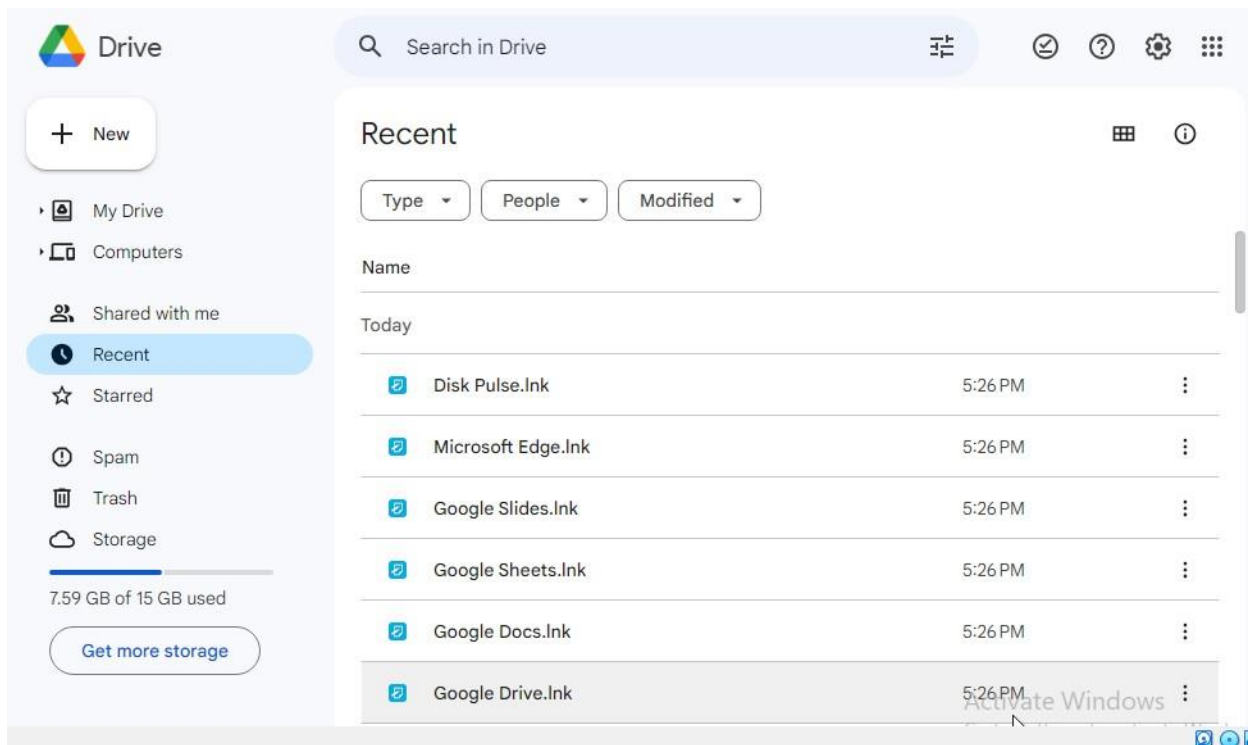
Today



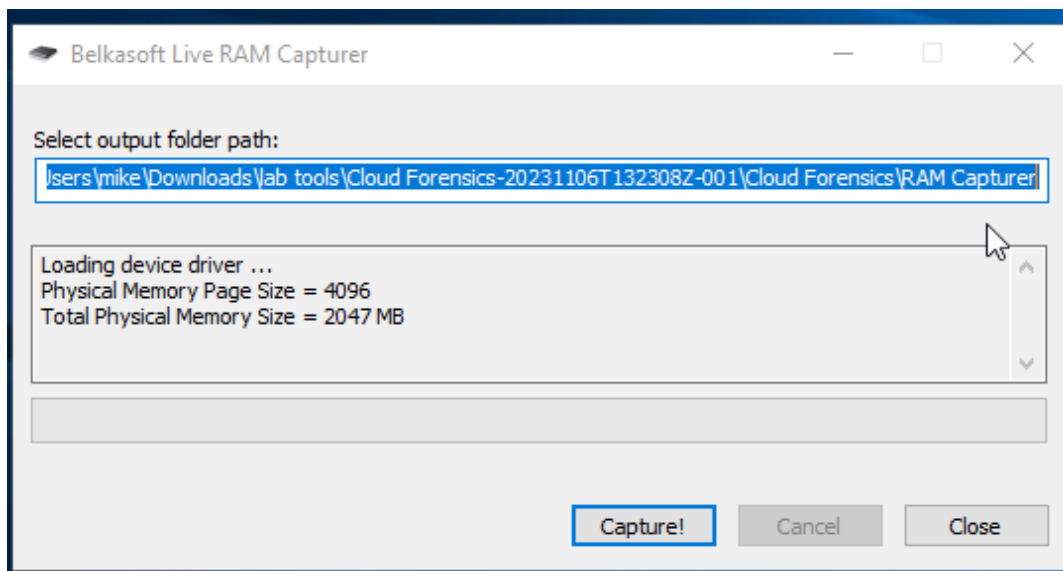
- In my drive section, right click on any image and click on manage versions option to see its versions. In the manage versions, click on the ellipsis on the far right to download the file.



