DROPBOX AND GOOGLE DRIVE INVESTIGATION

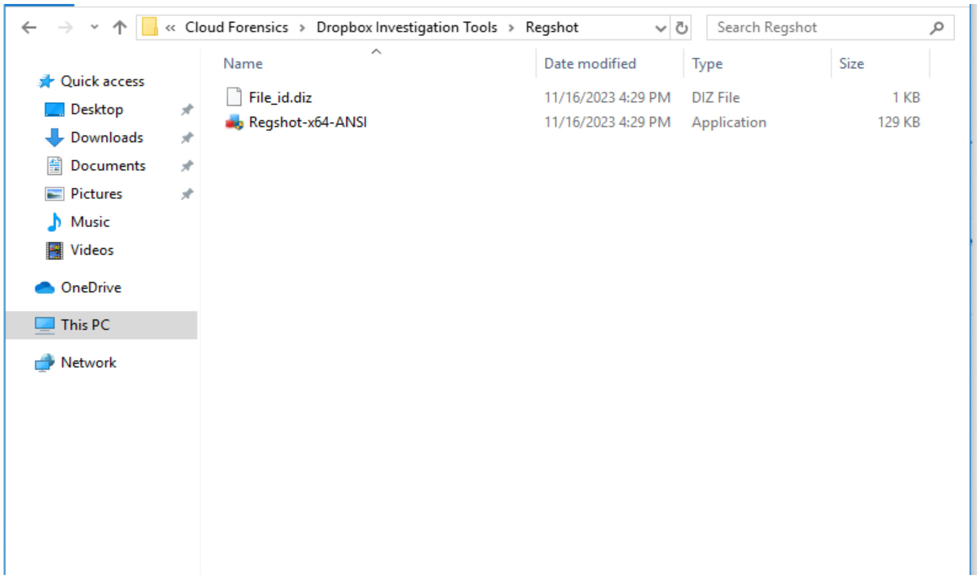
By

MICHAEL EDMOND ODONGO

JJJJ

DROPBOX INVESTIGATION

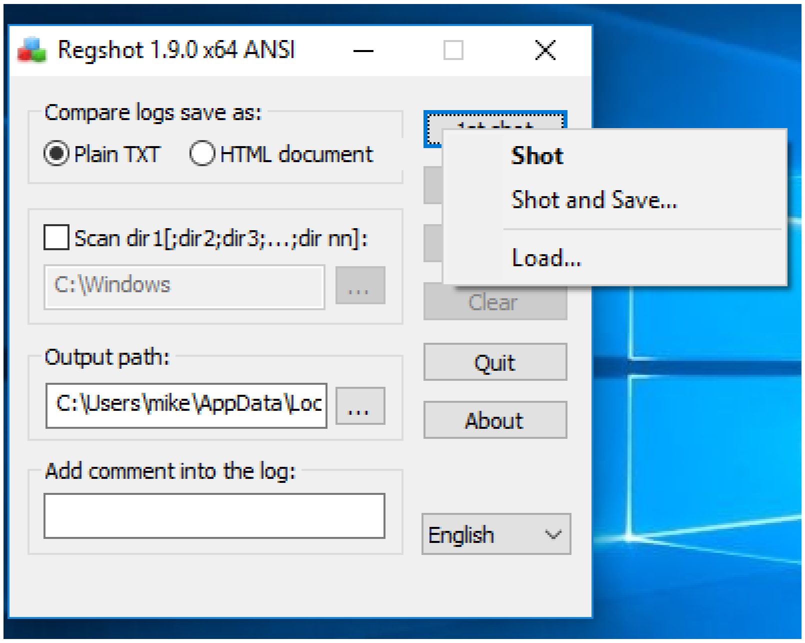
- **Navigate to the folder and double click the .exe file for the Regshot to launch the application.**



« Cloud Forensics › Dropbox Investigation Tools › Regshot

Name	Date modified	Type	Size
File_id.diz	11/16/2023 4:29 PM	DIZ File	1 KB
Regshot-x64-ANSI	11/16/2023 4:29 PM	Application	129 KB

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



Regshot 1.9.0 x64 ANSI

Compare logs save as:

● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

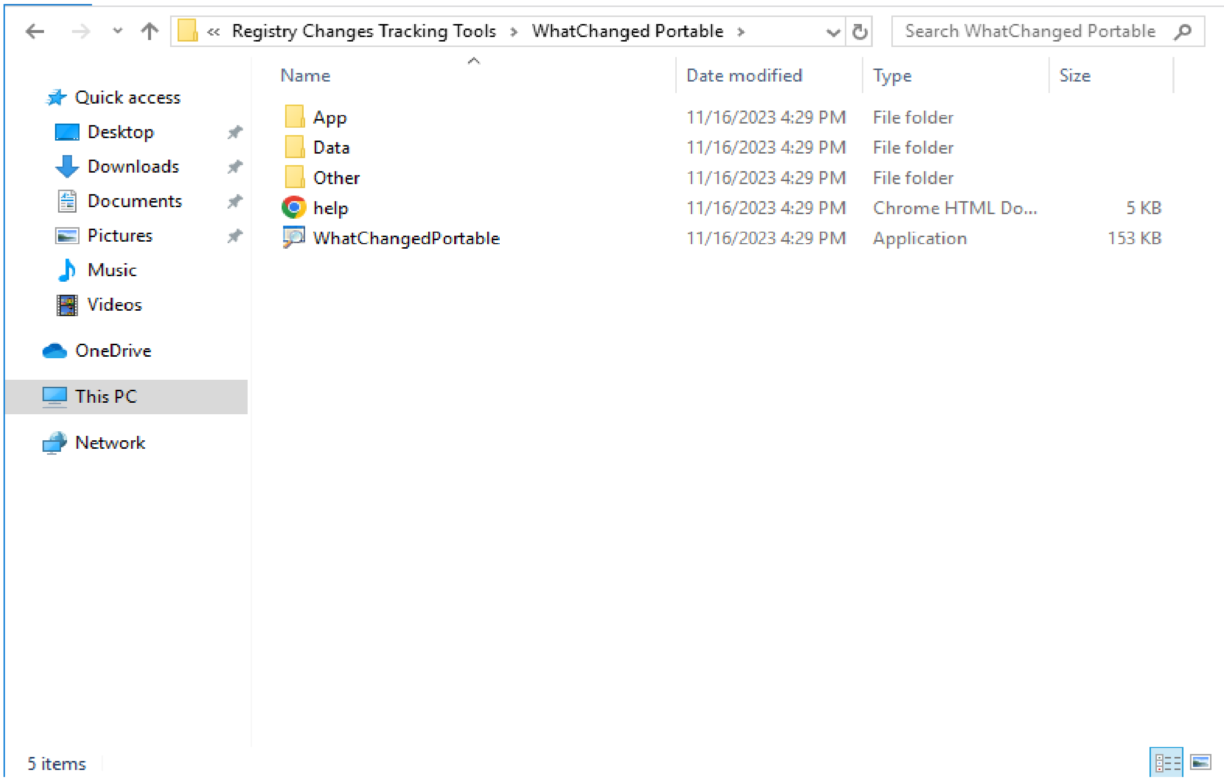
C:\Windows

Output path:

C:\Users\mike\AppData\Loc

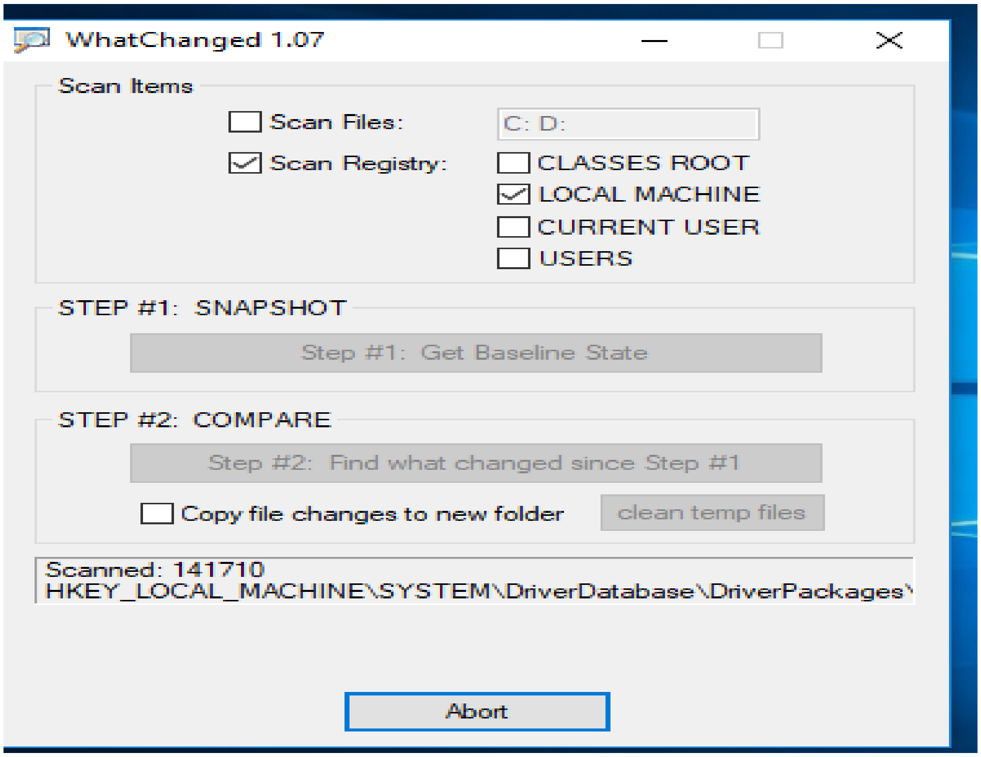
Add comment into the log:

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


« Registry Changes Tracking Tools › WhatChanged Portable ›
Search WhatChanged Portable
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
5 items

Name	Date modified	Type	Size
App	11/16/2023 4:29 PM	File folder	
Data	11/16/2023 4:29 PM	File folder	
Other	11/16/2023 4:29 PM	File folder	
help	11/16/2023 4:29 PM	Chrome HTML Do...	5 KB
WhatChangedPortable	11/16/2023 4:29 PM	Application	153 KB

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



WhatChanged 1.07

Scan Items

□ Scan Files: C: D:

☑ Scan Registry:

□ CLASSES ROOT

☑ LOCAL MACHINE

□ CURRENT USER

□ USERS

STEP #1: SNAPSHOT

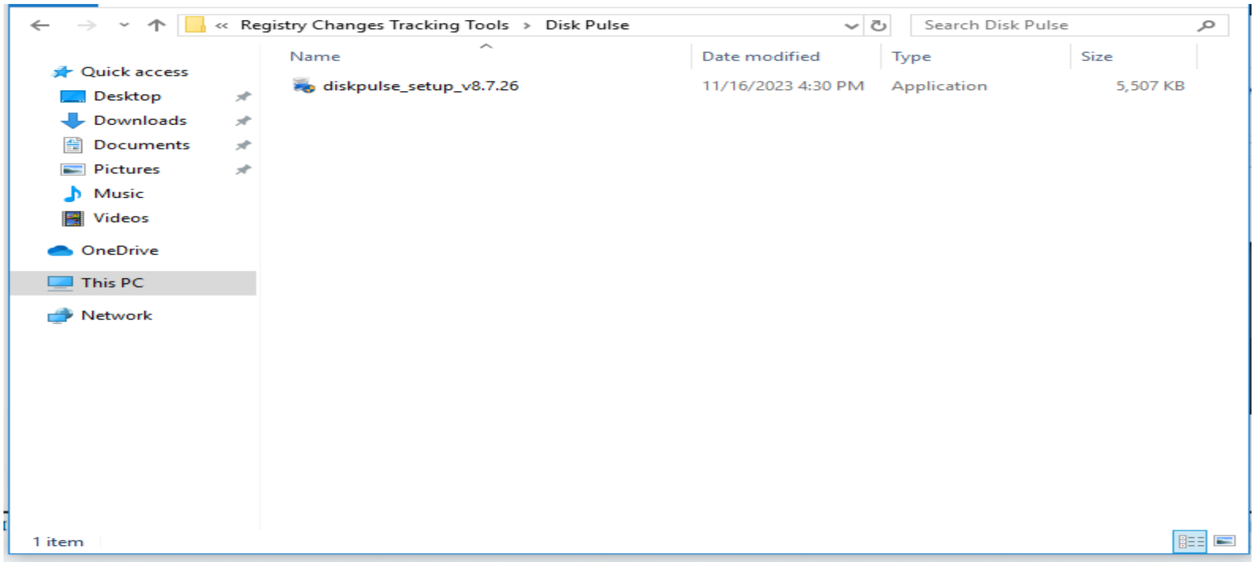
STEP #2: COMPARE

□ Copy file changes to new folder

```
Scanned: 141710
HKEY_LOCAL_MACHINE\SYSTEM\DriverDatabase\DriverPackages\
```

Step #1: Get Baseline State
Step #2: Find what changed since Step #1
clean temp files
Abort

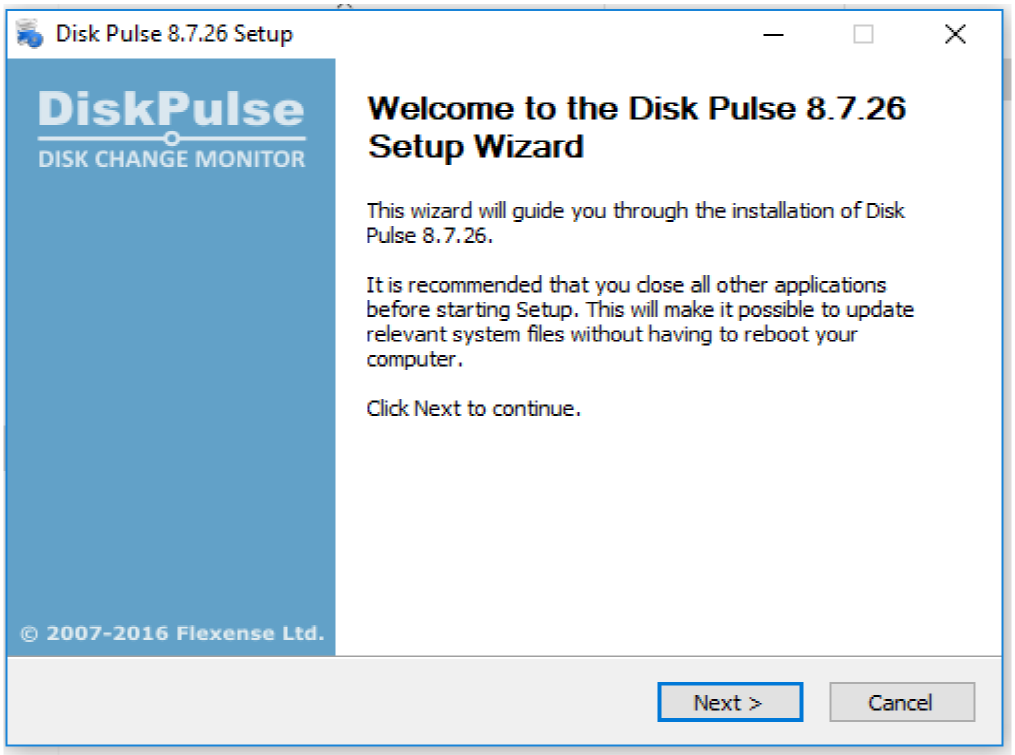
- **Navigate to the folder containing the Disk pulse executable, double click to launch it.**



Name	Date modified	Type	Size
diskpulse_setup_v8.7.26	11/16/2023 4:30 PM	Application	5,507 KB

1 item

- **The following wizard is displayed.**



Disk Pulse 8.7.26 Setup

Welcome to the Disk Pulse 8.7.26 Setup Wizard

This wizard will guide you through the installation of Disk Pulse 8.7.26.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

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

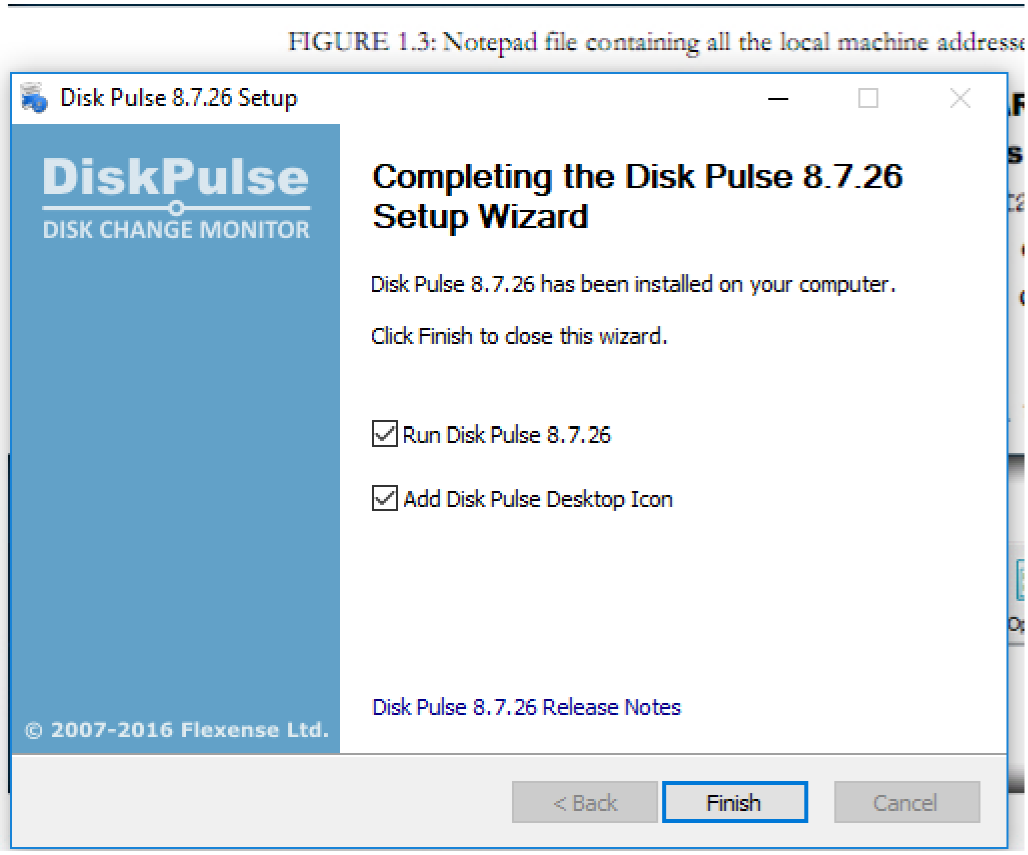


FIGURE 1.3: Notepad file containing all the local machine addresse

Disk Pulse 8.7.26 Setup

Completing the Disk Pulse 8.7.26 Setup Wizard

Disk Pulse 8.7.26 has been installed on your computer.

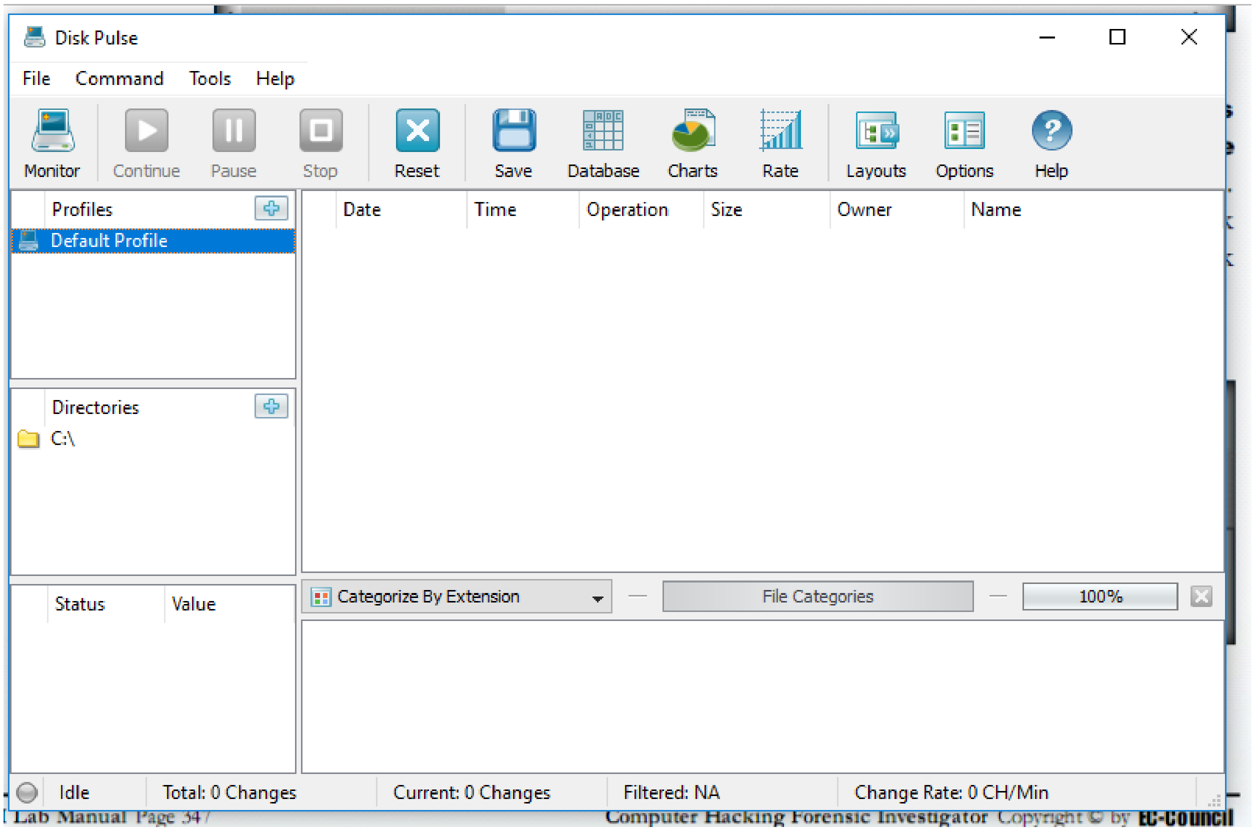
Click Finish to close this wizard.