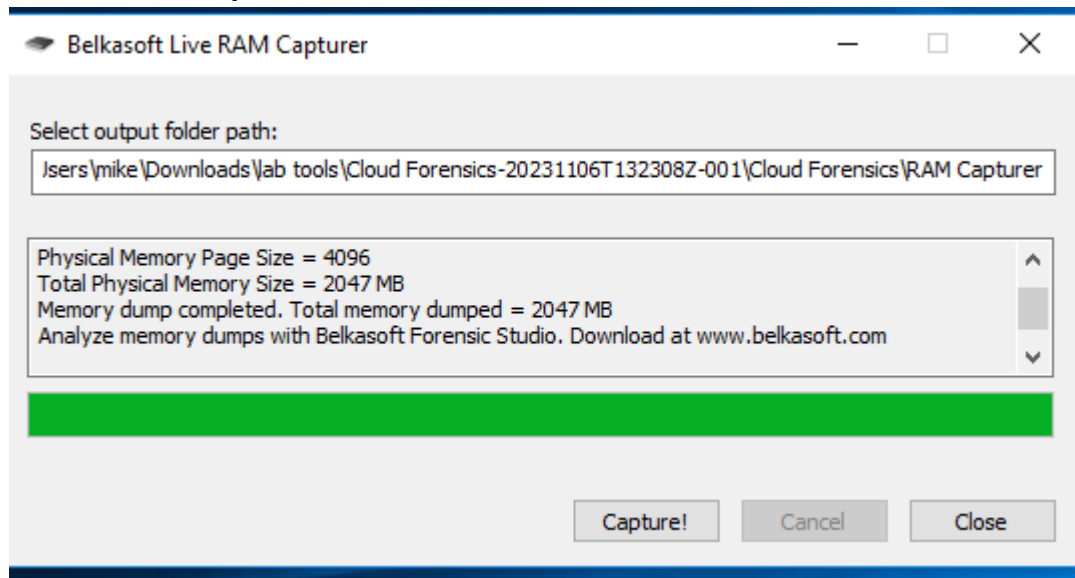
- Click on the recent in the left pane to view the recently accessed files.