☑ Run Disk Pulse 8.7.26

☑ Add Disk Pulse Desktop Icon

Disk Pulse 8.7.26 Release Notes

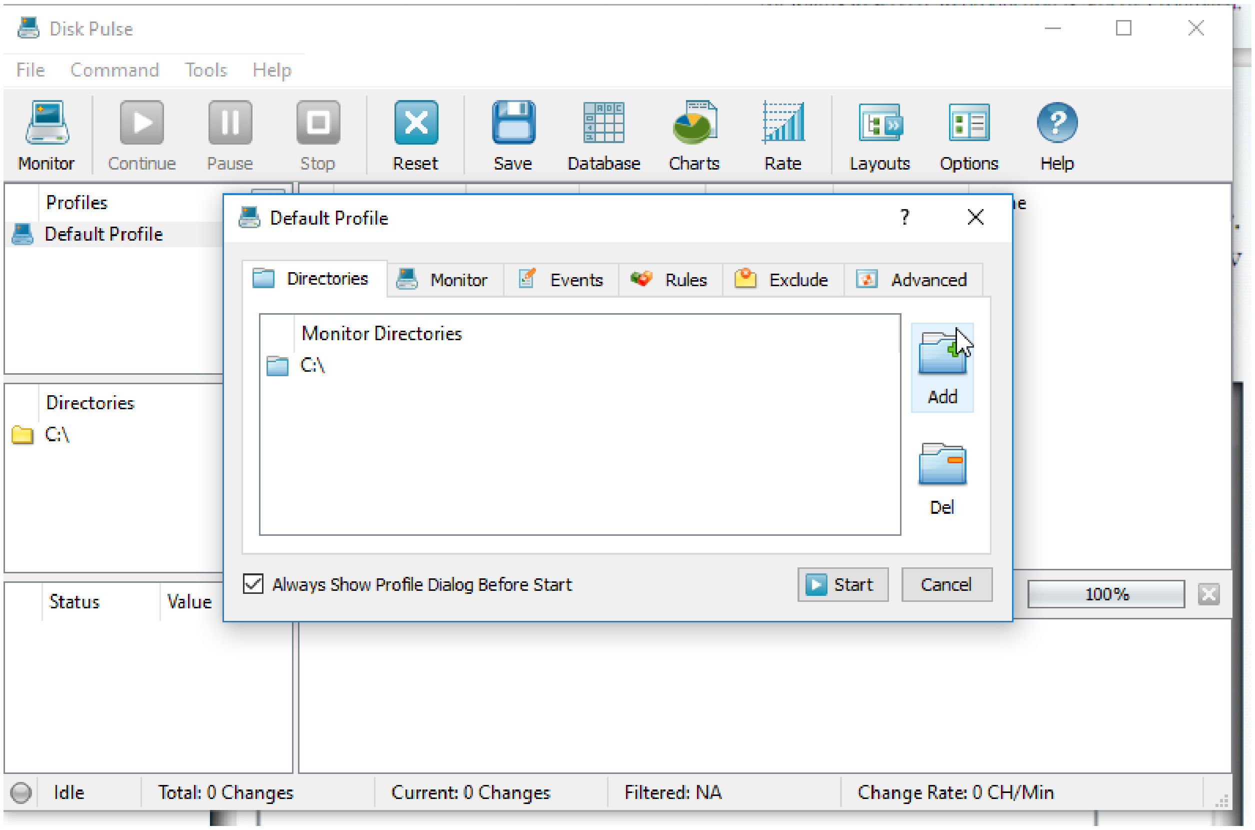
- **Disk Pulse graphical user interface is displayed as below once launched.**



Idle | Total: 0 Changes | Current: 0 Changes | Filtered: NA | Change Rate: 0 CH/Min

Lab Manual Page 347
Computer Hacking Forensic Investigator Copyright © by EC-Council

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

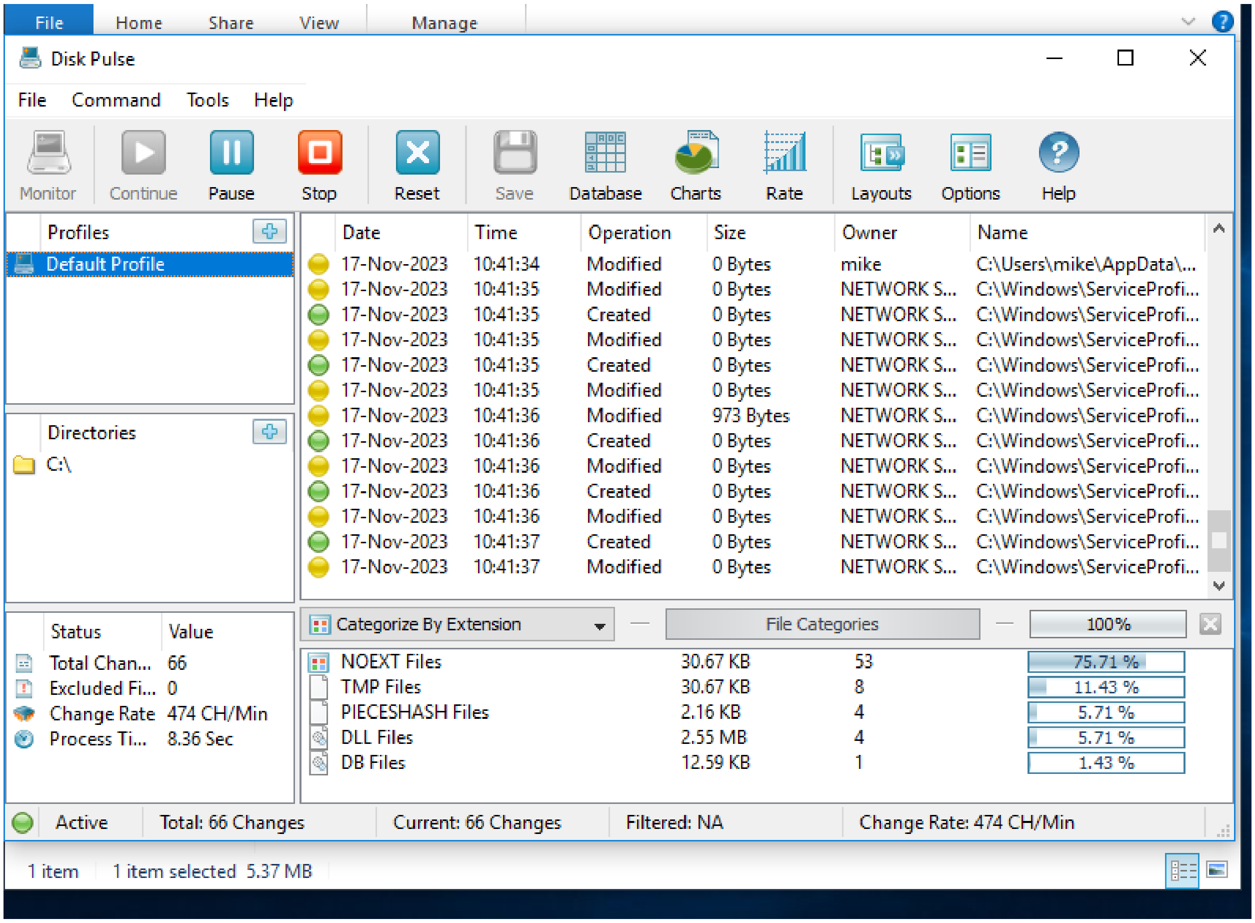

Disk Pulse
File Command Tools Help
Monitor Continue Pause Stop Reset Save Database Charts Rate Layouts Options Help
Profiles
Default Profile
Directories
C:\
Status Value
Default Profile
?
Directories Monitor Events Rules Exclude Advanced
Add
Del
Start
Cancel
100%

Monitor Directories
C:\

☑ Always Show Profile Dialog Before Start

Idle | Total: 0 Changes | Current: 0 Changes | Filtered: NA | Change Rate: 0 CH/Min

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



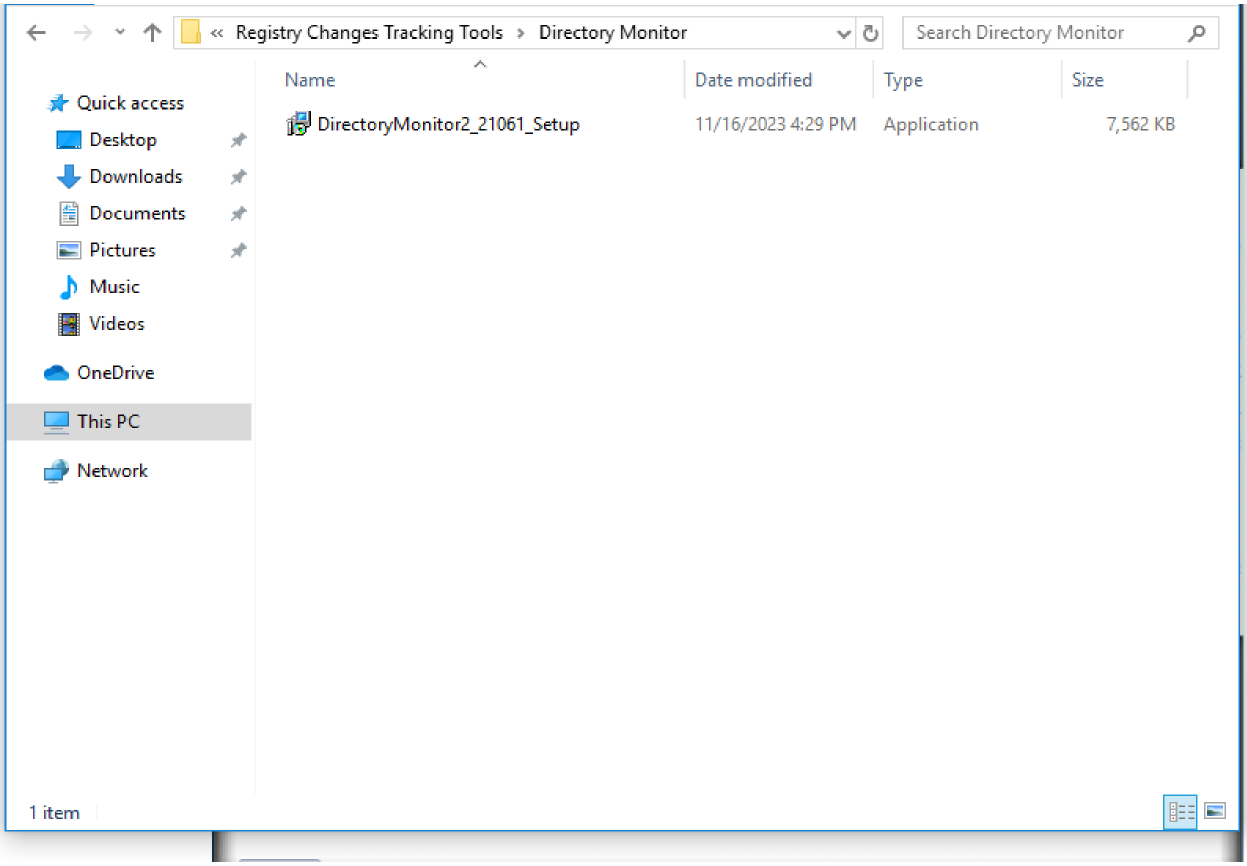
Date	Time	Operation	Size	Owner	Name
17-Nov-2023	10:41:34	Modified	0 Bytes	mike	C:\Users\mike\AppData\...
17-Nov-2023	10:41:35	Modified	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:35	Created	0 Bytes	NETWORK S...	C:\Windows\ServiceProfi...
17-Nov-2023	10:41:35	Modified	0 Bytes	NETWORK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

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

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 %

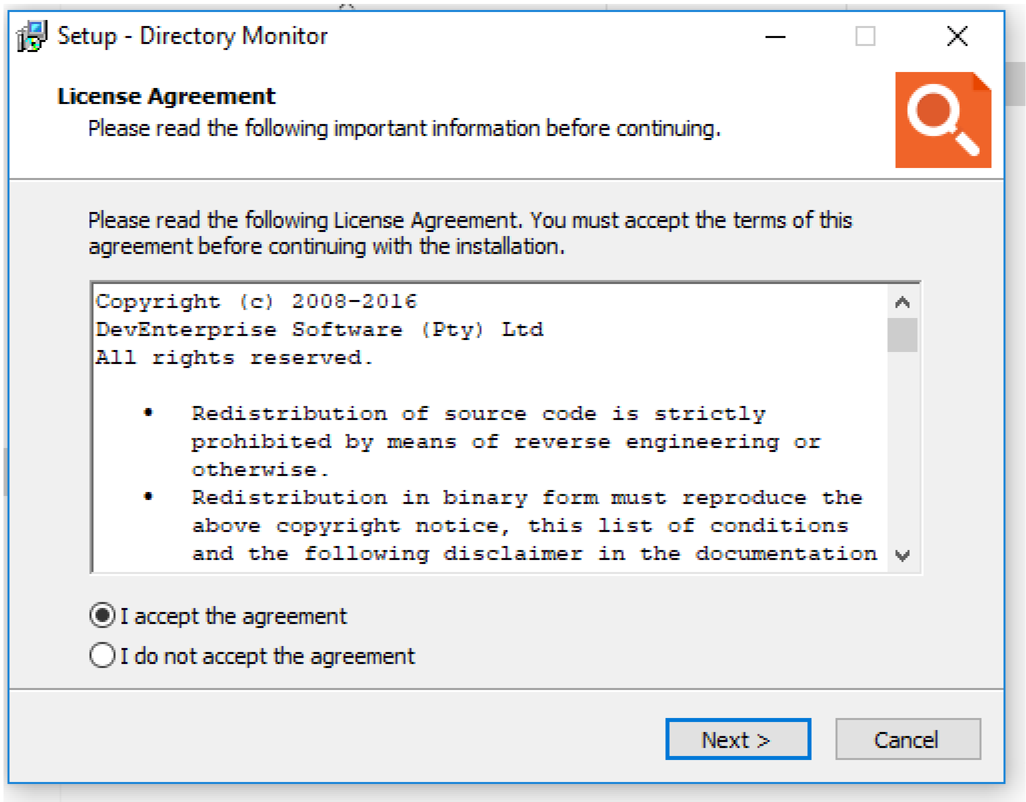
Active | Total: 66 Changes | Current: 66 Changes | Filtered: NA | Change Rate: 474 CH/Min

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



Name	Date modified	Type	Size
DirectoryMonitor2_21061_Setup	11/16/2023 4:29 PM	Application	7,562 KB

1 item



Setup - Directory Monitor

License Agreement

Please read the following important information before continuing.

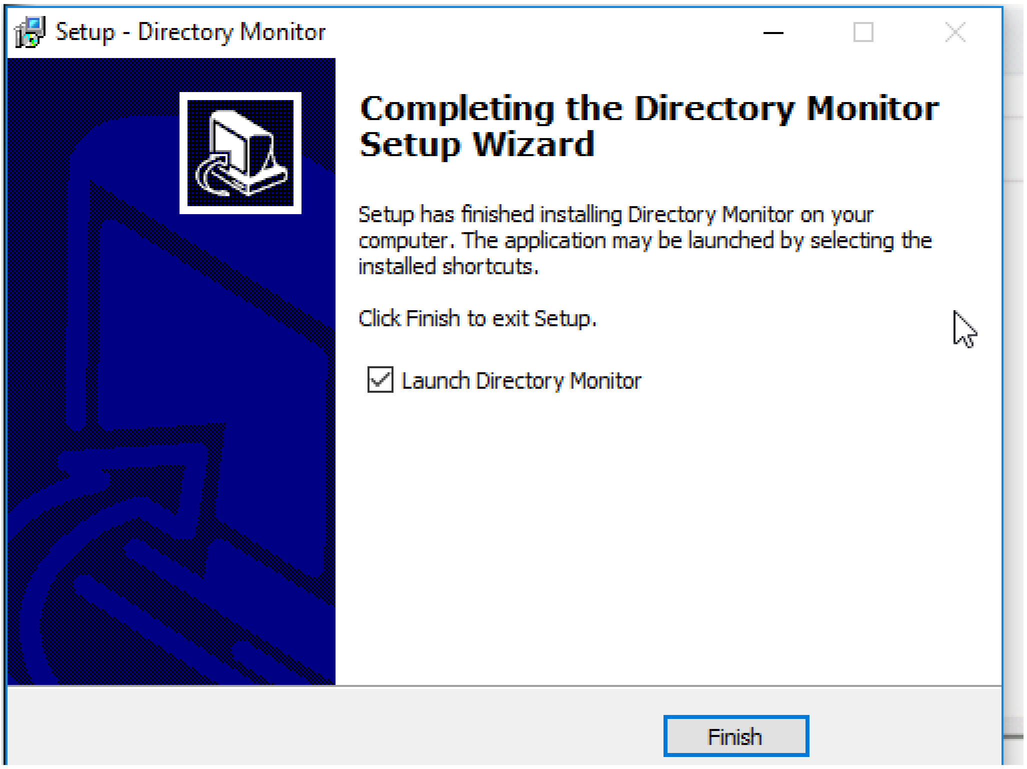
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

```
Copyright (c) 2008-2016
DevEnterprise Software (Pty) Ltd
All rights reserved.

   •  Redistribution of source code is strictly
      prohibited by means of reverse engineering or
      otherwise.
   •  Redistribution in binary form must reproduce the
      above copyright notice, this list of conditions
      and the following disclaimer in the documentation
```

● I accept the agreement

○ I do not accept the agreement

- **Follow the wizard below.**



Setup - Directory Monitor

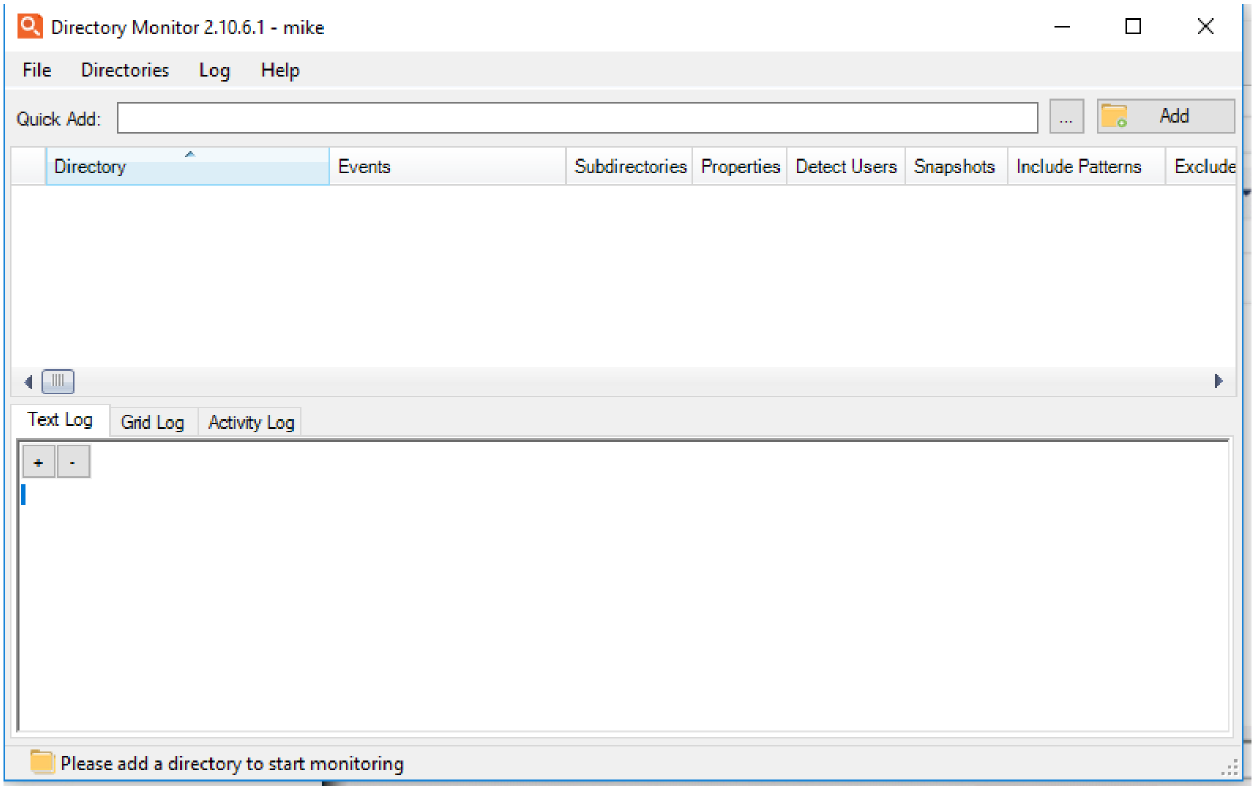
Completing the Directory Monitor Setup Wizard

Setup has finished installing Directory Monitor on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

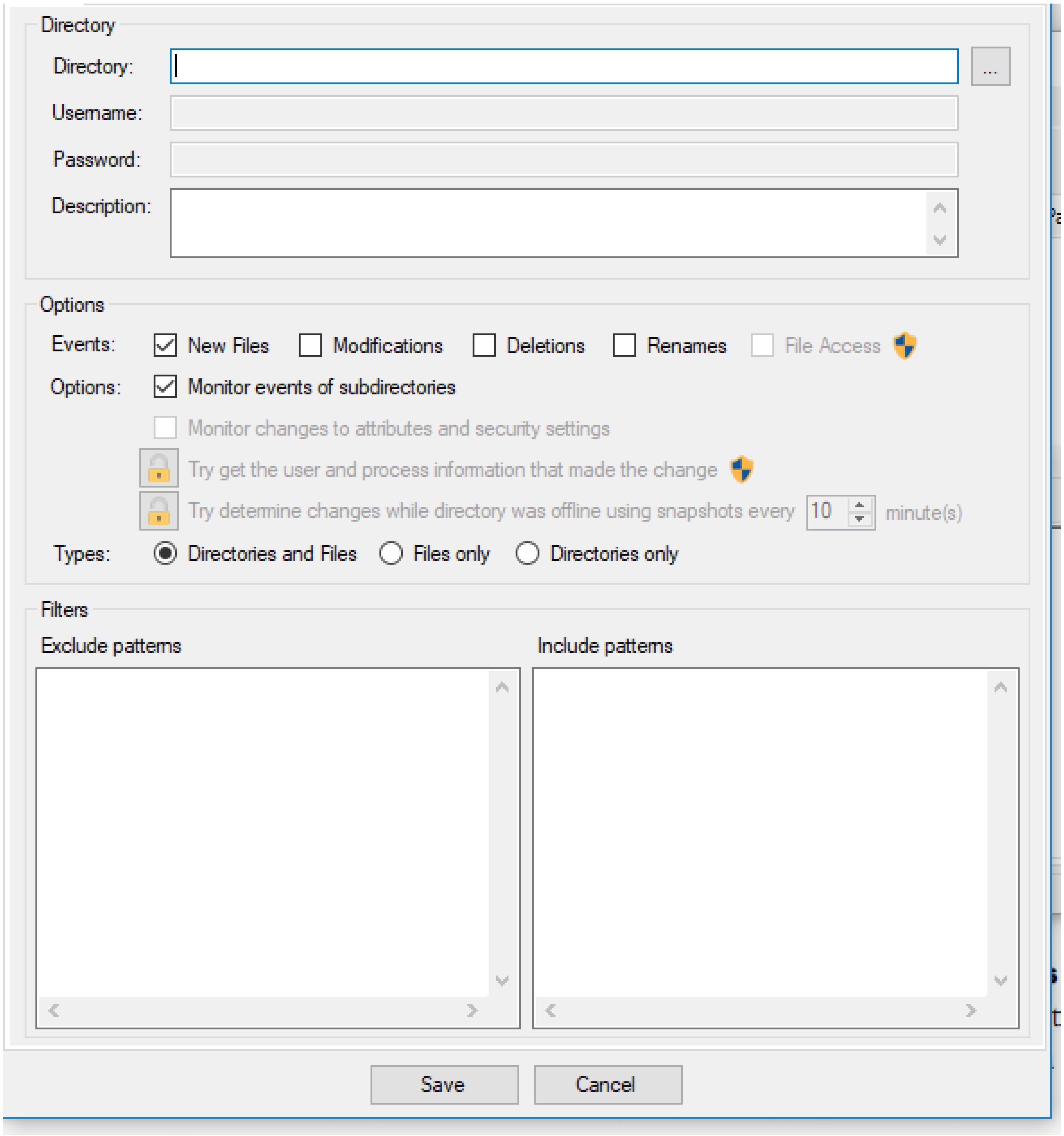
☑ Launch Directory Monitor

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



Please add a directory to start monitoring

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



Directory

Directory:

Username:

Password:

Description:

Options

Events: ☑ New Files □ Modifications □ Deletions □ Renames □ File Access

Options: ☑ Monitor events of subdirectories

□ Monitor changes to attributes and security settings

Try get the user and process information that made the change

Try determine changes while directory was offline using snapshots every 10 minute(s)

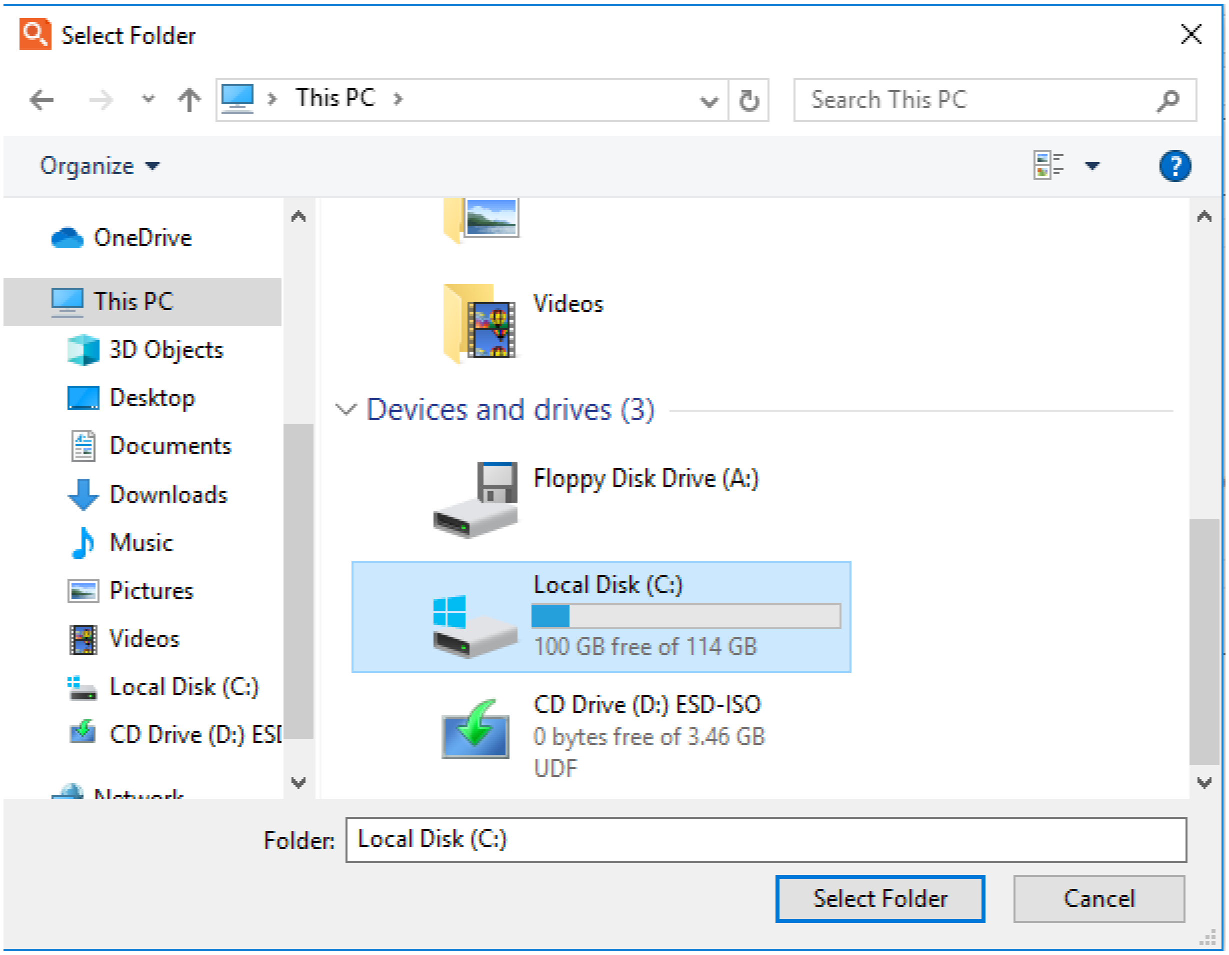
Types: ● Directories and Files ○ Files only ○ Directories only

Filters

Exclude patterns

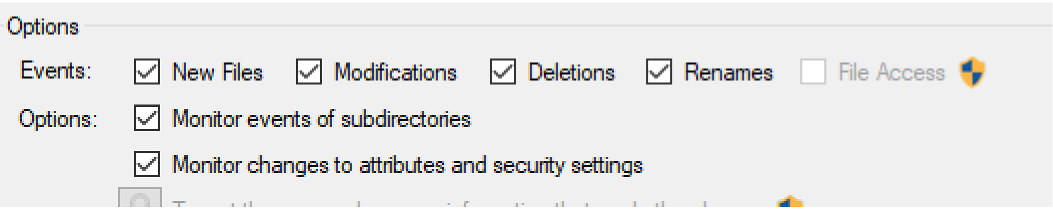
Include patterns

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



Folder: Local Disk (C:)

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

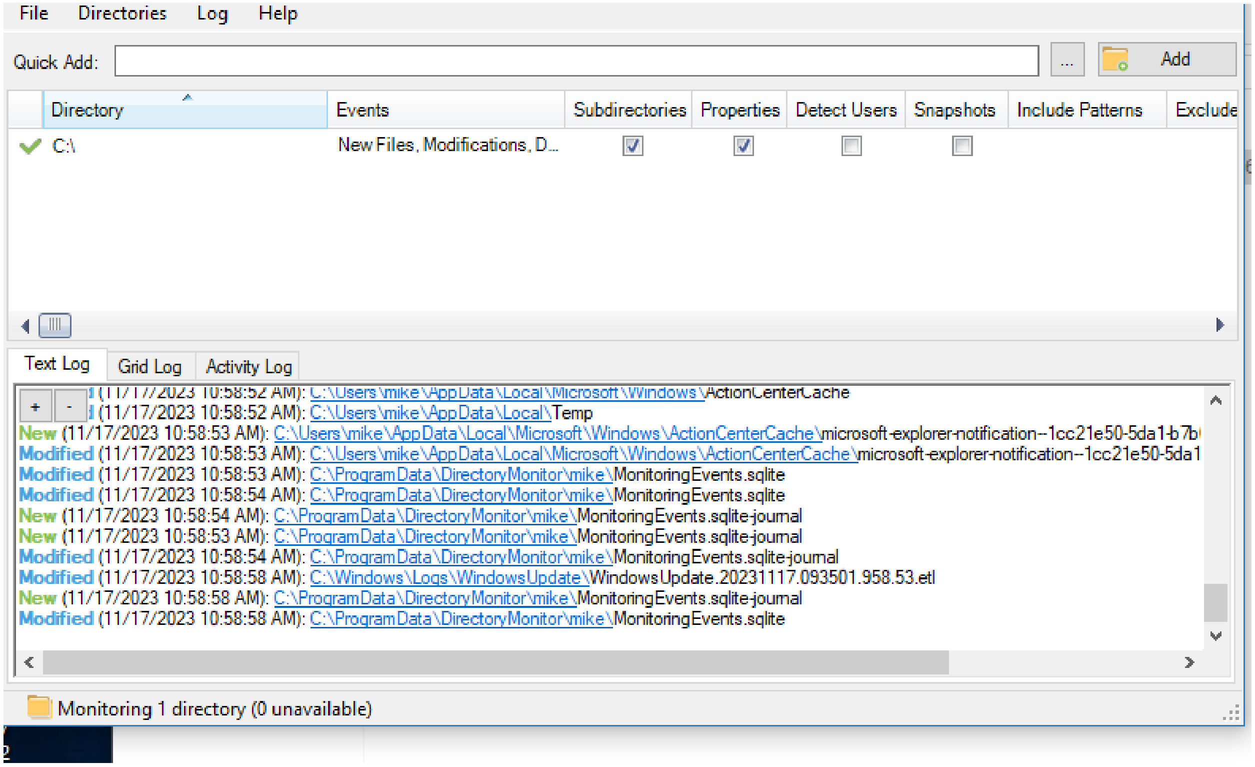


Events: ☑ New Files ☑ Modifications ☑ Deletions ☑ Renames □ File Access

Options: ☑ Monitor events of subdirectories

☑ Monitor changes to attributes and security settings

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

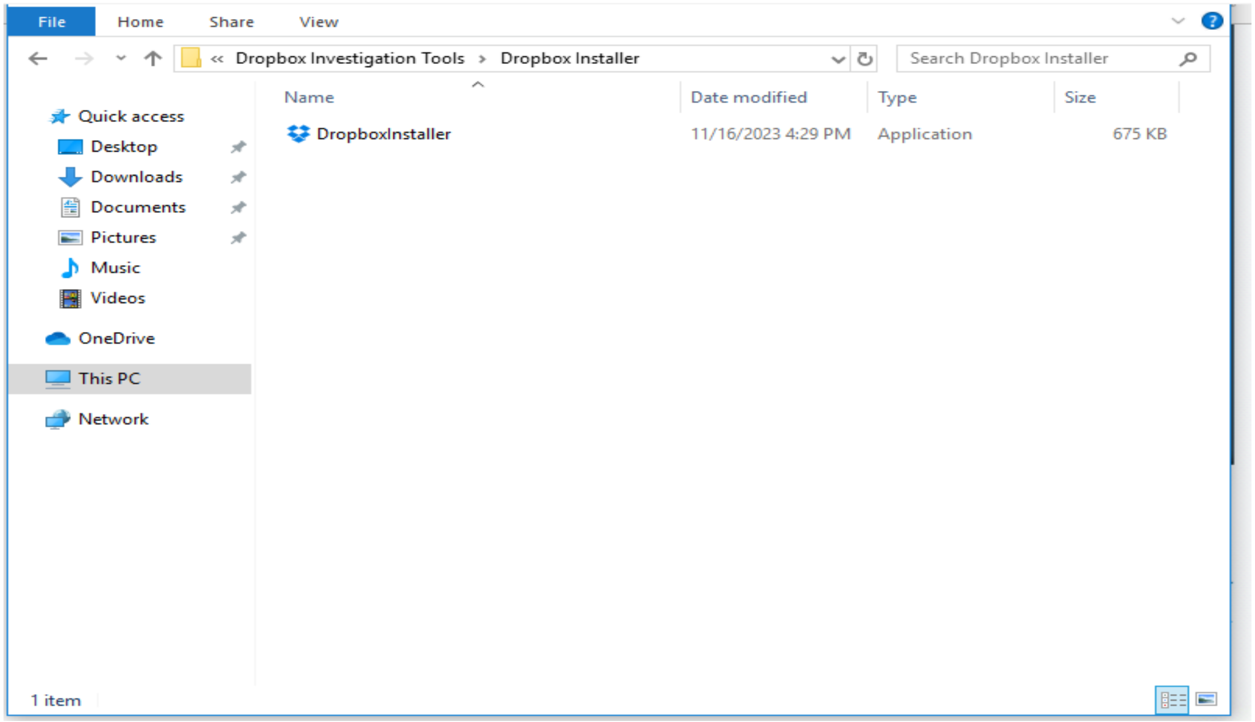


Directory	Events	Subdirectories	Properties	Detect Users	Snapshots	Include Patterns	Exclude
✓ C:\	New Files, Modifications, D...	☑	☑	□	□		

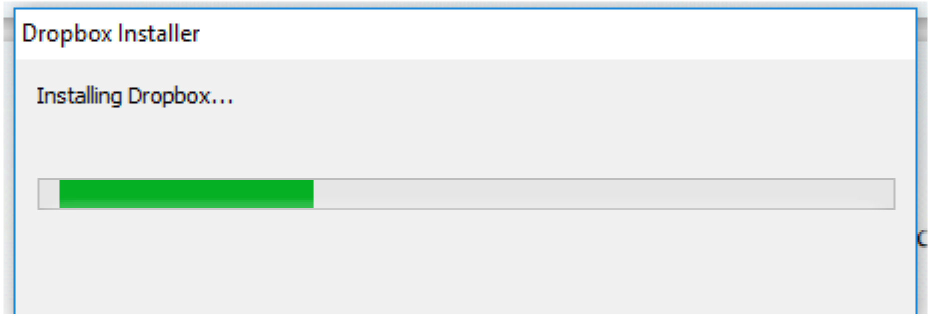
```
(11/17/2023 10:58:52 AM): C:\Users\mike\AppData\Local\Microsoft\Windows\ActionCenterCache
(11/17/2023 10:58:52 AM): C:\Users\mike\AppData\Local\Temp
New (11/17/2023 10:58:53 AM): C:\Users\mike\AppData\Local\Microsoft\Windows\ActionCenterCache\microsoft-explorer-notification--1cc21e50-5da1-b7b
Modified (11/17/2023 10:58:53 AM): C:\Users\mike\AppData\Local\Microsoft\Windows\ActionCenterCache\microsoft-explorer-notification--1cc21e50-5da1
Modified (11/17/2023 10:58:53 AM): C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite
Modified (11/17/2023 10:58:54 AM): C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite
New (11/17/2023 10:58:54 AM): C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
New (11/17/2023 10:58:53 AM): C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
Modified (11/17/2023 10:58:54 AM): C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
Modified (11/17/2023 10:58:58 AM): C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20231117.093501.958.53.etl
New (11/17/2023 10:58:58 AM): C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite-journal
Modified (11/17/2023 10:58:58 AM): C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite
```

Monitoring 1 directory (0 unavailable)

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



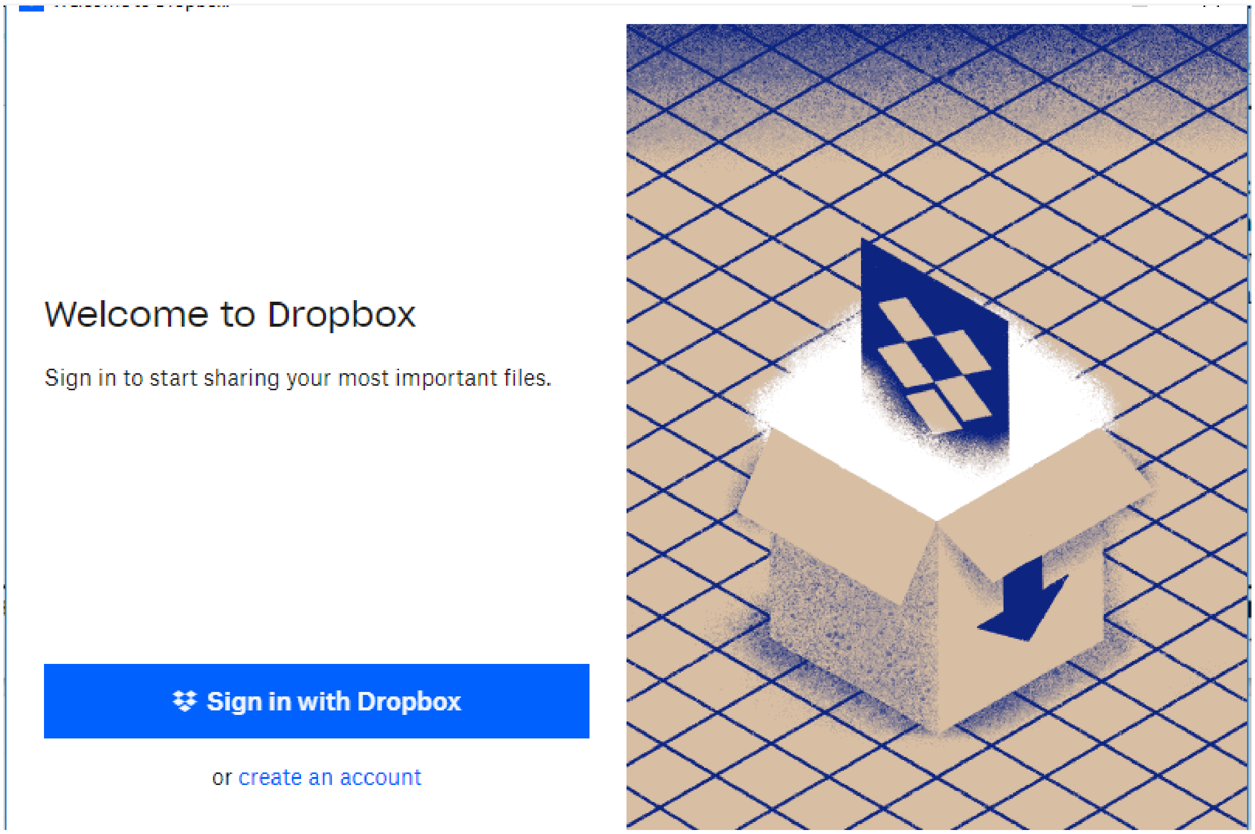
Name	Date modified	Type	Size
DropboxInstaller	11/16/2023 4:29 PM	Application	675 KB



Dropbox Installer

Installing Dropbox…

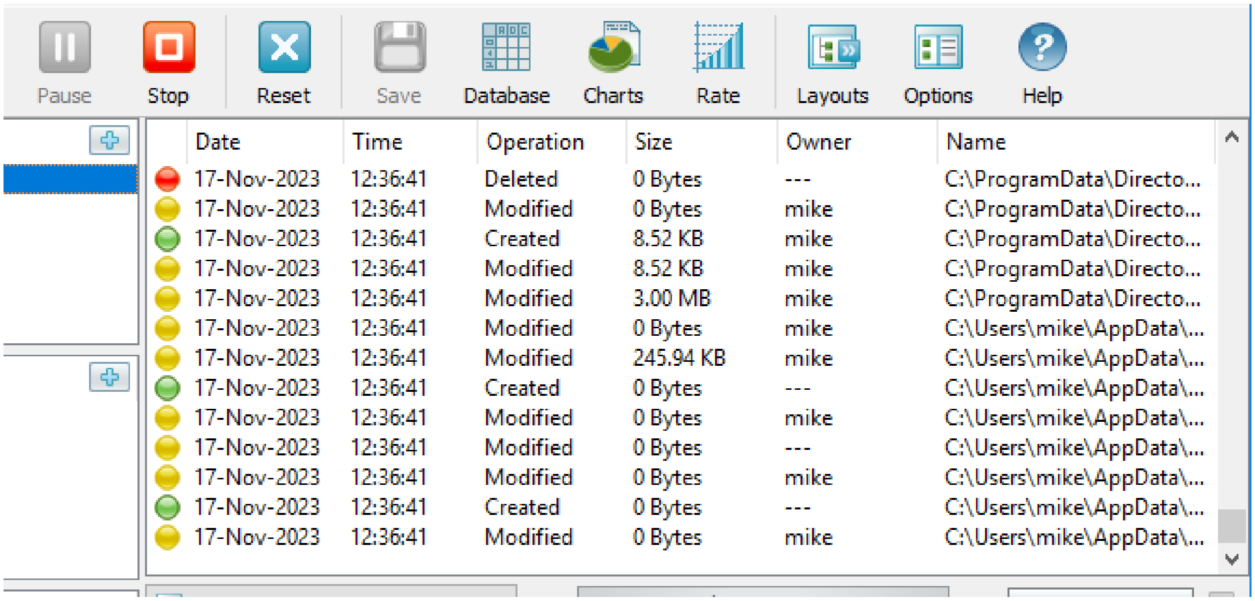
- **Sign into Dropbox.**



Welcome to Dropbox

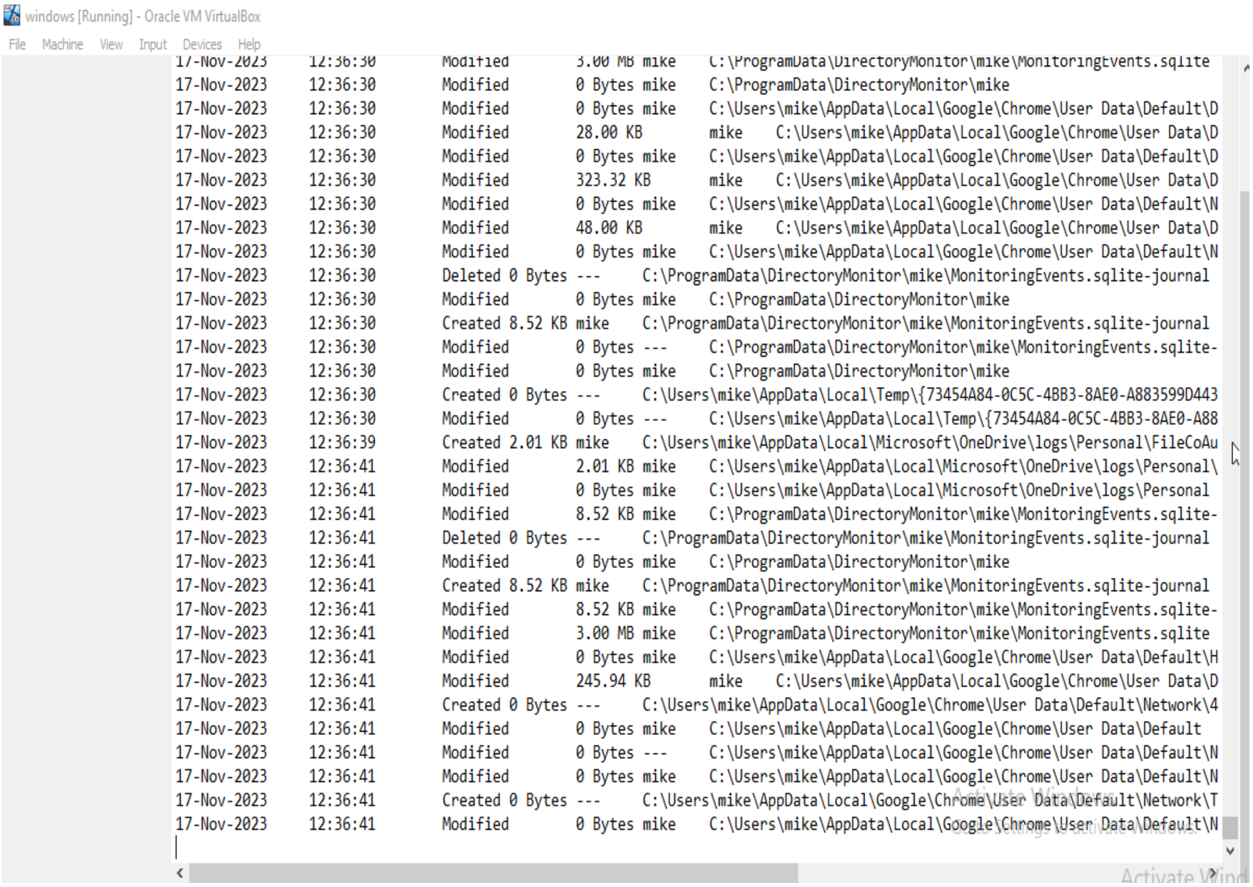
Sign in to start sharing your most important files.