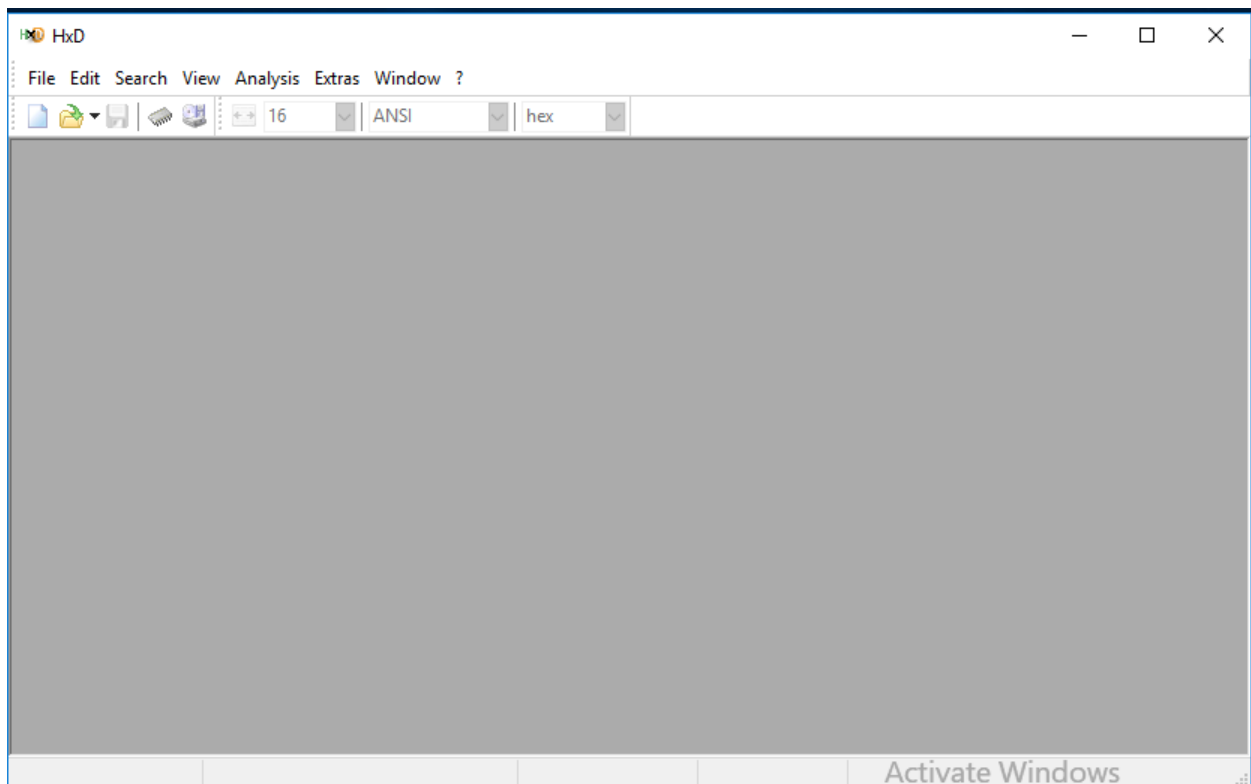
- Launch the RAM capturer.



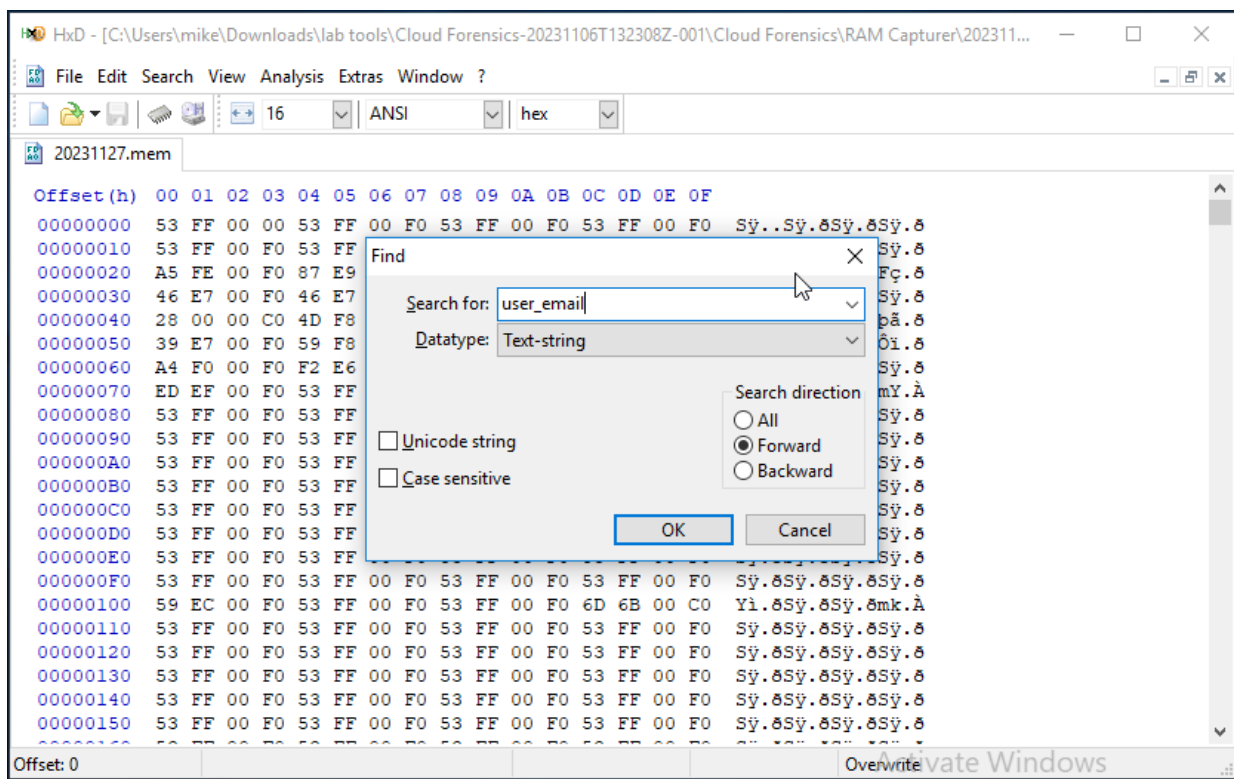
- Click on the capture button and once done click on close.