- **Once signed in Dropbox, pause the Disk Pulse.**



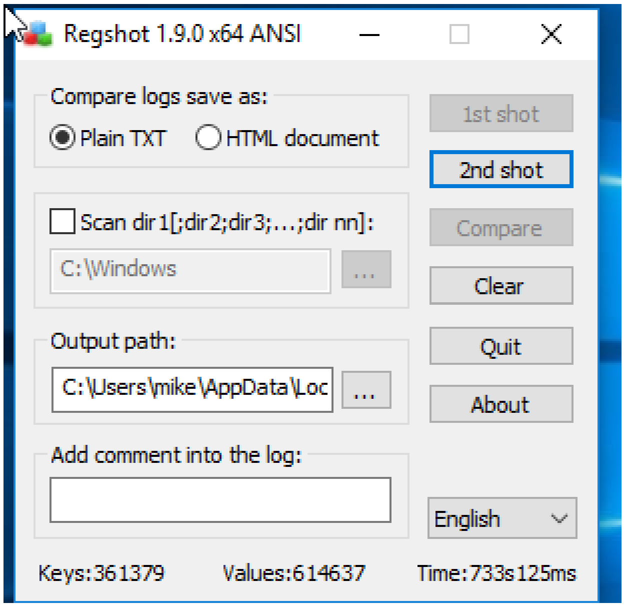
	Date	Time	Operation	Size	Owner	Name
🔴	17-Nov-2023	12:36:41	Deleted	0 Bytes	---	C:\ProgramData\Directo...
🟡	17-Nov-2023	12:36:41	Modified	0 Bytes	mike	C:\ProgramData\Directo...
🟢	17-Nov-2023	12:36:41	Created	8.52 KB	mike	C:\ProgramData\Directo...
🟡	17-Nov-2023	12:36:41	Modified	8.52 KB	mike	C:\ProgramData\Directo...
🟡	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.**



```
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\D
17-Nov-2023     12:36:30        Modified        28.00 KB        mike    C:\Users\mike\AppData\Local\Google\Chrome\User Data\D
17-Nov-2023     12:36:30        Modified        0 Bytes mike    C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\D
17-Nov-2023     12:36:30        Modified        323.32 KB       mike    C:\Users\mike\AppData\Local\Google\Chrome\User Data\D
17-Nov-2023     12:36:30        Modified        0 Bytes mike    C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\N
17-Nov-2023     12:36:30        Modified        48.00 KB        mike    C:\Users\mike\AppData\Local\Google\Chrome\User Data\D
17-Nov-2023     12:36:30        Modified        0 Bytes mike    C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\N
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-
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-
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-
17-Nov-2023     12:36:41        Modified        3.00 MB mike    C:\ProgramData\DirectoryMonitor\mike\MonitoringEvents.sqlite
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\D
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
17-Nov-2023     12:36:41        Modified        0 Bytes ---     C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\N
17-Nov-2023     12:36:41        Modified        0 Bytes mike    C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\N
17-Nov-2023     12:36:41        Created 0 Bytes ---     C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\Network\T
17-Nov-2023     12:36:41        Modified        0 Bytes mike    C:\Users\mike\AppData\Local\Google\Chrome\User Data\Default\N
```

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



Compare logs save as:
● Plain TXT ○ HTML document

☐ Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows

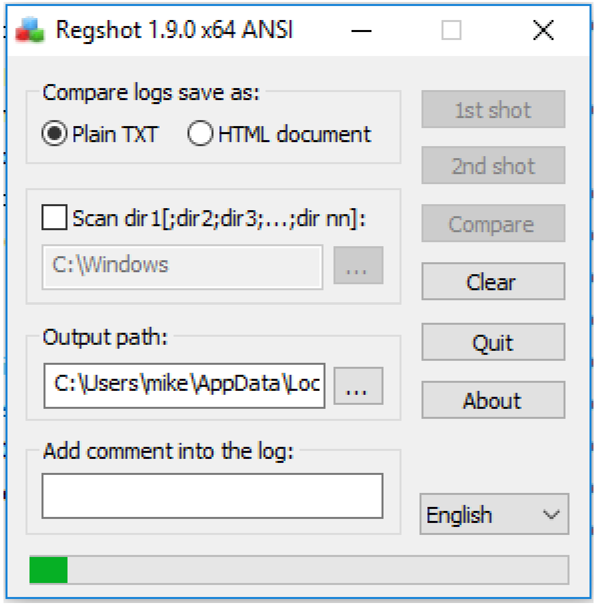
Output path:
C:\Users\mike\AppData\Loc

Add comment into the log:

English

Keys:361379 Values:614637 Time:733s125ms

- **Click on compare.**



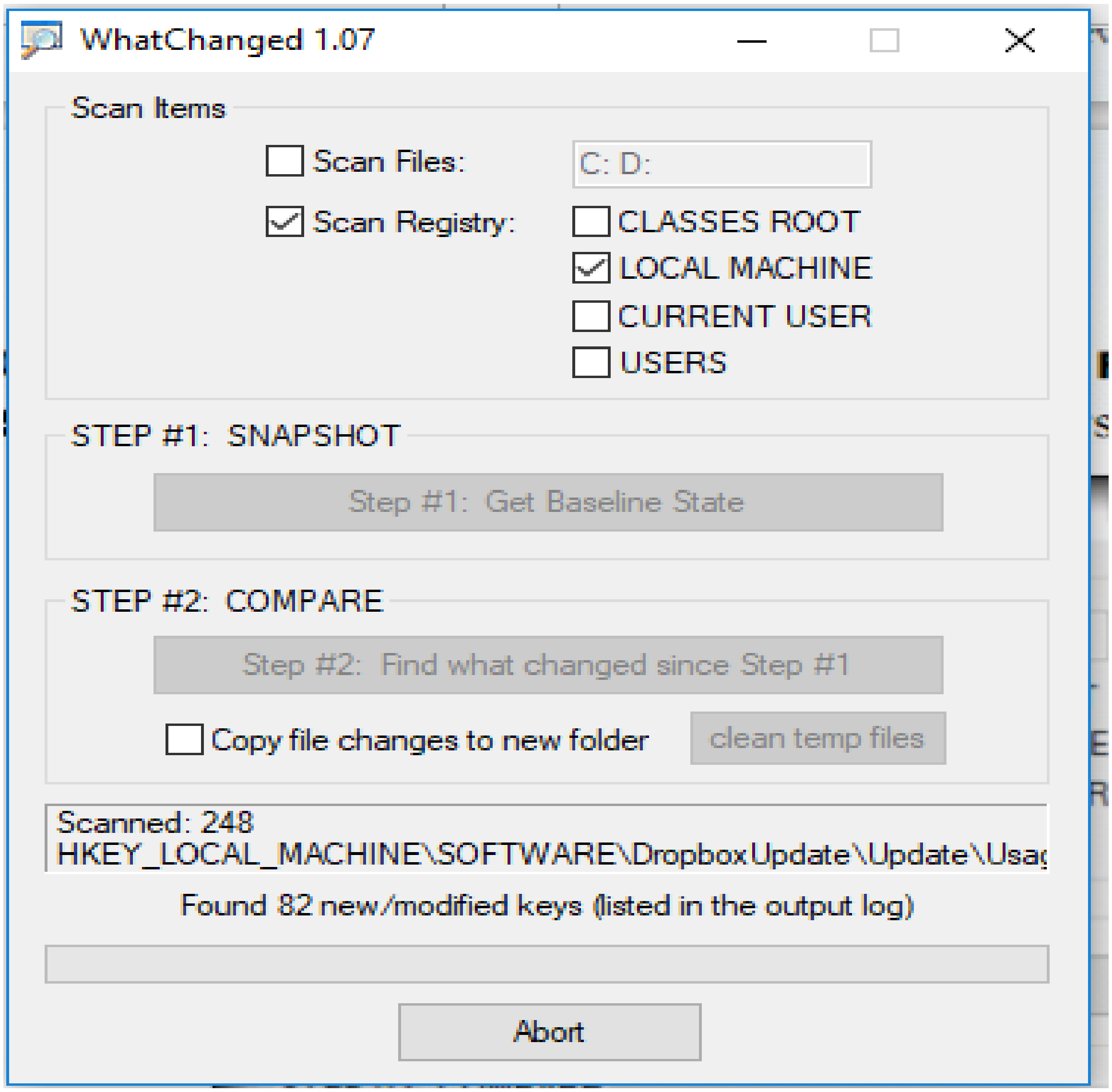
Compare logs save as:
● Plain TXT ○ HTML document

☐ Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows

Output path:
C:\Users\mike\AppData\Loc

Add comment into the log:

English



WhatChanged 1.07

Scan Items

□ Scan Files: C: D:

☑ Scan Registry:

□ CLASSES ROOT

☑ LOCAL MACHINE

□ CURRENT USER

□ USERS

STEP #1: SNAPSHOT

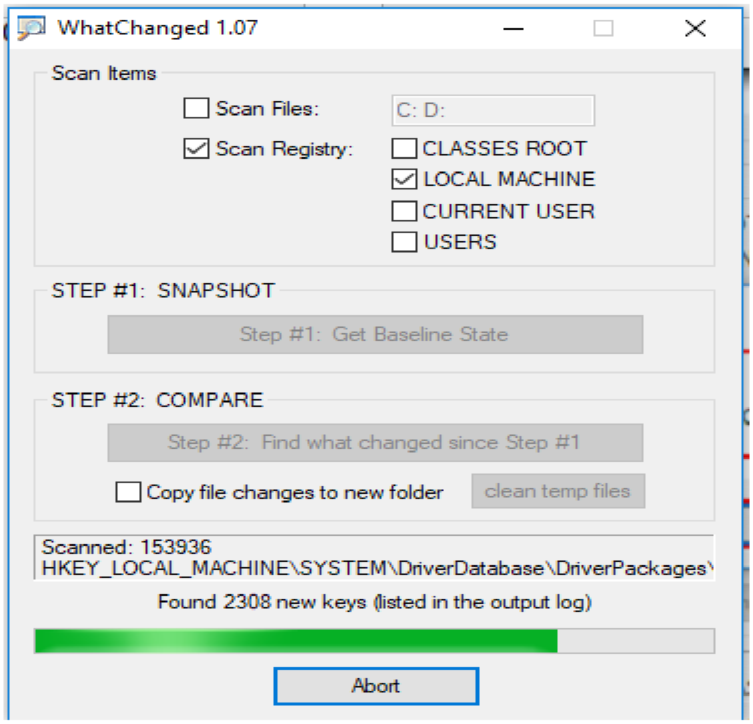
STEP #2: COMPARE

□ Copy file changes to new folder

```
Scanned: 248
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Usa
```

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

Step #1: Get Baseline State
Step #2: Find what changed since Step #1
clean temp files
Abort



☐ Scan Files: C: D:

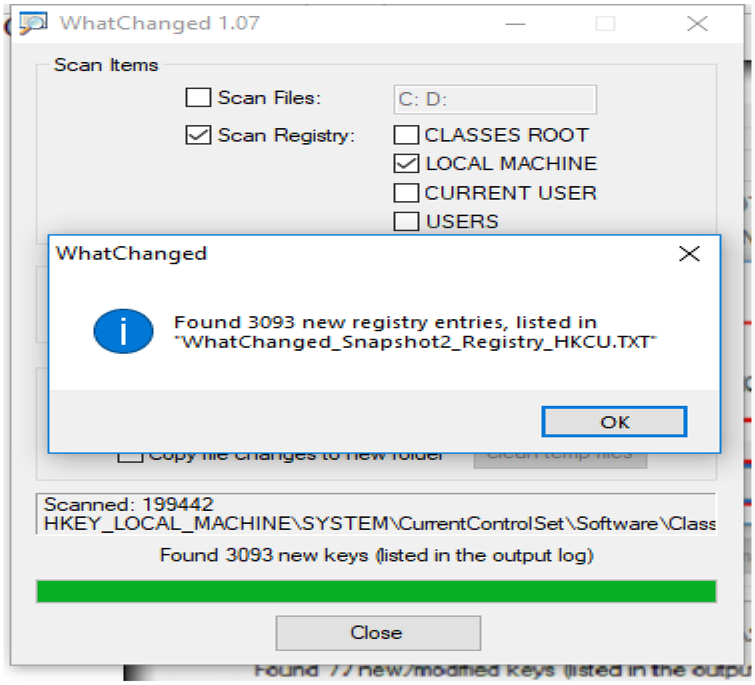
☑ Scan Registry: ☐ CLASSES ROOT ☑ LOCAL MACHINE ☐ CURRENT USER ☐ USERS

☐ Copy file changes to new folder

```
Scanned: 153936
HKEY_LOCAL_MACHINE\SYSTEM\DriverDatabase\DriverPackages\
```

Found 2308 new keys (listed in the output log)

- **Number of changes observed.**



☐ Scan Files: C: D:

☑ Scan Registry: ☐ CLASSES ROOT ☑ LOCAL MACHINE ☐ CURRENT USER ☐ USERS

☐ Copy file changes to new folder

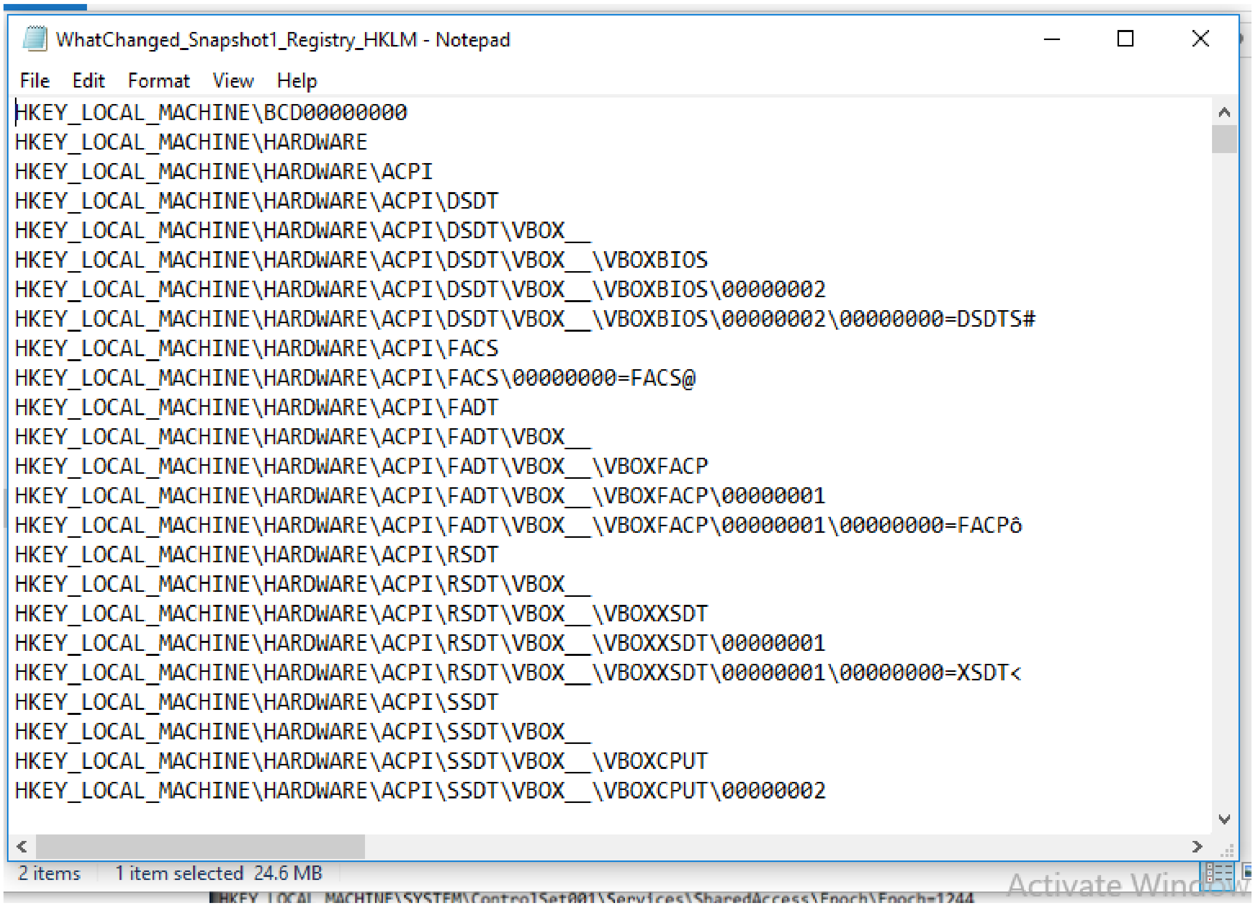
Found 3093 new registry entries, listed in "WhatChanged_Snapshot2_Registry_HKCU.TXT"

```
Scanned: 199442
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Software\Class
```

Found 3093 new keys (listed in the output log)

Found 77 new/modified keys (listed in the outpu

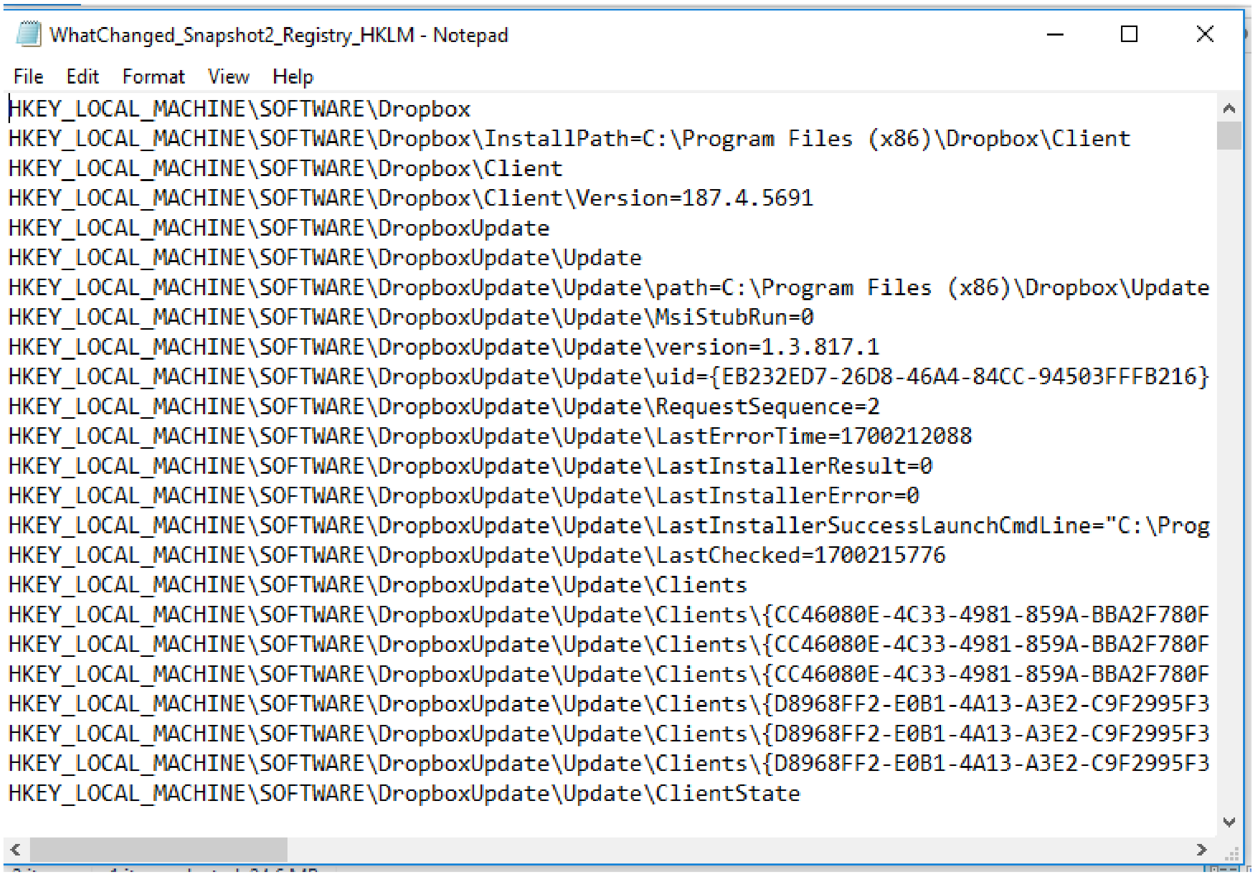
- **WhatChanged shot1**



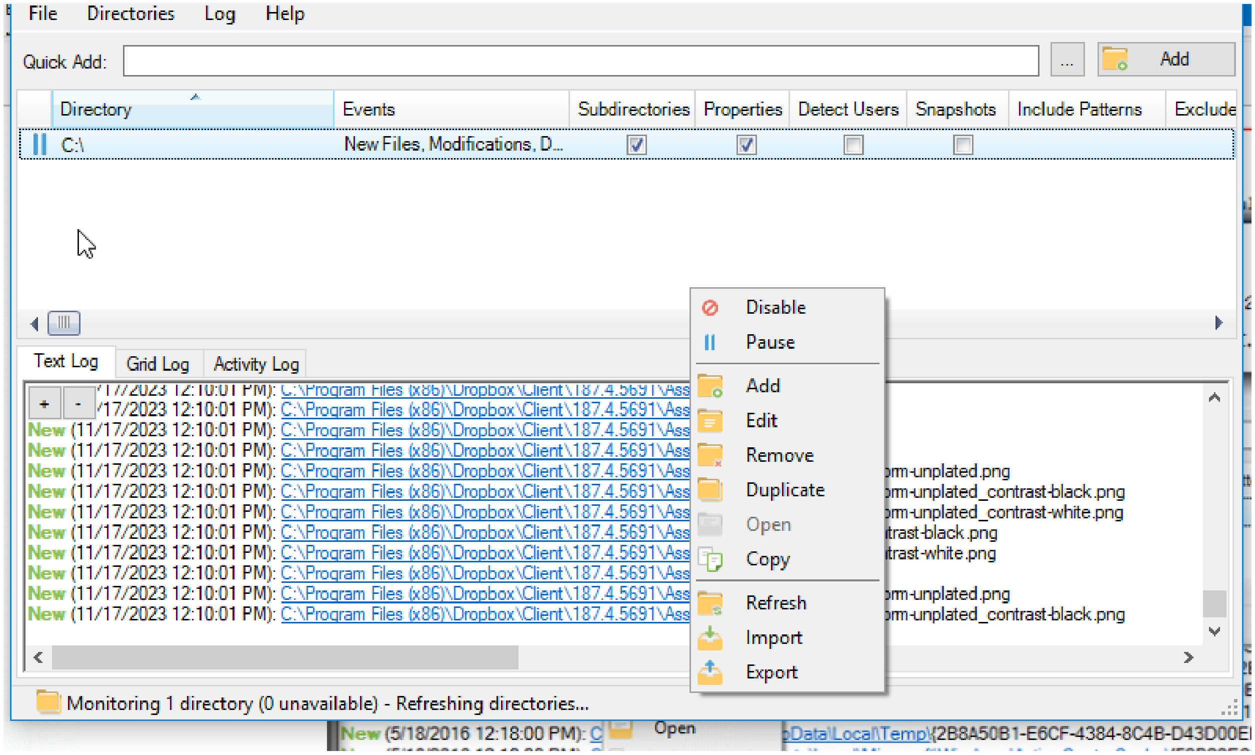
```
HKEY_LOCAL_MACHINE\BCD00000000
HKEY_LOCAL_MACHINE\HARDWARE
HKEY_LOCAL_MACHINE\HARDWARE\ACPI
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__\VBOXBIOS
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__\VBOXBIOS\00000002
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__\VBOXBIOS\00000002\00000000=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=FACPô
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\RSDT
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\RSDT\VBOX__
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\RSDT\VBOX__\VBOXXSDT
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\RSDT\VBOX__\VBOXXSDT\00000001
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\RSDT\VBOX__\VBOXXSDT\00000001\00000000=XSDT<
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
```

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Epoch\Epoch=1244
```

- **WhatChanged shot 2**



```
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
```

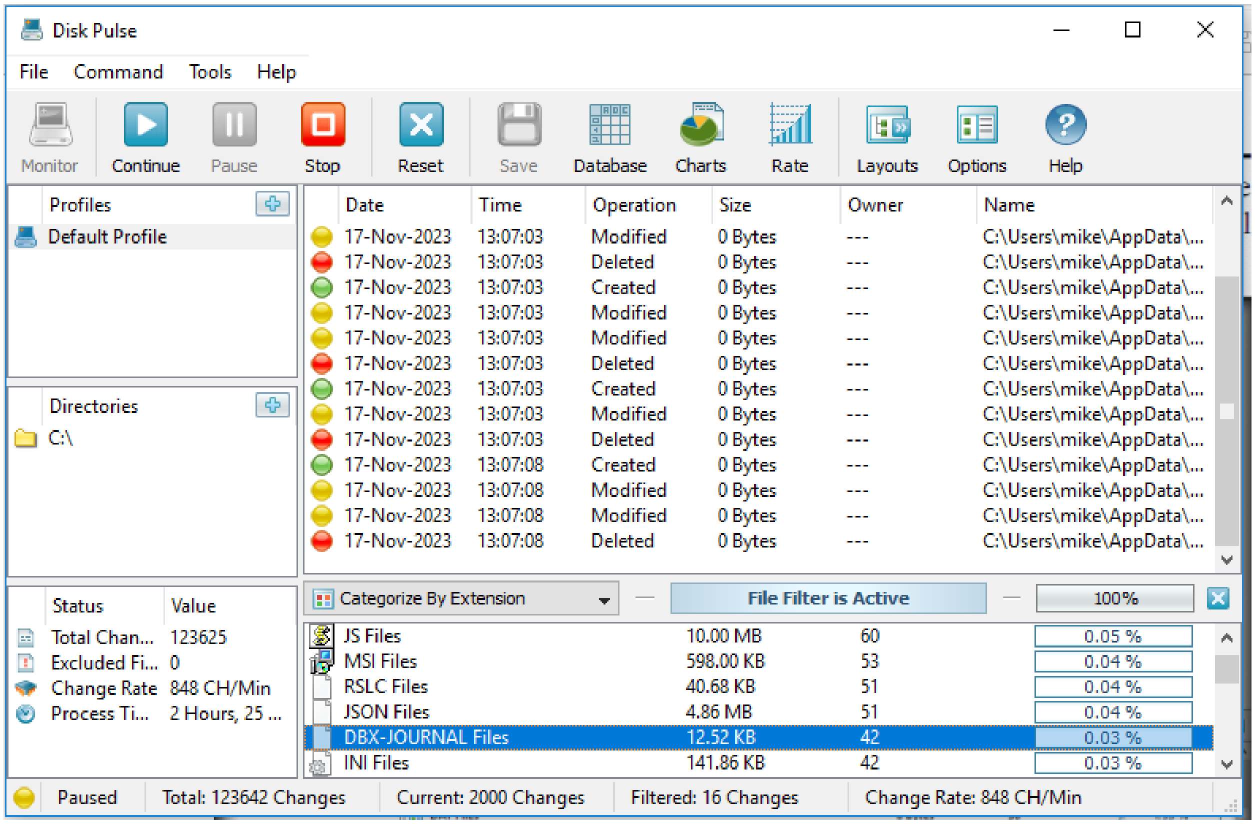


Directory	Events	Subdirectories	Properties	Detect Users	Snapshots	Include Patterns	Exclude
C:\	New Files, Modifications, D...	☑	☑	□	□		

```
'17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass
'17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass
New (11/17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass
New (11/17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass
New (11/17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass        orm-unplated.png
New (11/17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass        orm-unplated_contrast-black.png
New (11/17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass        orm-unplated_contrast-white.png
New (11/17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass        trast-black.png
New (11/17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass        trast-white.png
New (11/17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass
New (11/17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass        orm-unplated.png
New (11/17/2023 12:10:01 PM): C:\Program Files (x86)\Dropbox\Client\187.4.5691\Ass        orm-unplated_contrast-black.png
```

Monitoring 1 directory (0 unavailable) - Refreshing directories...

```
New (5/18/2016 12:18:00 PM): C     Open     pData\Local\Temp\{2B8A50B1-E6CF-4384-8C4B-D43D00E
```



	Date	Time	Operation	Size	Owner	Name
🟡	17-Nov-2023	13:07:03	Modified	0 Bytes	---	C:\Users\mike\AppData\...
🔴	17-Nov-2023	13:07:03	Deleted	0 Bytes	---	C:\Users\mike\AppData\...
🟢	17-Nov-2023	13:07:03	Created	0 Bytes	---	C:\Users\mike\AppData\...
🟡	17-Nov-2023	13:07:03	Modified	0 Bytes	---	C:\Users\mike\AppData\...
🟡	17-Nov-2023	13:07:03	Modified	0 Bytes	---	C:\Users\mike\AppData\...
🔴	17-Nov-2023	13:07:03	Deleted	0 Bytes	---	C:\Users\mike\AppData\...
🟢	17-Nov-2023	13:07:03	Created	0 Bytes	---	C:\Users\mike\AppData\...
🟡	17-Nov-2023	13:07:03	Modified	0 Bytes	---	C:\Users\mike\AppData\...
🔴	17-Nov-2023	13:07:03	Deleted	0 Bytes	---	C:\Users\mike\AppData\...
🟢	17-Nov-2023	13:07:08	Created	0 Bytes	---	C:\Users\mike\AppData\...
🟡	17-Nov-2023	13:07:08	Modified	0 Bytes	---	C:\Users\mike\AppData\...
🟡	17-Nov-2023	13:07:08	Modified	0 Bytes	---	C:\Users\mike\AppData\...
🔴	17-Nov-2023	13:07:08	Deleted	0 Bytes	---	C:\Users\mike\AppData\...

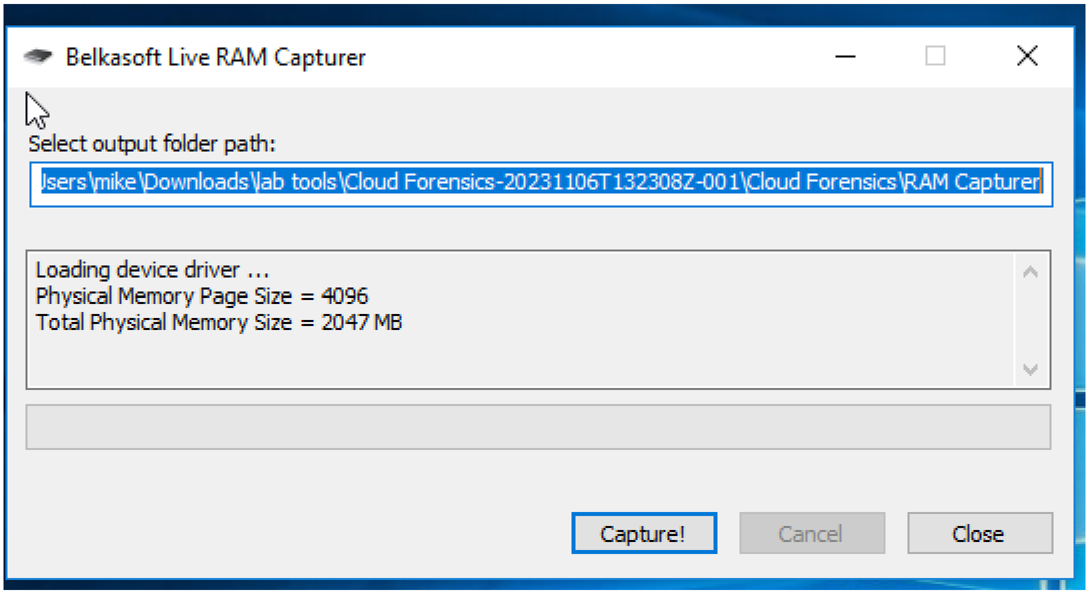
Status	Value
Total Chan...	123625
Excluded Fi...	0
Change Rate	848 CH/Min
Process Ti...	2 Hours, 25 ...

Categorize By Extension — File Filter is Active — 100%

JS Files	10.00 MB	60	0.05 %
MSI Files	598.00 KB	53	0.04 %
RSLC Files	40.68 KB	51	0.04 %
JSON Files	4.86 MB	51	0.04 %
DBX-JOURNAL Files	12.52 KB	42	0.03 %
INI Files	141.86 KB	42	0.03 %

Paused | Total: 123642 Changes | Current: 2000 Changes | Filtered: 16 Changes | Change Rate: 848 CH/Min

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

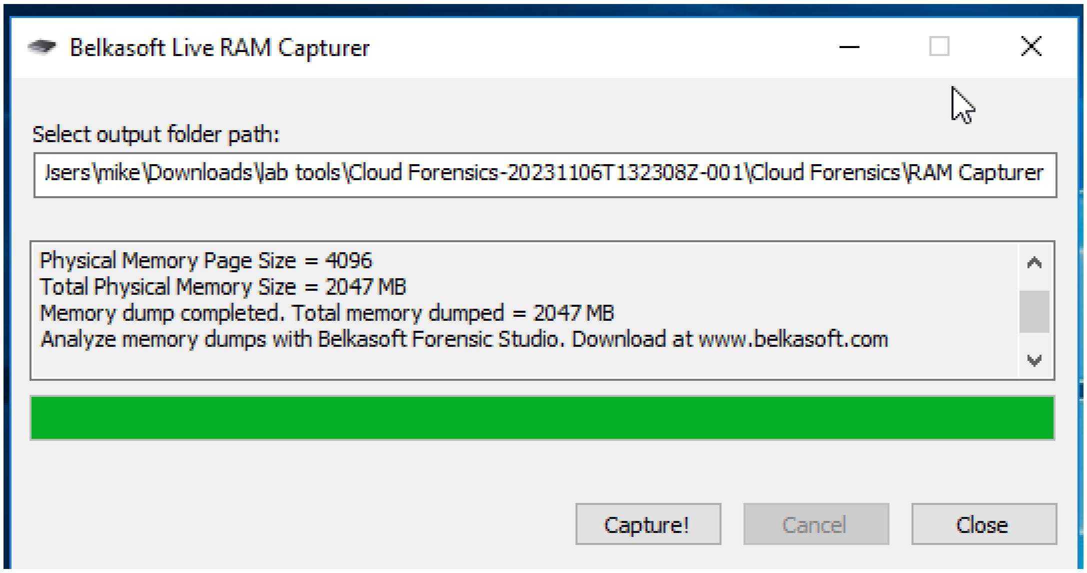


Select output folder path:

Jsers\mike\Downloads\lab tools\Cloud Forensics-20231106T132308Z-001\Cloud Forensics\RAM Capturer

```
Loading device driver ...
Physical Memory Page Size = 4096
Total Physical Memory Size = 2047 MB
```

- **Once the scan completes click on close.**



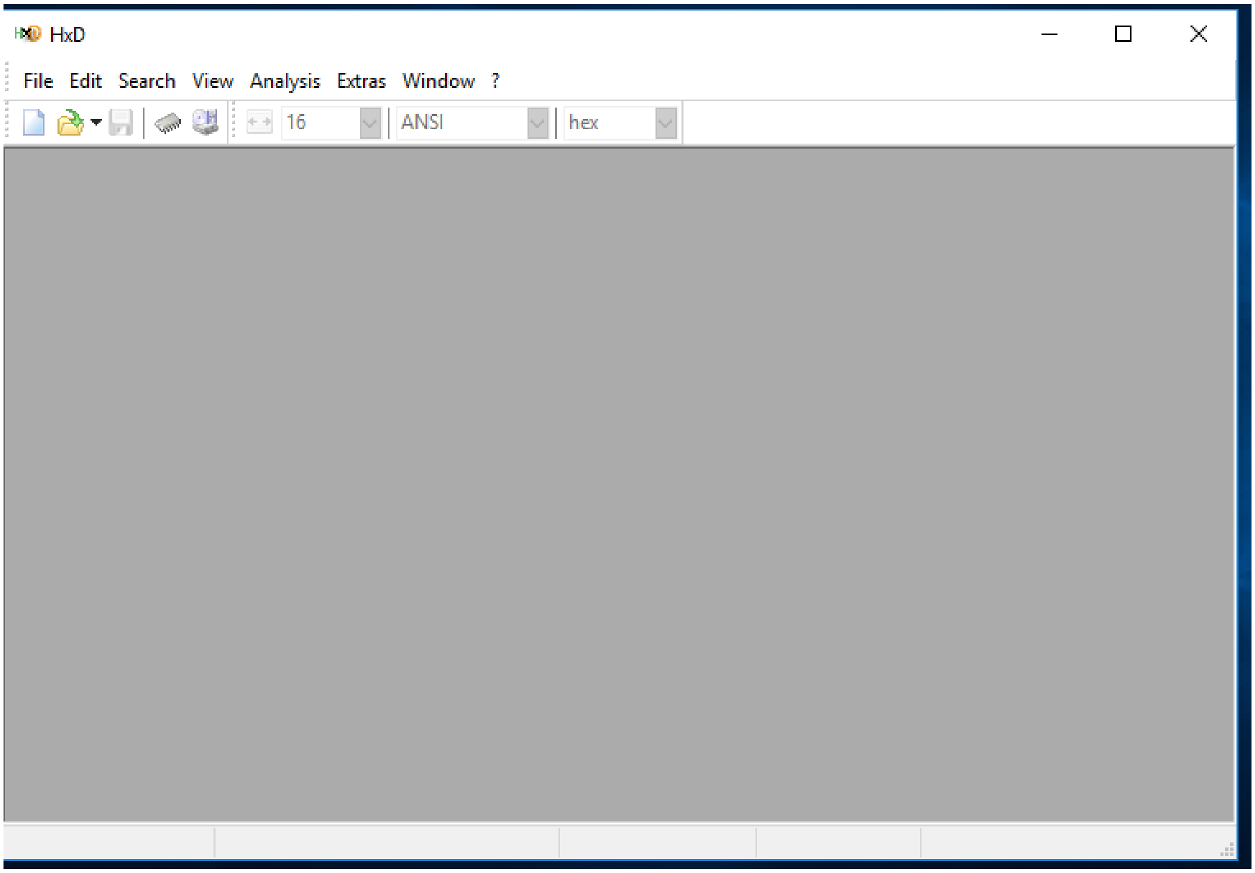
Belkasoft Live RAM Capturer

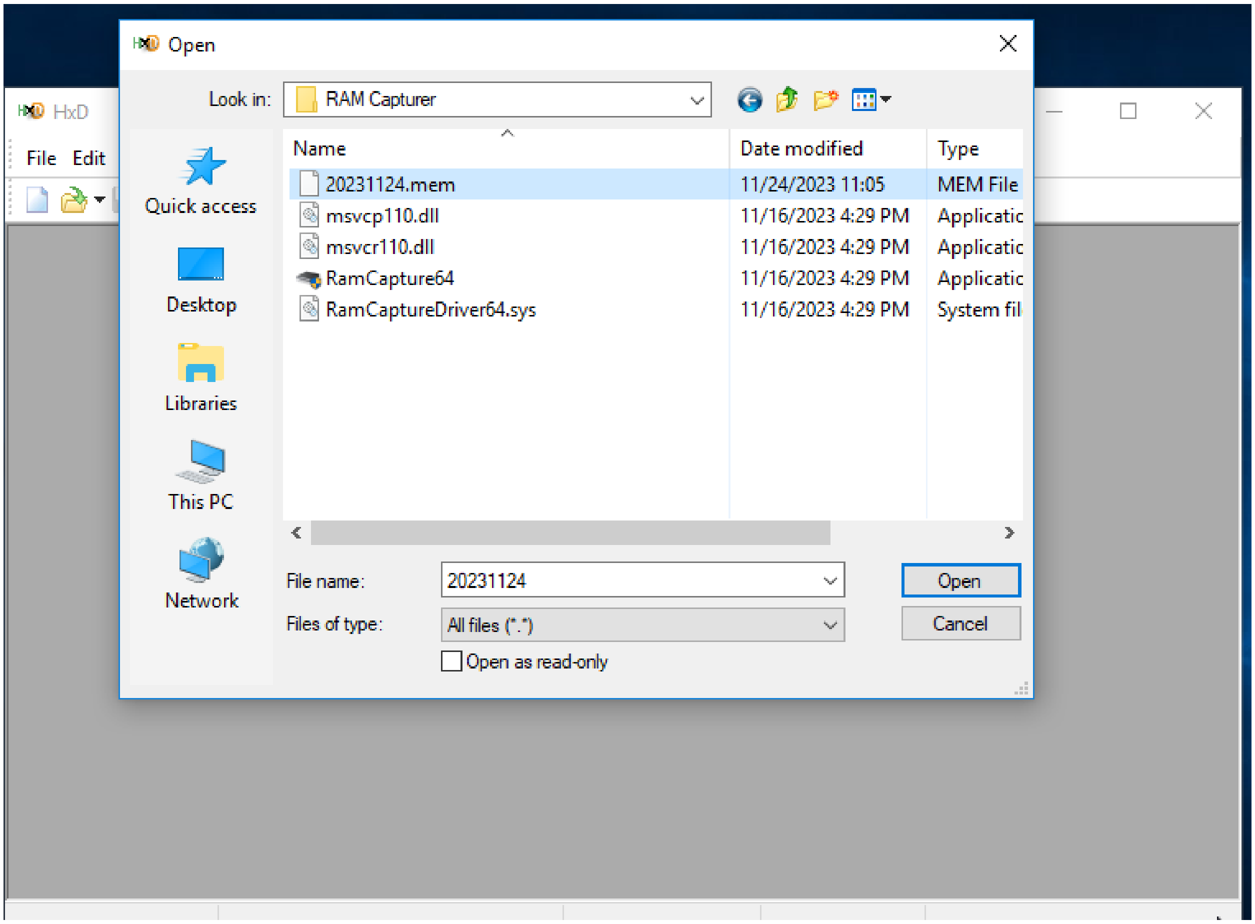
Select output folder path:

Jsers\mike\Downloads\lab tools\Cloud Forensics-20231106T132308Z-001\Cloud Forensics\RAM Capturer

```
Physical Memory Page Size = 4096
Total Physical Memory Size = 2047 MB
Memory dump completed. Total memory dumped = 2047 MB
Analyze memory dumps with Belkasoft Forensic Studio. Download at www.belkasoft.com
```

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





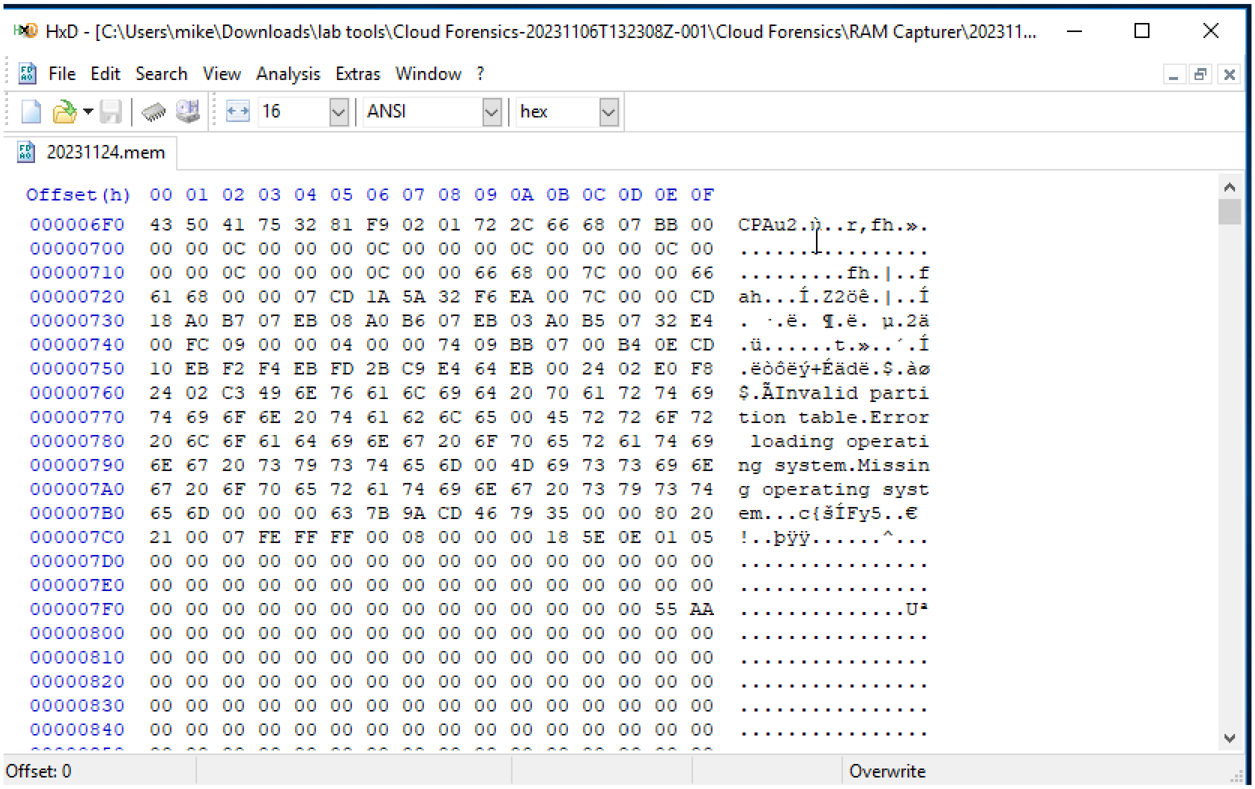
Look in: RAM Capturer

Name	Date modified	Type
20231124.mem	11/24/2023 11:05	MEM File
msvcp110.dll	11/16/2023 4:29 PM	Applicatic
msvcr110.dll	11/16/2023 4:29 PM	Applicatic
RamCapture64	11/16/2023 4:29 PM	Applicatic
RamCaptureDriver64.sys	11/16/2023 4:29 PM	System fil

File name: 20231124

Files of type: All files (*.*)

□ Open as read-only

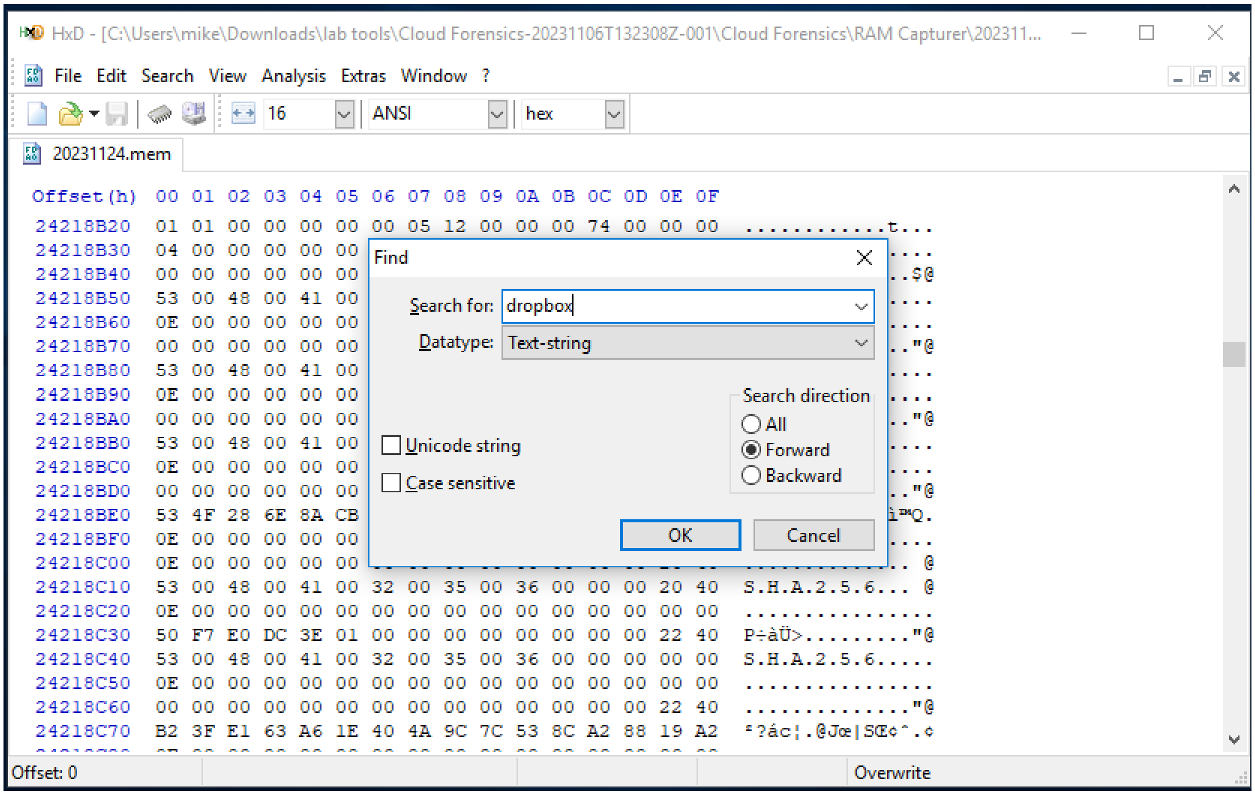


HxD - [C:\Users\mike\Downloads\lab tools\Cloud Forensics-20231106T132308Z-001\Cloud Forensics\RAM Capturer\202311...

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

000006F0  43 50 41 75 32 81 F9 02 01 72 2C 66 68 07 BB 00   CPAu2.ù..r,fh.».
00000700  00 00 0C 00 00 00 0C 00 00 00 0C 00 00 00 0C 00   ................
00000710  00 00 0C 00 00 00 0C 00 00 66 68 00 7C 00 00 66   .........fh.|..f
00000720  61 68 00 00 07 CD 1A 5A 32 F6 EA 00 7C 00 00 CD   ah...Í.Z2öê.|..Í
00000730  18 A0 B7 07 EB 08 A0 B6 07 EB 03 A0 B5 07 32 E4   . ·.ë. ¶.ë. µ.2ä
00000740  00 FC 09 00 00 04 00 00 74 09 BB 07 00 B4 0E CD   .ü......t.»..´.Í
00000750  10 EB F2 F4 EB FD 2B C9 E4 64 EB 00 24 02 E0 F8   .ëòôëý+Éädë.$.àø
00000760  24 02 C3 49 6E 76 61 6C 69 64 20 70 61 72 74 69   $.ÃInvalid parti
00000770  74 69 6F 6E 20 74 61 62 6C 65 00 45 72 72 6F 72   tion table.Error
00000780  20 6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74 69    loading operati
00000790  6E 67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E   ng system.Missin
000007A0  67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74   g operating syst
000007B0  65 6D 00 00 00 63 7B 9A CD 46 79 35 00 00 80 20   em...c{šÍFy5..€
000007C0  21 00 07 FE FF FF 00 08 00 00 00 18 5E 0E 01 05   !..þÿÿ......^...
000007D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000007E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000007F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA   ..............Uª
00000800  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000810  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000820  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000830  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000840  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Offset: 0

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


HxD - [C:\Users\mike\Downloads\lab tools\Cloud Forensics-20231106T132308Z-001\Cloud Forensics\RAM Capturer\202311...

20231124.mem

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
24218B20  01 01 00 00 00 00 00 05 12 00 00 00 74 00 00 00  .............t...
24218B30  04 00 00 00 00 00                                 ....
24218B40  00 00 00 00 00 00                                 ..$@
24218B50  53 00 48 00 41 00                                 ....
24218B60  0E 00 00 00 00 00                                 ....
24218B70  00 00 00 00 00 00                                 .."@
24218B80  53 00 48 00 41 00                                 ....
24218B90  0E 00 00 00 00 00                                 ....
24218BA0  00 00 00 00 00 00                                 .."@
24218BB0  53 00 48 00 41 00                                 ....
24218BC0  0E 00 00 00 00 00                                 ....
24218BD0  00 00 00 00 00 00                                 .."@
24218BE0  53 4F 28 6E 8A CB                                 ì™Q.
24218BF0  0E 00 00 00 00 00                                 ....
24218C00  0E 00 00 00 00 00                                 .. @
24218C10  53 00 48 00 41 00 32 00 35 00 36 00 00 00 20 40  S.H.A.2.5.6... @
24218C20  0E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
24218C30  50 F7 E0 DC 3E 01 00 00 00 00 00 00 00 00 22 40  P÷àÜ>........."@
24218C40  53 00 48 00 41 00 32 00 35 00 36 00 00 00 00 00  S.H.A.2.5.6.....
24218C50  0E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
24218C60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 40  .............."@
24218C70  B2 3F E1 63 A6 1E 40 4A 9C 7C 53 8C A2 88 19 A2  ²?ác¦.@Jœ|SŒ¢ˆ.¢
```