- Launch the HxD tool and click on open icon to view hex value of captured RAM data.



- Access the find dialog box using Ctrl + F.



- Launch disk pulse and click on monitor.

The screenshot shows the Disk Pulse application window. The interface includes a menu bar (File, Command, Tools, Help), a toolbar with icons for Monitor, Continue, Pause, Stop, Reset, Save, Database, Charts, Rate, Layouts, Options, and Help, and a main data display area.

Profiles: Default Profile

Directories: C:\

Status:

Status	Value
Total Chan...	67
Excluded Fi...	0
Change Rate	484 CH/Min
Process Ti...	8.31 Sec

File Categories:

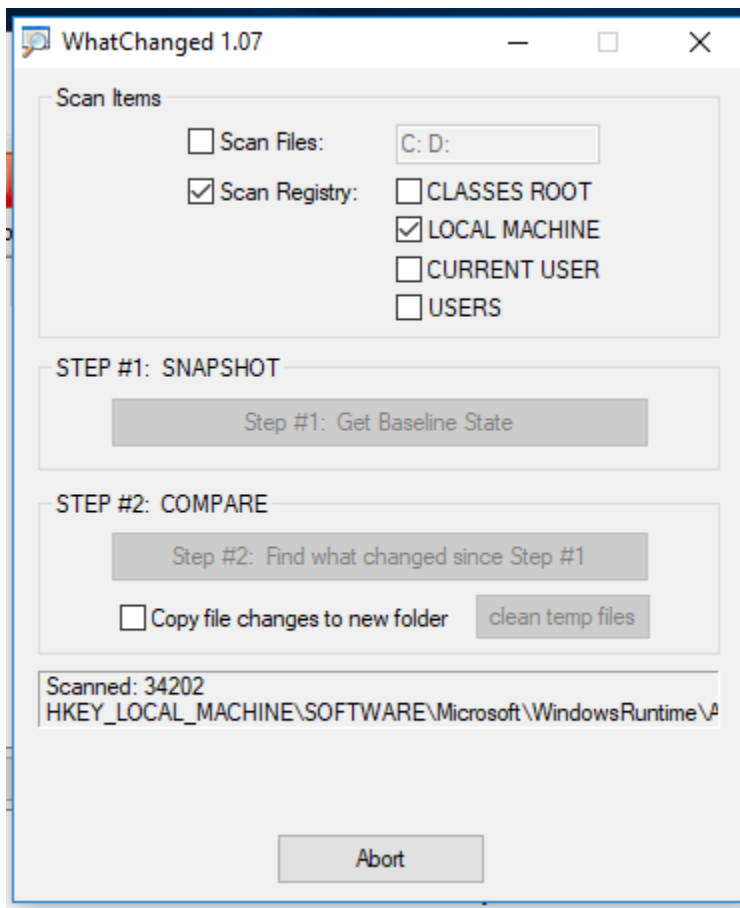
File Categories	Count	Percentage
NOEXT Files	31	43.66 %
TMP Files	13	18.31 %
LEVELDB Files	13	18.31 %
LOG Files	3	4.23 %
DBTMP Files	3	4.23 %
PF Files	3	4.23 %

Main Data Table:

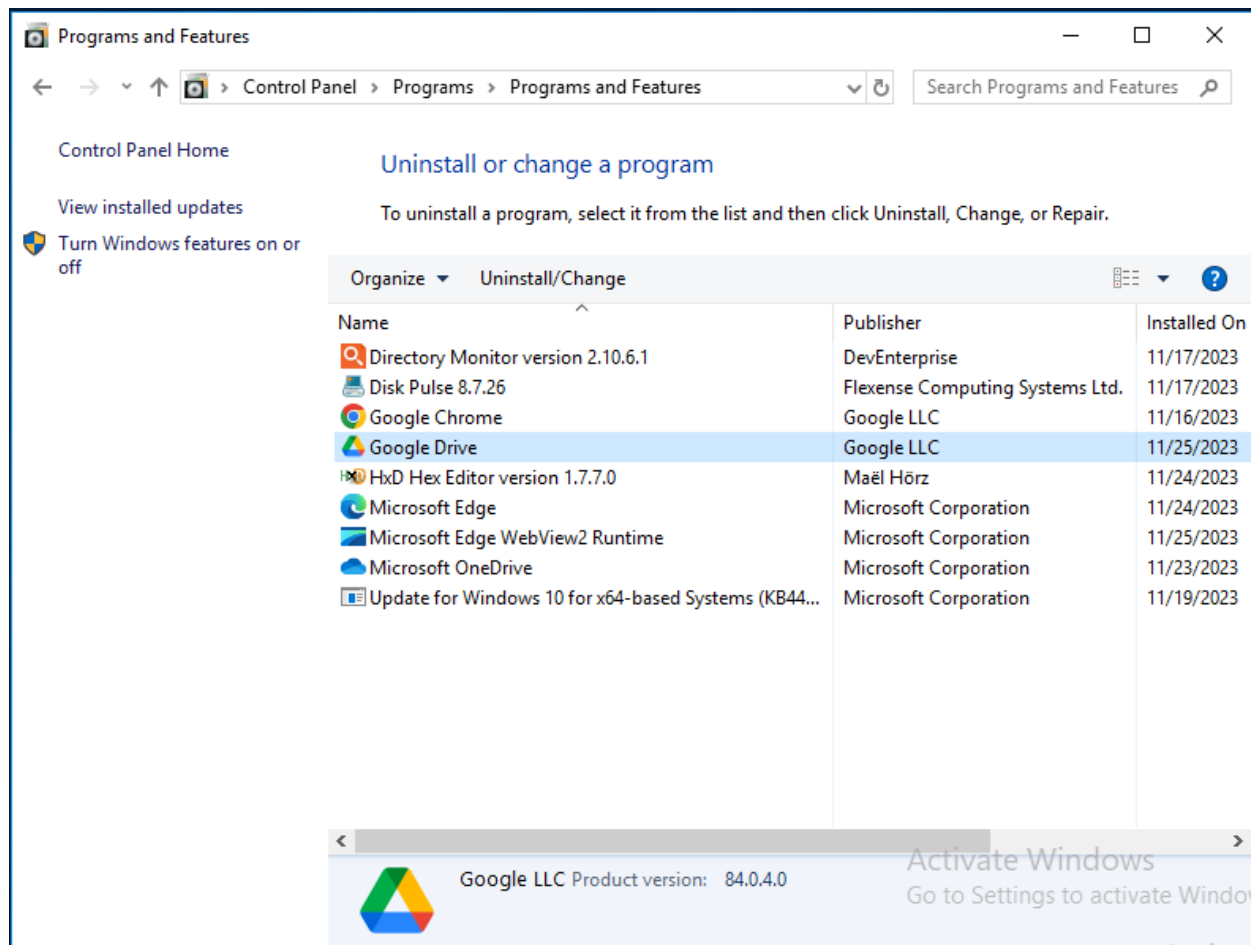
Date	Time	Operation	Size	Owner	Name
27-Nov-2023	12:33:19	Created	0 Bytes	---	C:\ProgramData\Micros...
27-Nov-2023	12:33:19	Modified	0 Bytes	---	C:\ProgramData\Micros...
27-Nov-2023	12:33:19	Created	0 Bytes	---	C:\ProgramData\Micros...
27-Nov-2023	12:33:19	Modified	0 Bytes	---	C:\ProgramData\Micros...
27-Nov-2023	12:33:21	Modified	0 Bytes	SYSTEM	C:\Windows\Prefetch\A...
27-Nov-2023	12:33:22	Deleted	0 Bytes	---	C:\Users\mike\Downloa...
27-Nov-2023	12:33:22	Modified	0 Bytes	mike	C:\Users\mike\Downloa...
27-Nov-2023	12:33:22	Created	0 Bytes	mike	C:\Users\mike\Downloa...
27-Nov-2023	12:33:22	Modified	0 Bytes	mike	C:\Users\mike\Downloa...
27-Nov-2023	12:33:23	Modified	0 Bytes	SYSTEM	C:\Windows\Prefetch\C...
27-Nov-2023	12:33:23	Created	0 Bytes	mike	C:\Users\mike\AppData\...
27-Nov-2023	12:33:25	Modified	0 Bytes	mike	C:\Users\mike\AppData\...
27-Nov-2023	12:33:25	Modified	28.22 KB	mike	C:\Users\mike\AppData\...