Find

Search for: dropbox

Datatype: Text-string

□ Unicode string

□ Case sensitive

Search direction

○ All

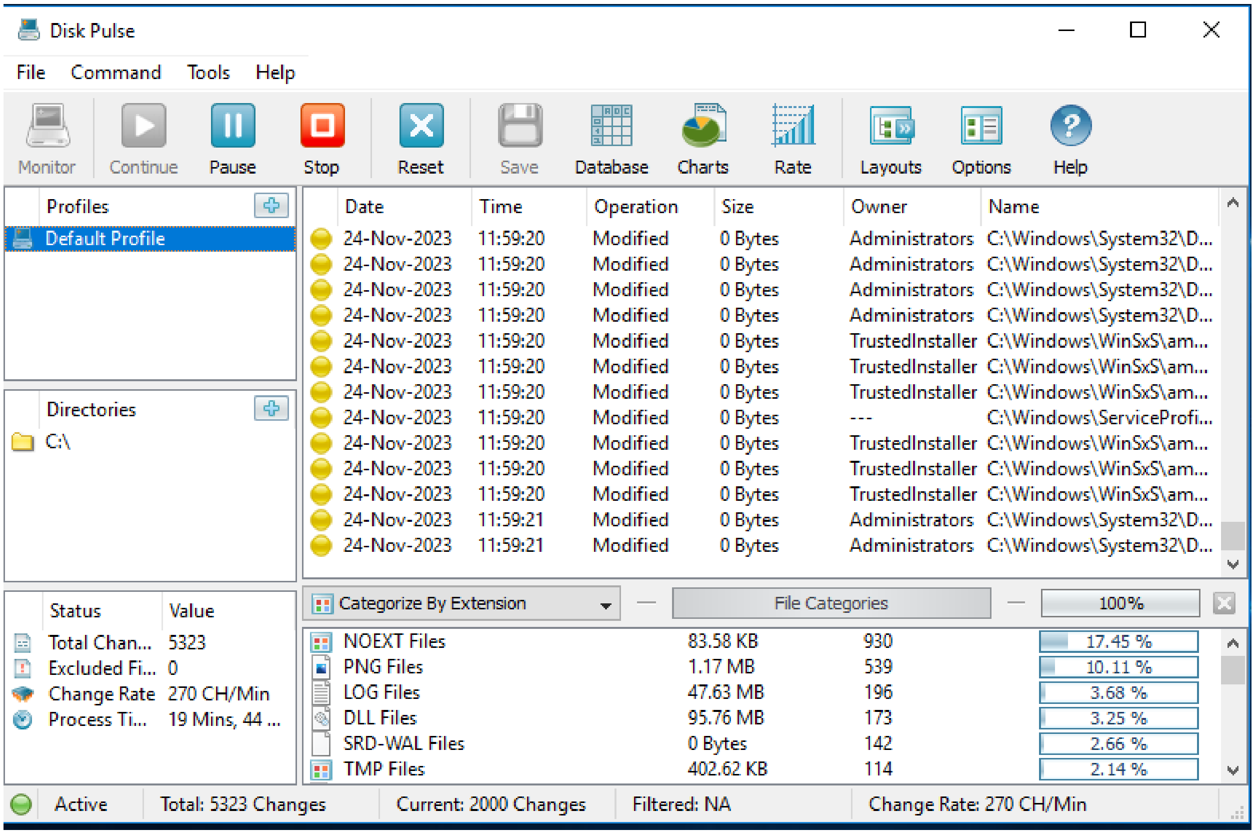
● Forward

○ Backward

Offset: 0

Overwrite

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

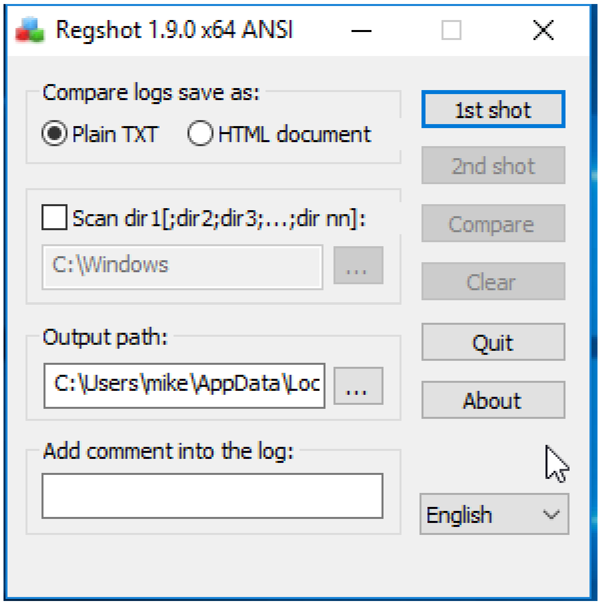


Date	Time	Operation	Size	Owner	Name
24-Nov-2023	11:59:20	Modified	0 Bytes	Administrators	C:\Windows\System32\D...
24-Nov-2023	11:59:20	Modified	0 Bytes	Administrators	C:\Windows\System32\D...
24-Nov-2023	11:59:20	Modified	0 Bytes	Administrators	C:\Windows\System32\D...
24-Nov-2023	11:59:20	Modified	0 Bytes	Administrators	C:\Windows\System32\D...
24-Nov-2023	11:59:20	Modified	0 Bytes	TrustedInstaller	C:\Windows\WinSxS\am...
24-Nov-2023	11:59:20	Modified	0 Bytes	TrustedInstaller	C:\Windows\WinSxS\am...
24-Nov-2023	11:59:20	Modified	0 Bytes	TrustedInstaller	C:\Windows\WinSxS\am...
24-Nov-2023	11:59:20	Modified	0 Bytes	---	C:\Windows\ServiceProfi...
24-Nov-2023	11:59:20	Modified	0 Bytes	TrustedInstaller	C:\Windows\WinSxS\am...
24-Nov-2023	11:59:20	Modified	0 Bytes	TrustedInstaller	C:\Windows\WinSxS\am...
24-Nov-2023	11:59:20	Modified	0 Bytes	TrustedInstaller	C:\Windows\WinSxS\am...
24-Nov-2023	11:59:21	Modified	0 Bytes	Administrators	C:\Windows\System32\D...
24-Nov-2023	11:59:21	Modified	0 Bytes	Administrators	C:\Windows\System32\D...

Status	Value
Total Chan...	5323
Excluded Fi...	0
Change Rate	270 CH/Min
Process Ti...	19 Mins, 44 ...

NOEXT Files	83.58 KB	930	17.45 %
PNG Files	1.17 MB	539	10.11 %
LOG Files	47.63 MB	196	3.68 %
DLL Files	95.76 MB	173	3.25 %
SRD-WAL Files	0 Bytes	142	2.66 %
TMP Files	402.62 KB	114	2.14 %

Active | Total: 5323 Changes | Current: 2000 Changes | Filtered: NA | Change Rate: 270 CH/Min



Compare logs save as:

● Plain TXT ○ HTML document

□ Scan dir 1[;dir2;dir3;...;dir nn]:

C:\Windows

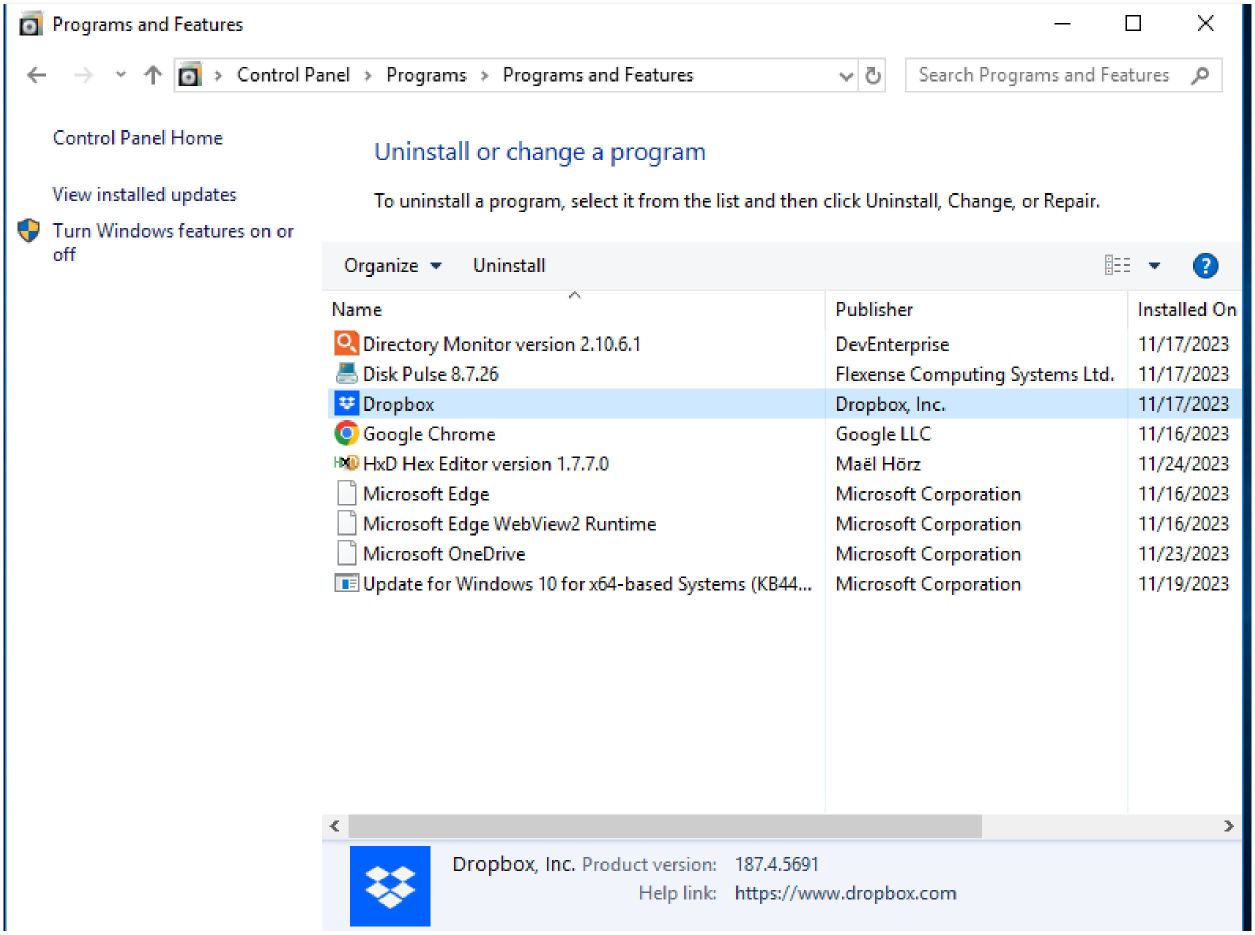
Output path:

C:\Users\mike\AppData\Loc

Add comment into the log:

English

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

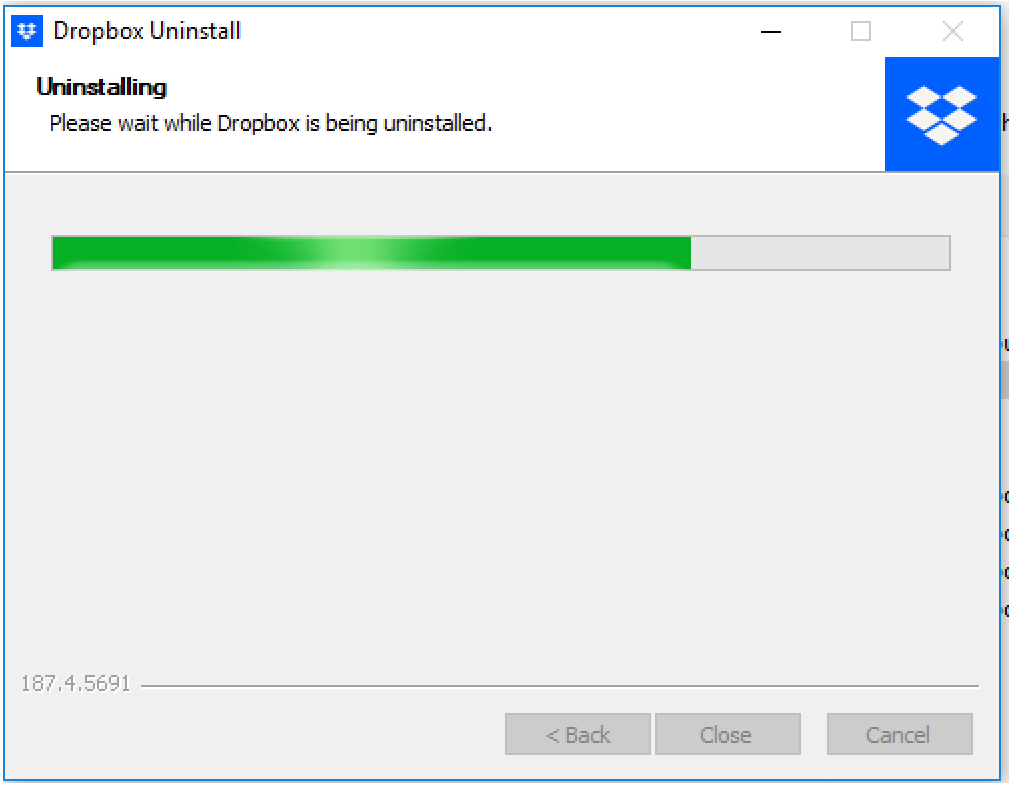

Programs and Features
Control Panel > Programs > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize
Uninstall

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On
Directory Monitor version 2.10.6.1	DevEnterprise	11/17/2023
Disk Pulse 8.7.26	Flexense Computing Systems Ltd.	11/17/2023
Dropbox	Dropbox, Inc.	11/17/2023
Google Chrome	Google LLC	11/16/2023
HxD Hex Editor version 1.7.7.0	Maël Hörz	11/24/2023
Microsoft Edge	Microsoft Corporation	11/16/2023
Microsoft Edge WebView2 Runtime	Microsoft Corporation	11/16/2023
Microsoft OneDrive	Microsoft Corporation	11/23/2023
Update for Windows 10 for x64-based Systems (KB44...	Microsoft Corporation	11/19/2023

Dropbox, Inc. Product version: 187.4.5691
Help link: https://www.dropbox.com



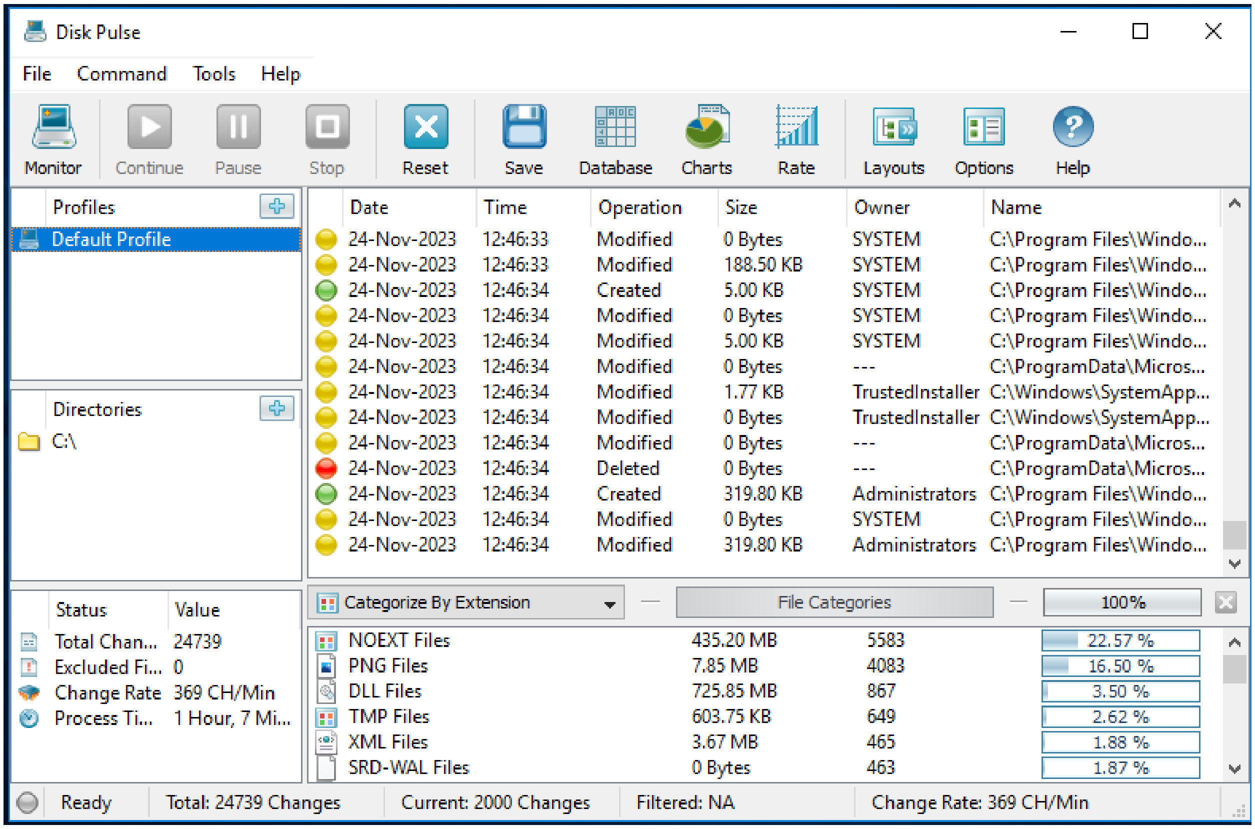
Dropbox Uninstall

Uninstalling

Please wait while Dropbox is being uninstalled.

187.4.5691

- **On the already running Disk pulse, click on stop**



Disk Pulse

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...

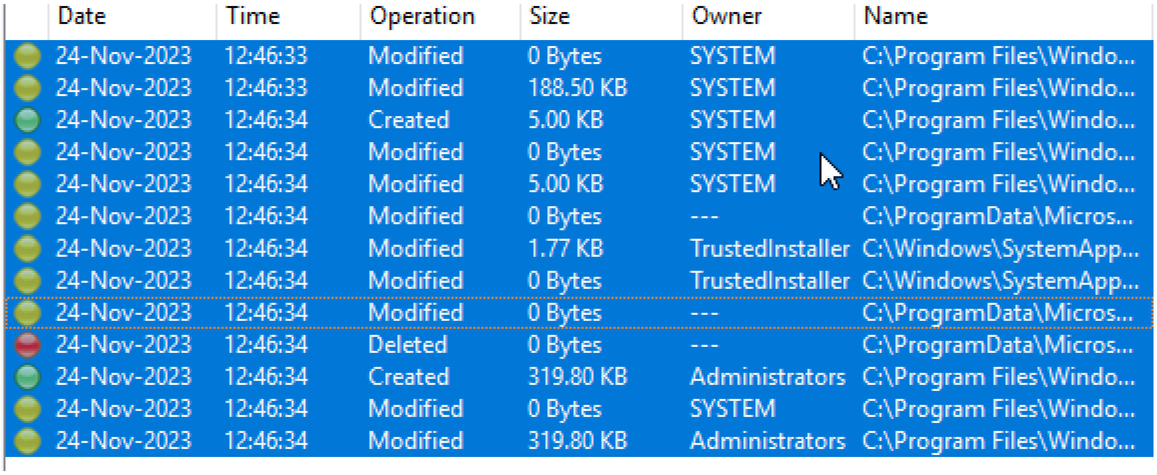
Status	Value
Total Chan...	24739
Excluded Fi...	0
Change Rate	369 CH/Min
Process Ti...	1 Hour, 7 Mi...