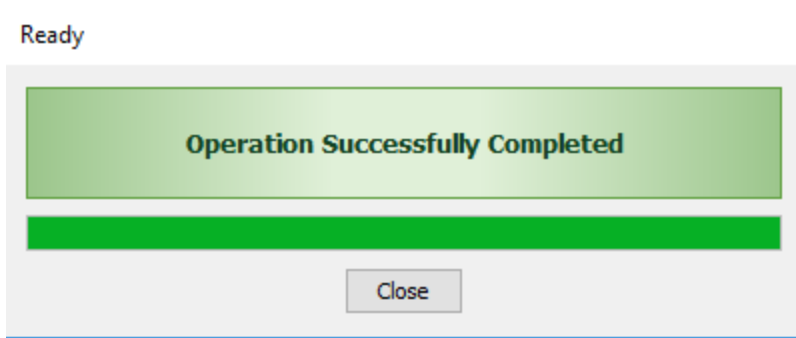
Footer: Active | Total: 67 Changes | Current: 67 Changes | Filtered: NA | Change Rate: 484 CH/Min

- Launch WhatChanged and click on 'Get Baseline state'.

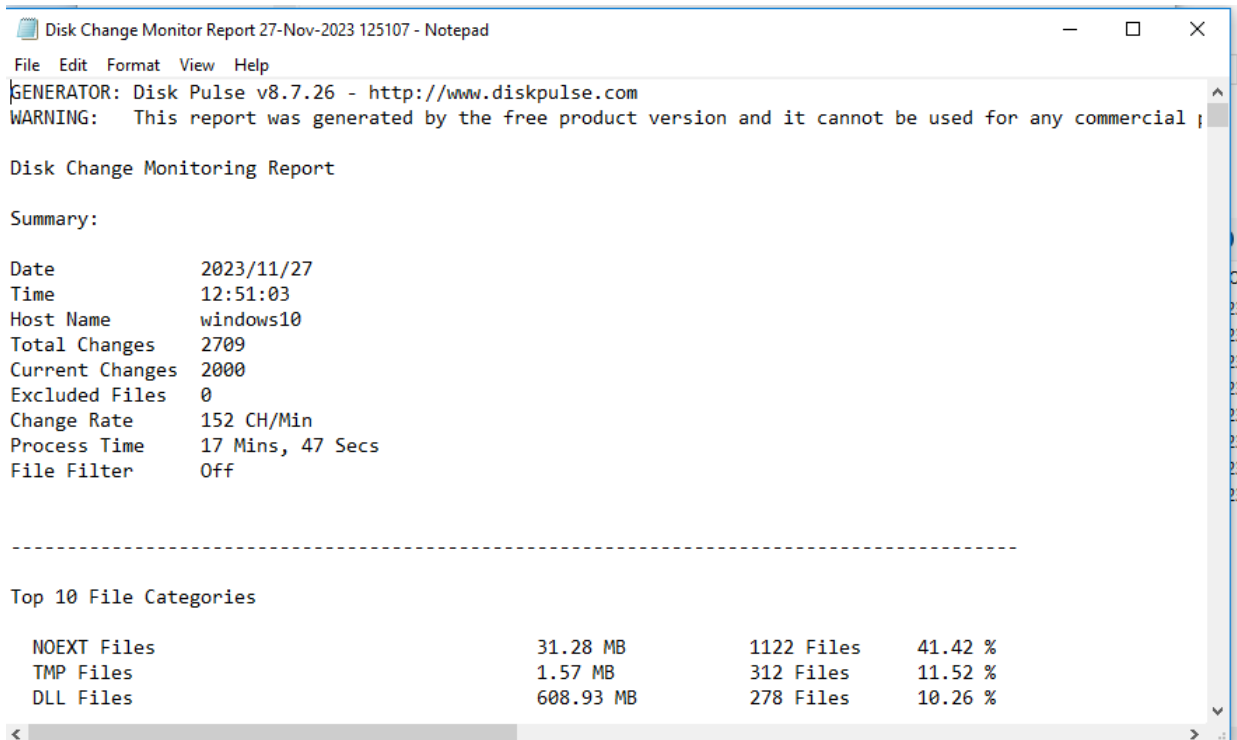


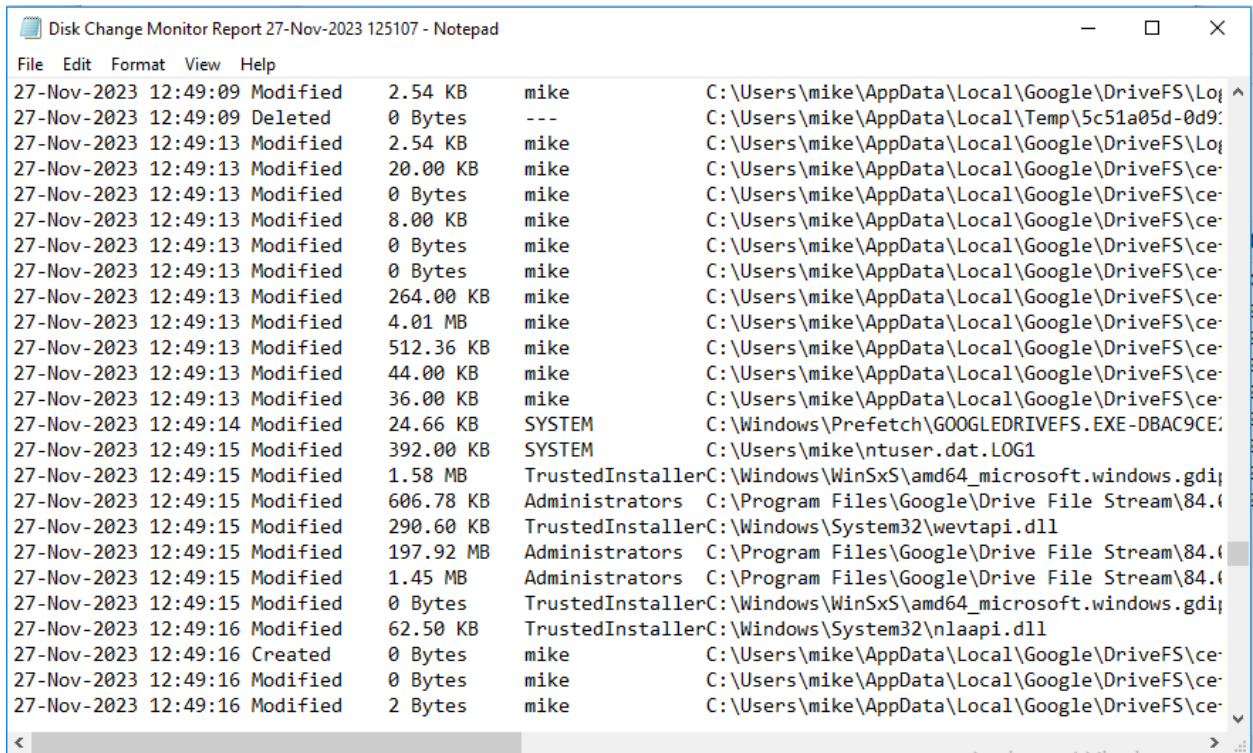
- Navigate to control panel, under the programs click on uninstall a program and double click on google drive to uninstall.





- **Output text by disk pulse, including all the modified files and folders.**





- **Screenshot of Googles Program's files directory(Drive folder) disappears after uninstalling the client.**