Categorize By Extension — File Categories — 100%

NOEXT Files	435.20 MB	5583	22.57 %
PNG Files	7.85 MB	4083	16.50 %
DLL Files	725.85 MB	867	3.50 %
TMP Files	603.75 KB	649	2.62 %
XML Files	3.67 MB	465	1.88 %
SRD-WAL Files	0 Bytes	463	1.87 %

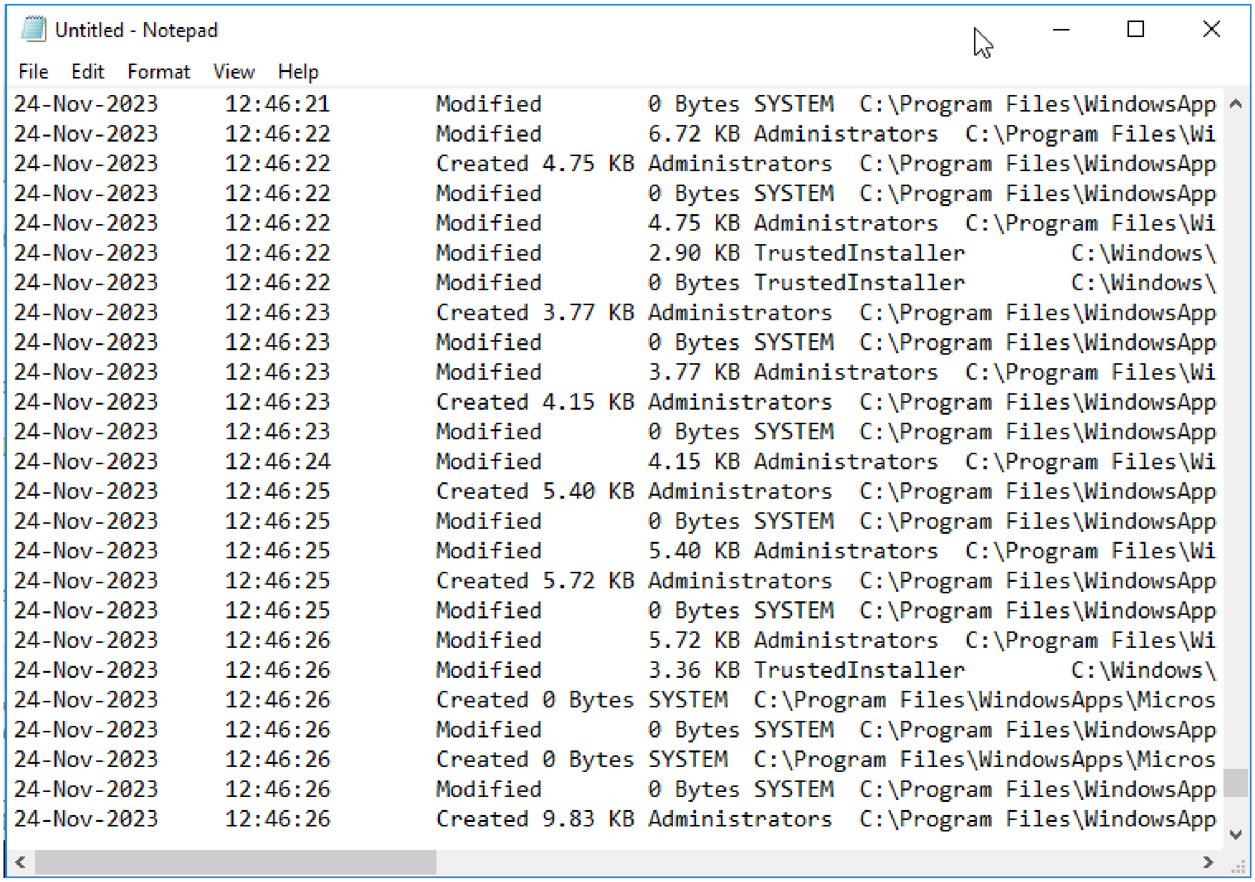
Ready | Total: 24739 Changes | Current: 2000 Changes | Filtered: NA | Change Rate: 369 CH/Min

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



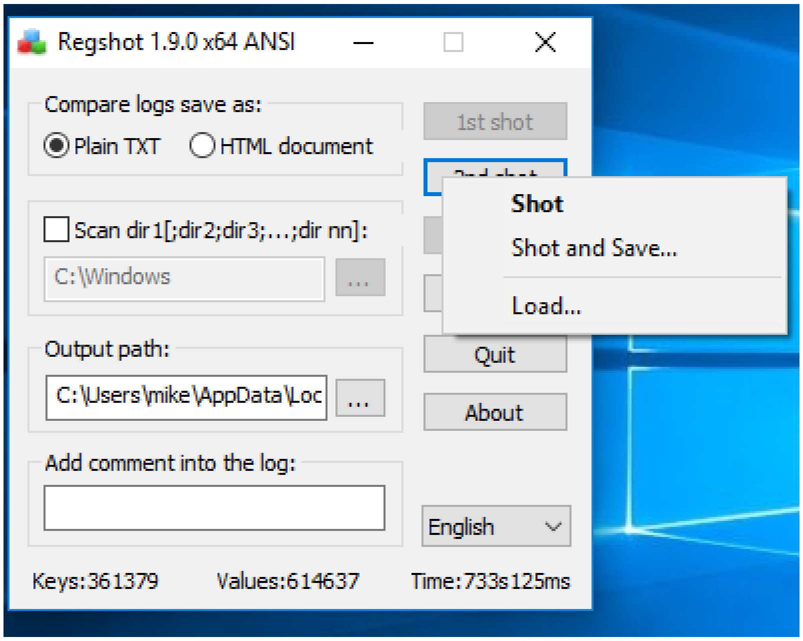
	Date	Time	Operation	Size	Owner	Name
🟡	24-Nov-2023	12:46:33	Modified	0 Bytes	SYSTEM	C:\Program Files\Windo...
🟡	24-Nov-2023	12:46:33	Modified	188.50 KB	SYSTEM	C:\Program Files\Windo...
🟢	24-Nov-2023	12:46:34	Created	5.00 KB	SYSTEM	C:\Program Files\Windo...
🟡	24-Nov-2023	12:46:34	Modified	0 Bytes	SYSTEM	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.**



```
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.**


Regshot 1.9.0 x64 ANSI

Compare logs save as:
● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows

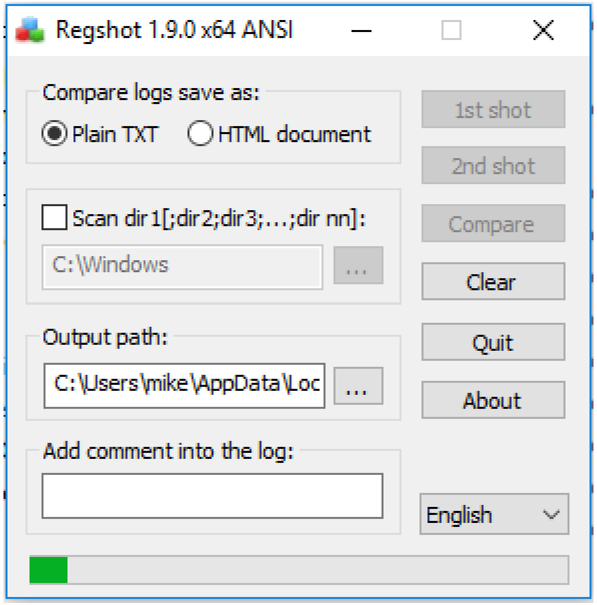
Output path:
C:\Users\mike\AppData\Loc

Add comment into the log:

English

Keys:361379 Values:614637 Time:733s125ms

- **Click on the compare.**


Regshot 1.9.0 x64 ANSI

Compare logs save as:
● Plain TXT ○ HTML document

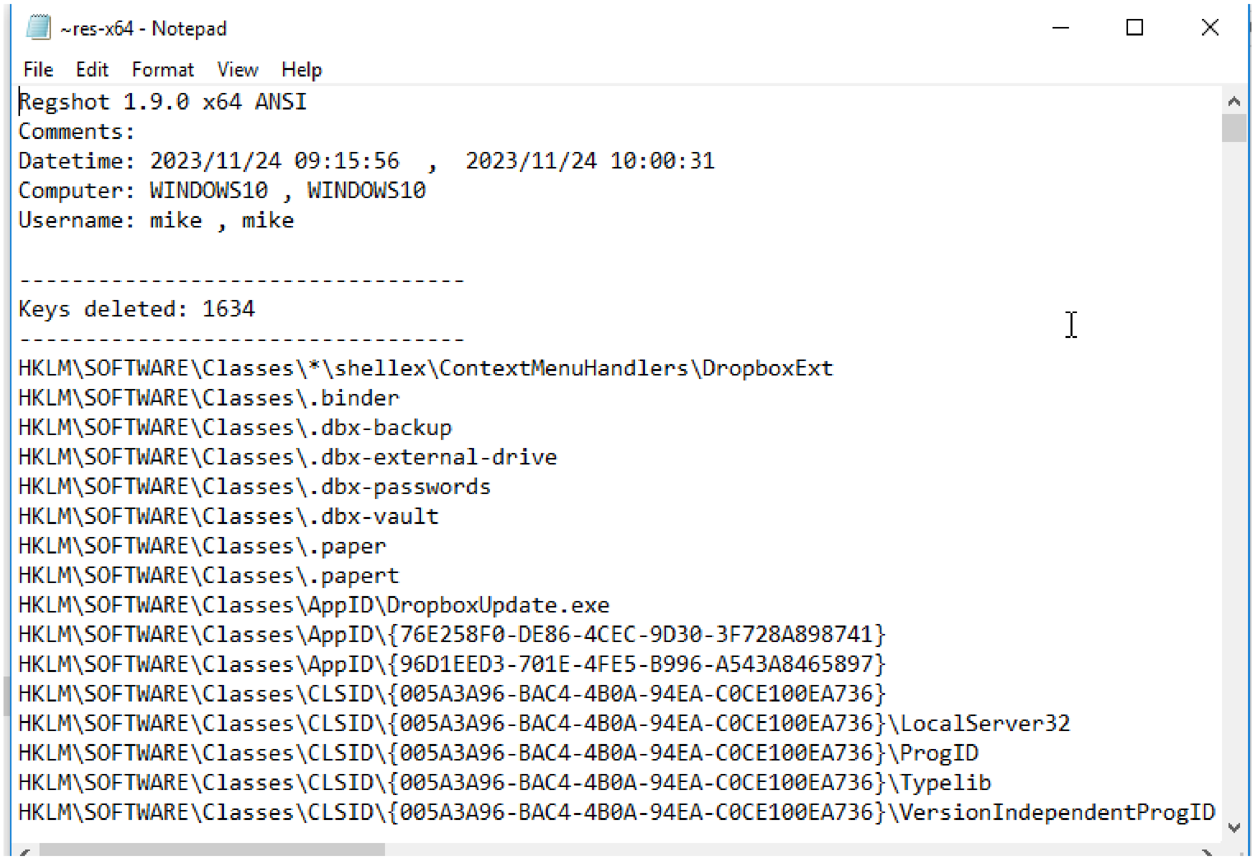
□ Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows

Output path:
C:\Users\mike\AppData\Loc

Add comment into the log:

English

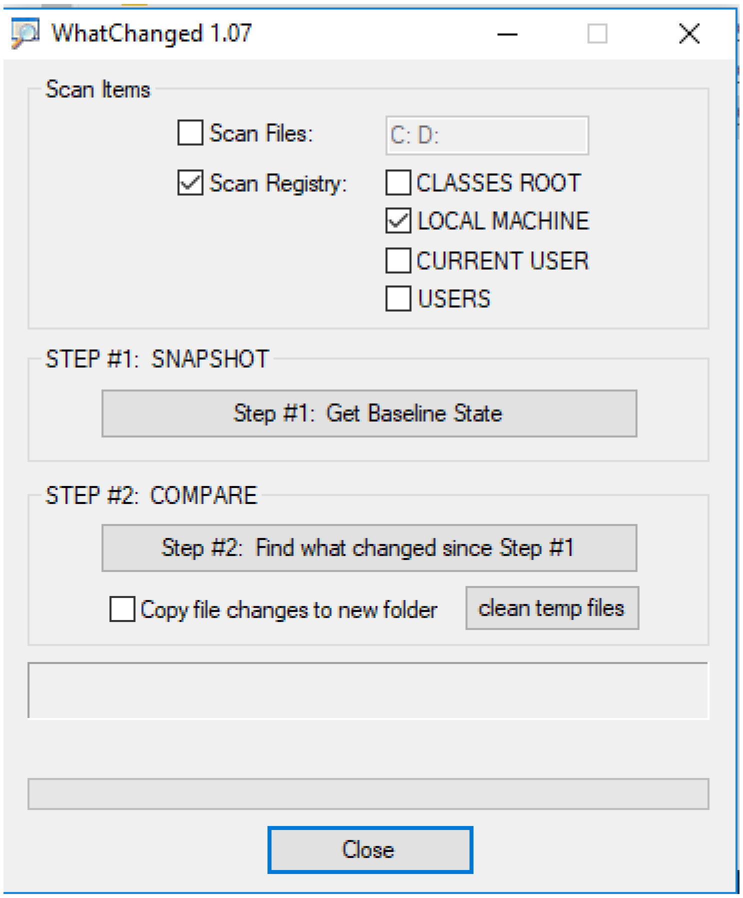
- **The tool prompts a notepad file after comparing first and second shot.**



```
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.***



WhatChanged 1.07

Scan Items

☐ Scan Files: C: D:

☑ Scan Registry: ☐ CLASSES ROOT

☑ LOCAL MACHINE

☐ CURRENT USER

☐ USERS

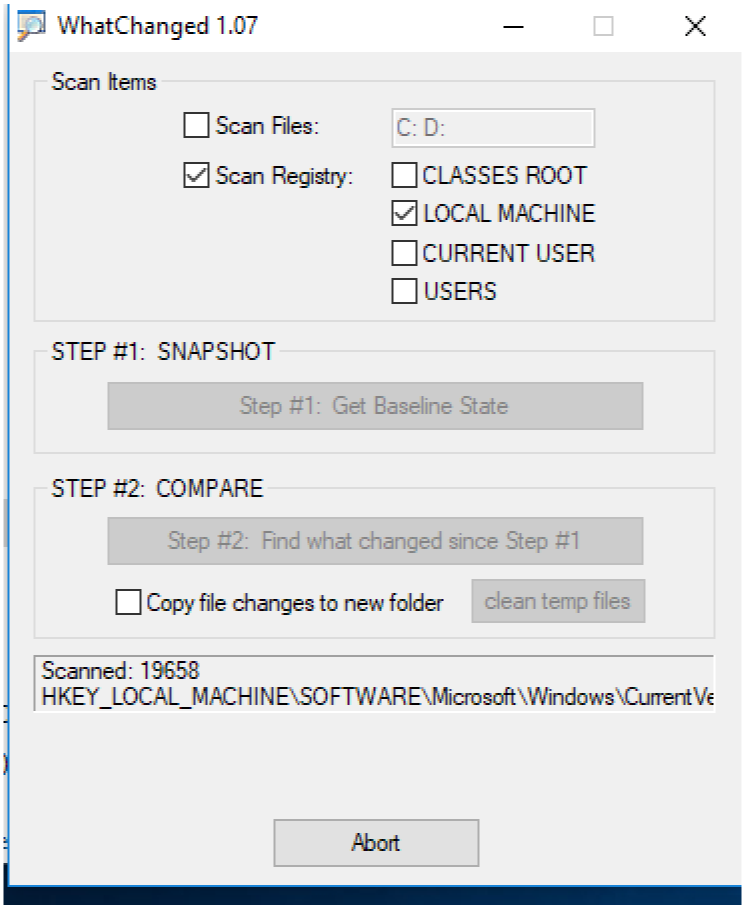
STEP #1: SNAPSHOT

STEP #2: COMPARE

☐ Copy file changes to new folder

Step #1: Get Baseline State
Step #2: Find what changed since Step #1
clean temp files
Close

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



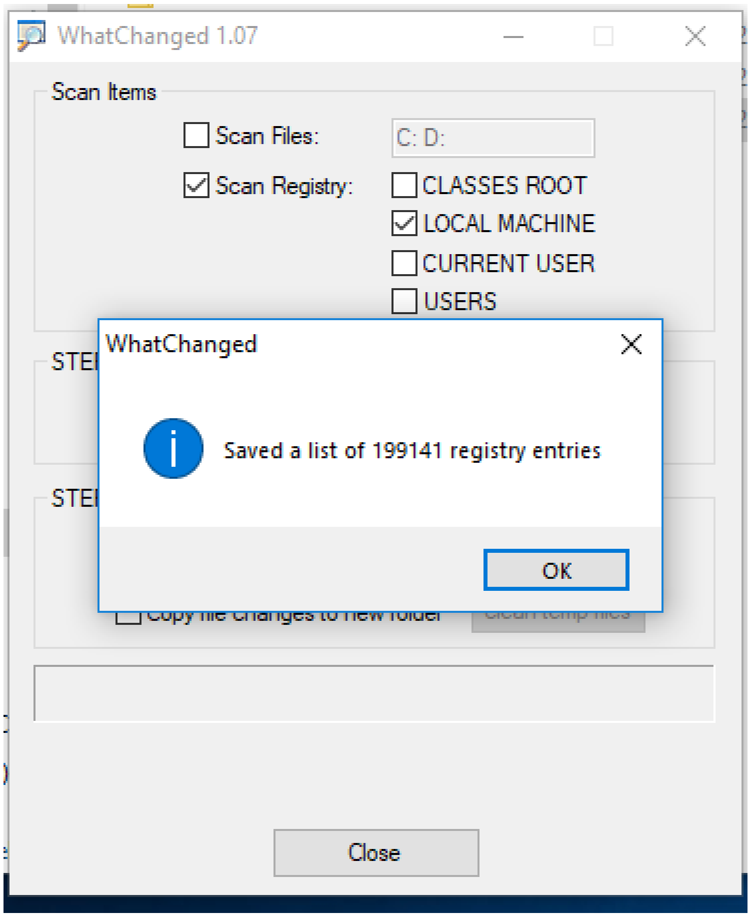
□ Scan Files: C: D:

☑ Scan Registry: □ CLASSES ROOT ☑ LOCAL MACHINE □ CURRENT USER □ USERS

□ Copy file changes to new folder

```
Scanned: 19658
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVe
```

- **Dialog box displaying total number of entries recorded.**



WhatChanged 1.07

Scan Items

☐ Scan Files: C: D:

☑ Scan Registry:
☐ CLASSES ROOT
☑ LOCAL MACHINE
☐ CURRENT USER
☐ USERS

STE

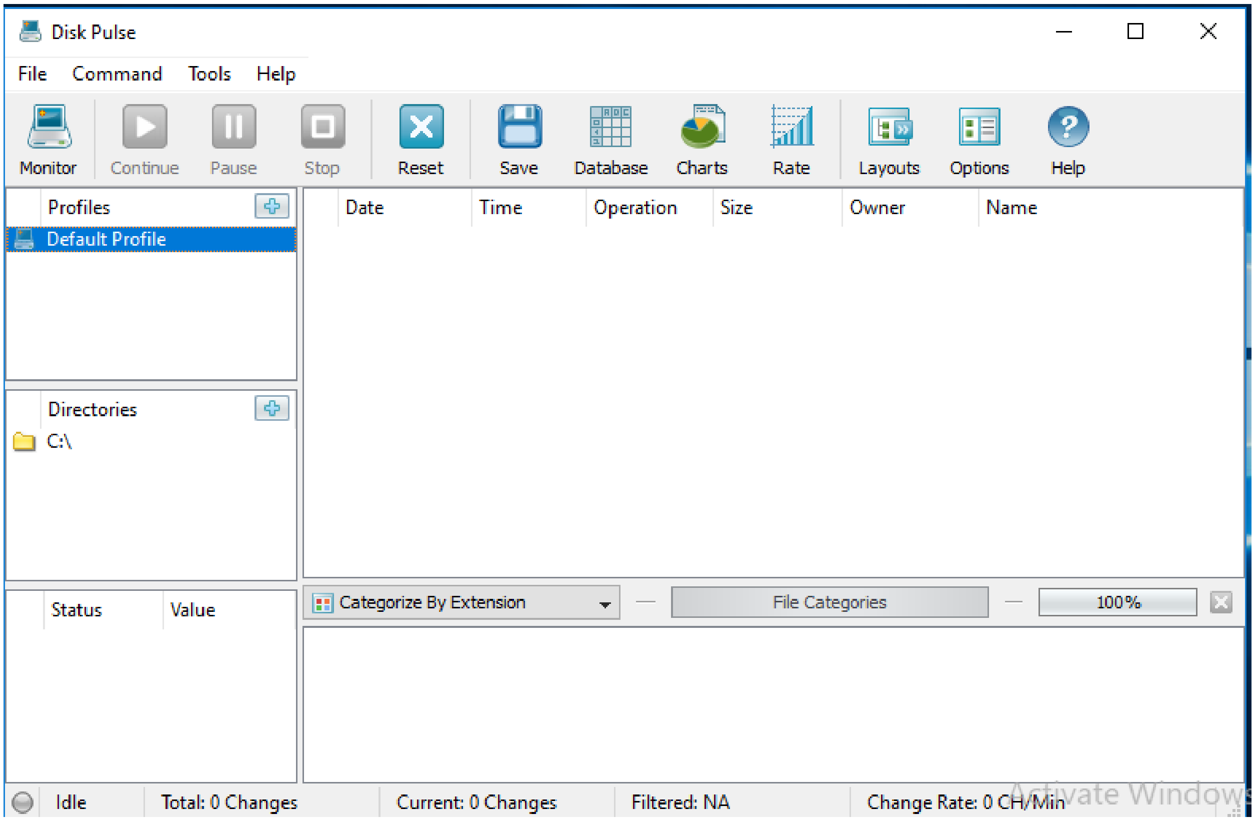
STE

☐ Copy file changes to new folder

WhatChanged

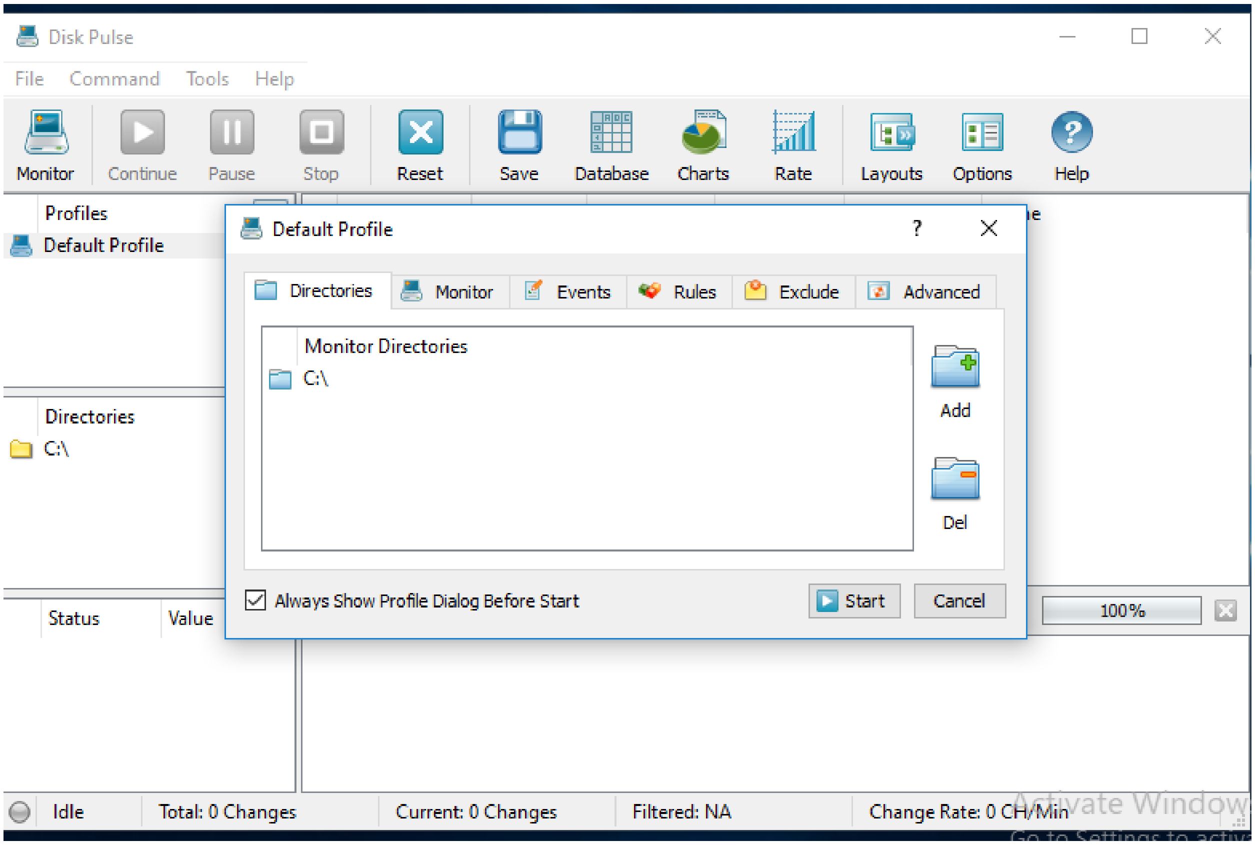
Saved a list of 199141 registry entries

- **Launch the Disk Pulse.**



Idle | Total: 0 Changes | Current: 0 Changes | Filtered: NA | Change Rate: 0 CH/Min

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



Default Profile

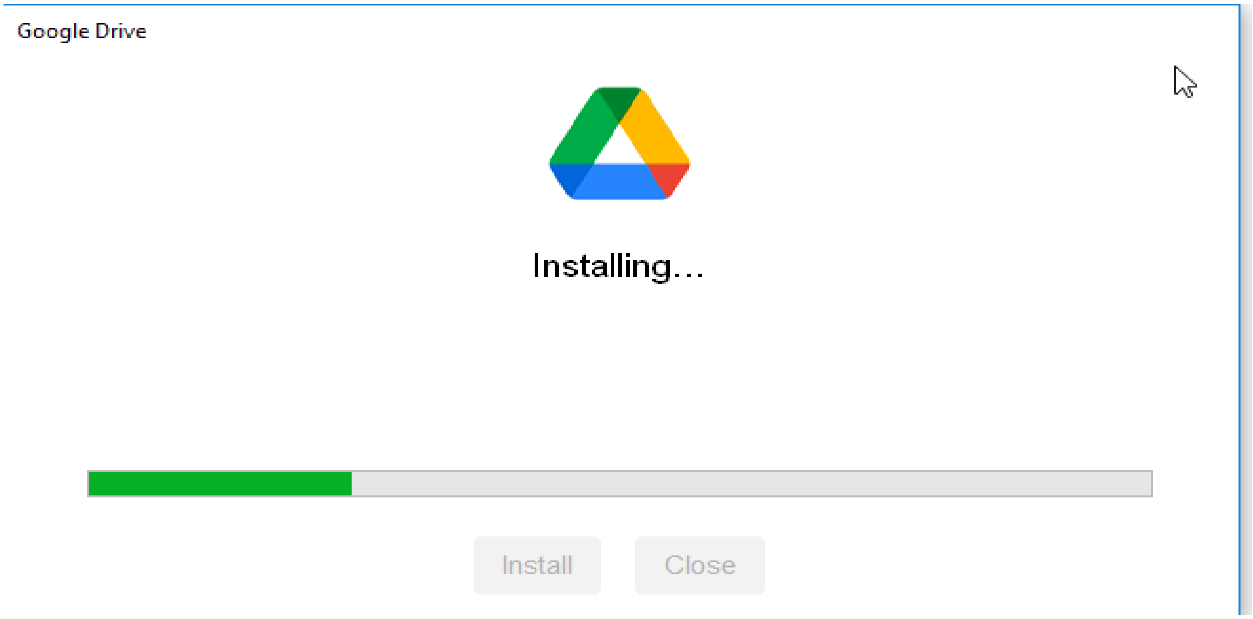
Monitor Directories

C:\

☑ Always Show Profile Dialog Before Start

Idle | Total: 0 Changes | Current: 0 Changes | Filtered: NA | Change Rate: 0 CH/Min

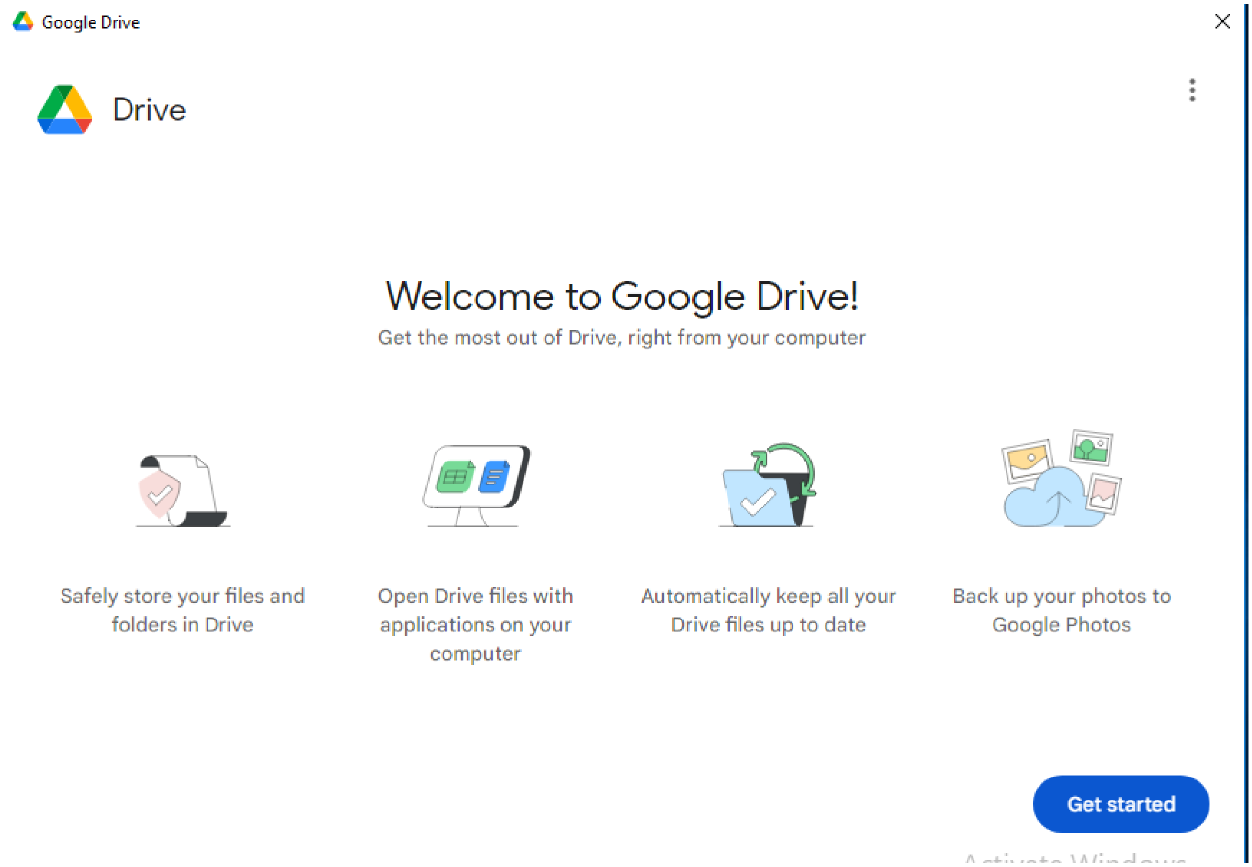
- **Install the google drive client.**



Google Drive

Installing…

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



Google Drive

Drive

Welcome to Google Drive!

Get the most out of Drive, right from your computer

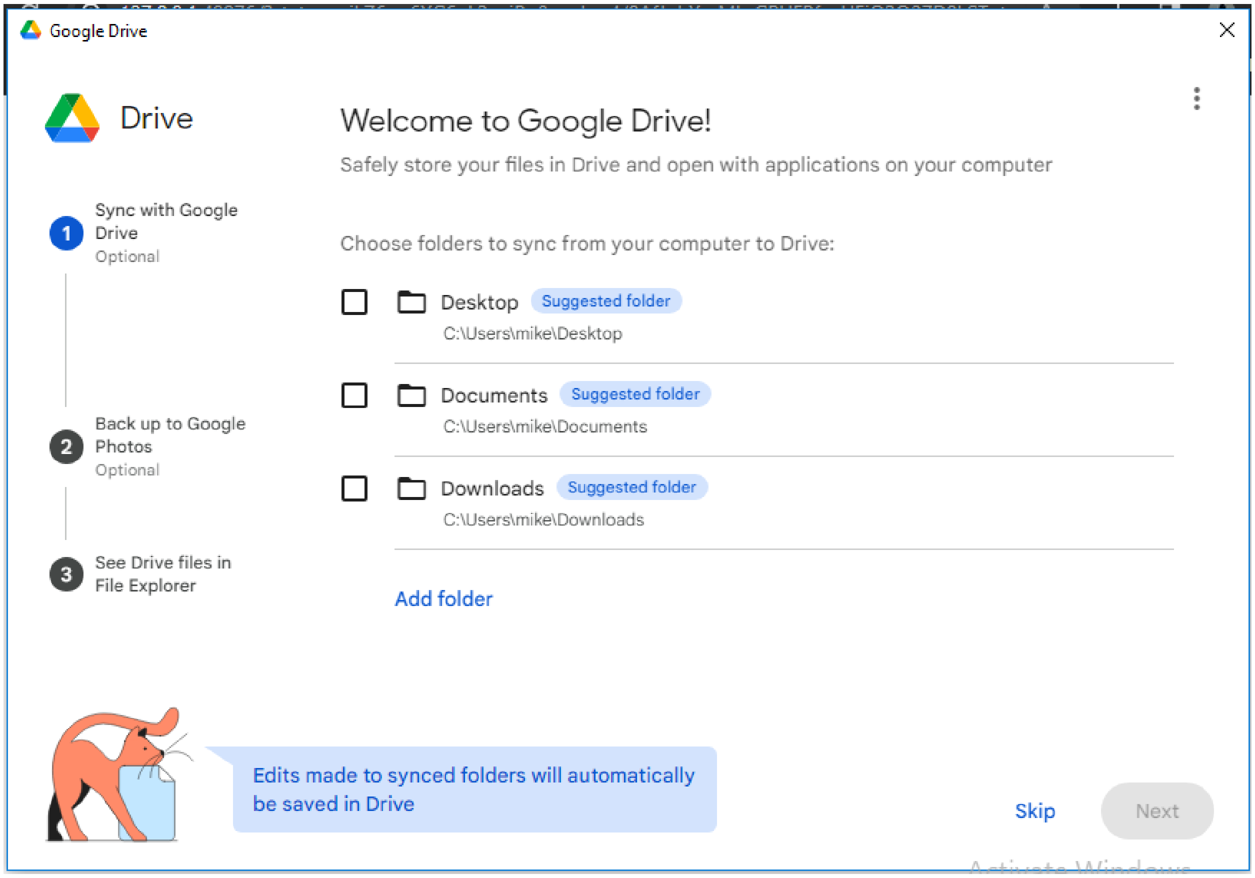
Safely store your files and folders in Drive

Open Drive files with applications on your computer

Automatically keep all your Drive files up to date

Back up your photos to Google Photos

- **Select the folder of choice to sync.**



Google Drive

Drive

Welcome to Google Drive!

Safely store your files in Drive and open with applications on your computer

1 Sync with Google Drive
Optional
2 Back up to Google Photos
Optional
3 See Drive files in File Explorer

Choose folders to sync from your computer to Drive:

□ Desktop Suggested folder
C:\Users\mike\Desktop

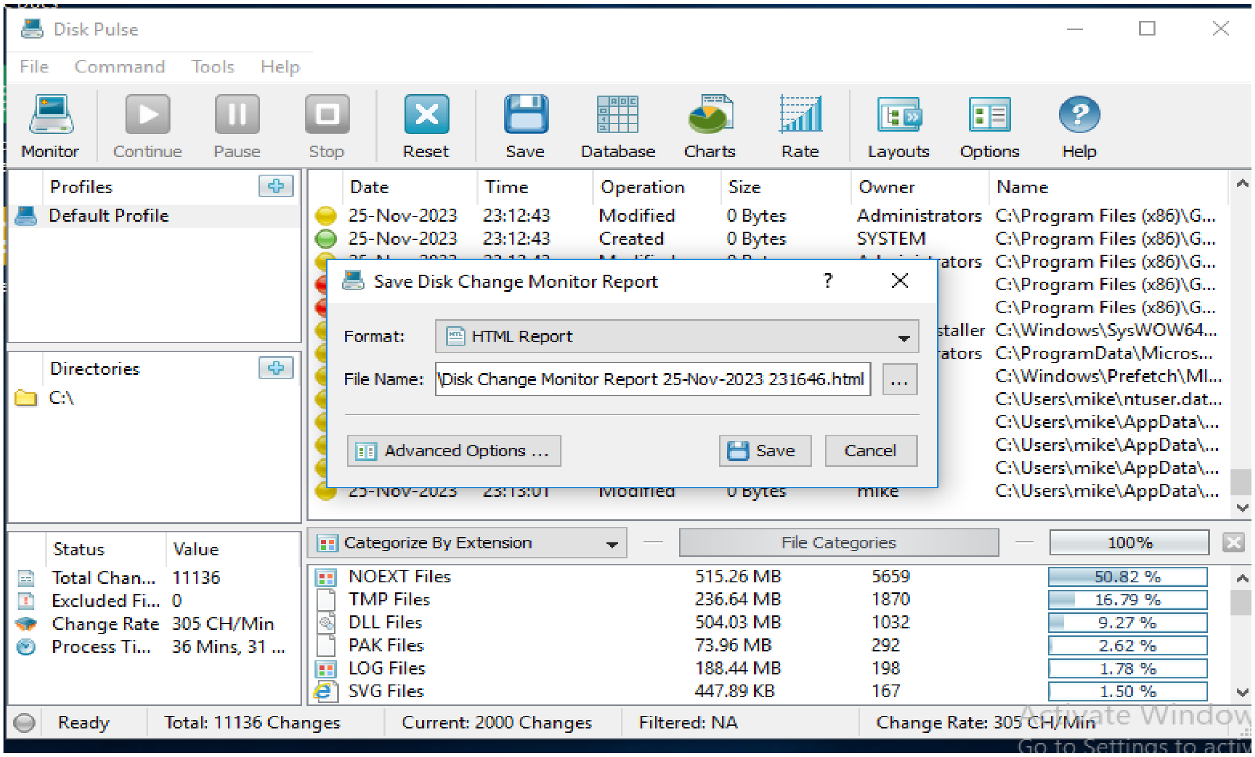
□ Documents Suggested folder
C:\Users\mike\Documents

□ Downloads Suggested folder
C:\Users\mike\Downloads

Add folder

Edits made to synced folders will automatically be saved in Drive

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



Date	Time	Operation	Size	Owner	Name
25-Nov-2023	23:12:43	Modified	0 Bytes	Administrators	C:\Program Files (x86)\G...
25-Nov-2023	23:12:43	Created	0 Bytes	SYSTEM	C:\Program Files (x86)\G...
				...ators	C:\Program Files (x86)\G...
					C:\Program Files (x86)\G...
					C:\Program Files (x86)\G...
				...staller	C:\Windows\SysWOW64...
				...ators	C:\ProgramData\Micros...
					C:\Windows\Prefetch\MI...
					C:\Users\mike\ntuser.dat...
					C:\Users\mike\AppData\...
					C:\Users\mike\AppData\...
					C:\Users\mike\AppData\...
25-Nov-2023	23:13:01	Modified	0 Bytes	mike	C:\Users\mike\AppData\...

Save Disk Change Monitor Report

Format: HTML Report

File Name: \Disk Change Monitor Report 25-Nov-2023 231646.html

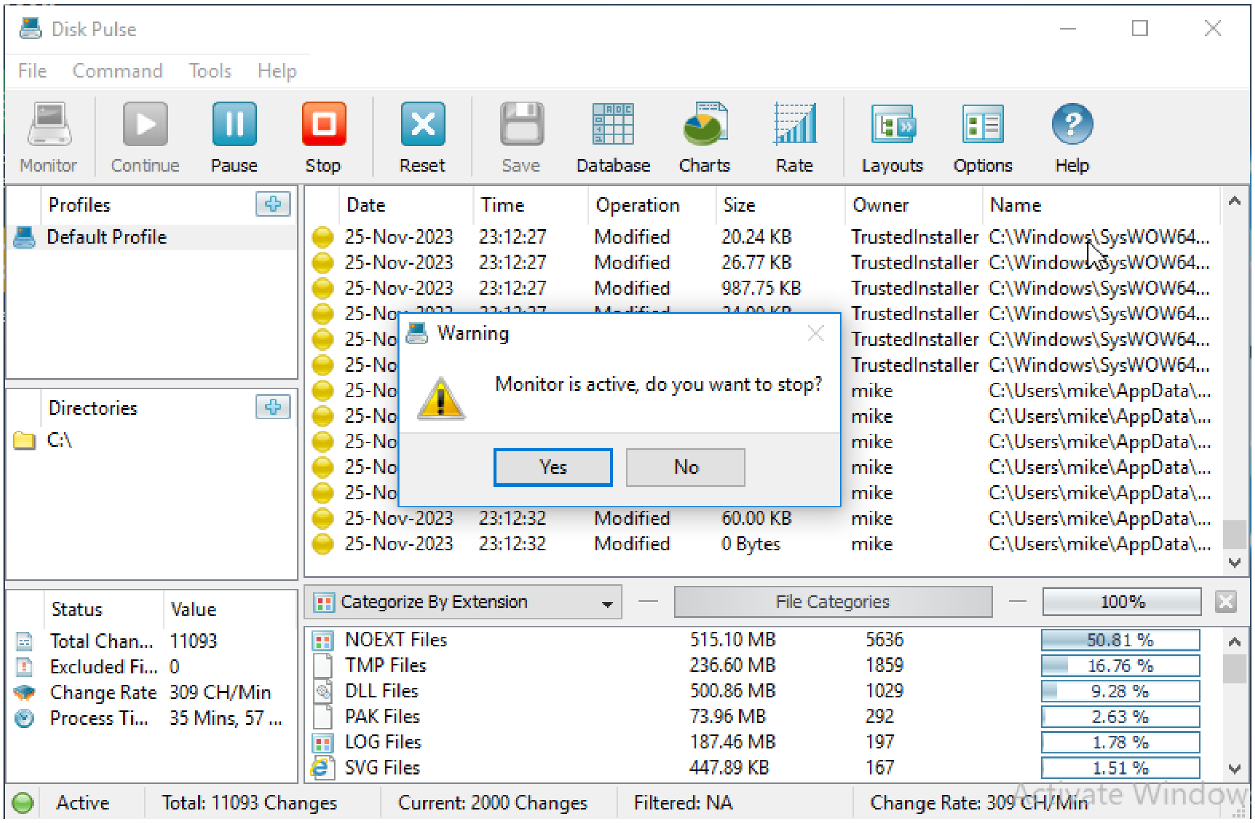
Advanced Options ... | Save | Cancel

Status	Value
Total Chan...	11136
Excluded Fi...	0
Change Rate	305 CH/Min
Process Ti...	36 Mins, 31 ...

NOEXT Files	515.26 MB	5659	50.82 %
TMP Files	236.64 MB	1870	16.79 %
DLL Files	504.03 MB	1032	9.27 %
PAK Files	73.96 MB	292	2.62 %
LOG Files	188.44 MB	198	1.78 %
SVG Files	447.89 KB	167	1.50 %

Ready | Total: 11136 Changes | Current: 2000 Changes | Filtered: NA | Change Rate: 305 CH/Min

- **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.**



Date	Time	Operation	Size	Owner	Name
25-Nov-2023	23:12:27	Modified	20.24 KB	TrustedInstaller	C:\Windows\SysWOW64...
25-Nov-2023	23:12:27	Modified	26.77 KB	TrustedInstaller	C:\Windows\SysWOW64...
25-Nov-2023	23:12:27	Modified	987.75 KB	TrustedInstaller	C:\Windows\SysWOW64...
25-No				TrustedInstaller	C:\Windows\SysWOW64...
25-No				TrustedInstaller	C:\Windows\SysWOW64...
25-No				TrustedInstaller	C:\Windows\SysWOW64...
25-No				mike	C:\Users\mike\AppData\...
25-No				mike	C:\Users\mike\AppData\...
25-No				mike	C:\Users\mike\AppData\...
25-No				mike	C:\Users\mike\AppData\...
25-No				mike	C:\Users\mike\AppData\...
25-Nov-2023	23:12:32	Modified	60.00 KB	mike	C:\Users\mike\AppData\...
25-Nov-2023	23:12:32	Modified	0 Bytes	mike	C:\Users\mike\AppData\...

Warning

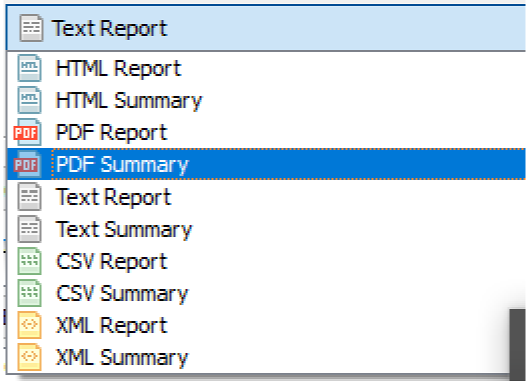
Monitor is active, do you want to stop?

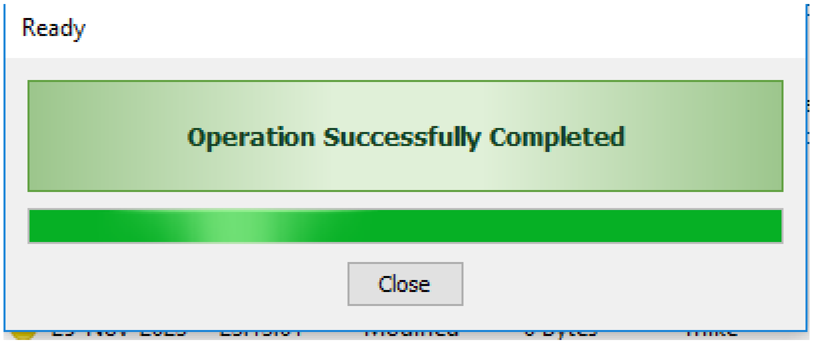
Yes No

Status	Value
Total Chan...	11093
Excluded Fi...	0
Change Rate	309 CH/Min
Process Ti...	35 Mins, 57 ...

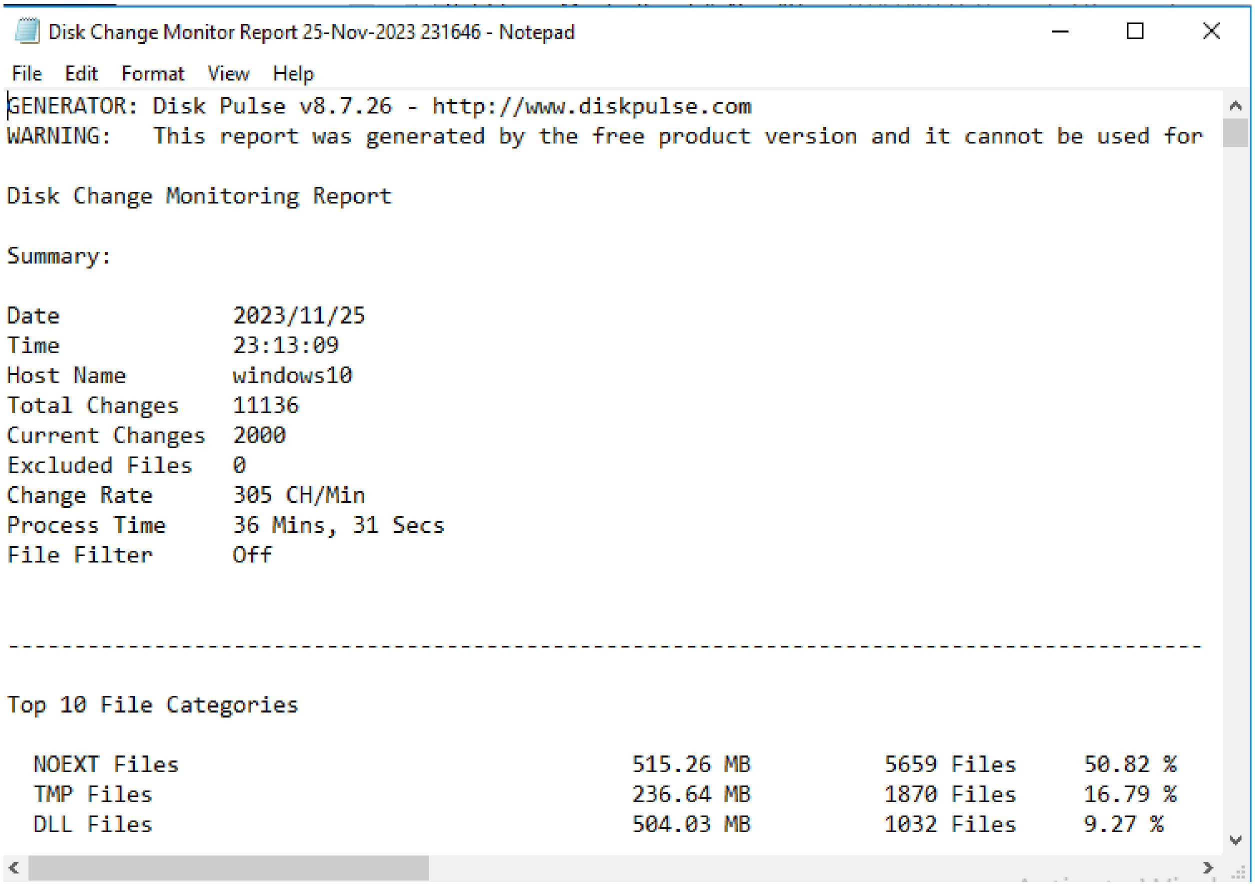
NOEXT Files	515.10 MB	5636	50.81 %
TMP Files	236.60 MB	1859	16.76 %
DLL Files	500.86 MB	1029	9.28 %
PAK Files	73.96 MB	292	2.63 %
LOG Files	187.46 MB	197	1.78 %
SVG Files	447.89 KB	167	1.51 %

Active | Total: 11093 Changes | Current: 2000 Changes | Filtered: NA | Change Rate: 309 CH/Min



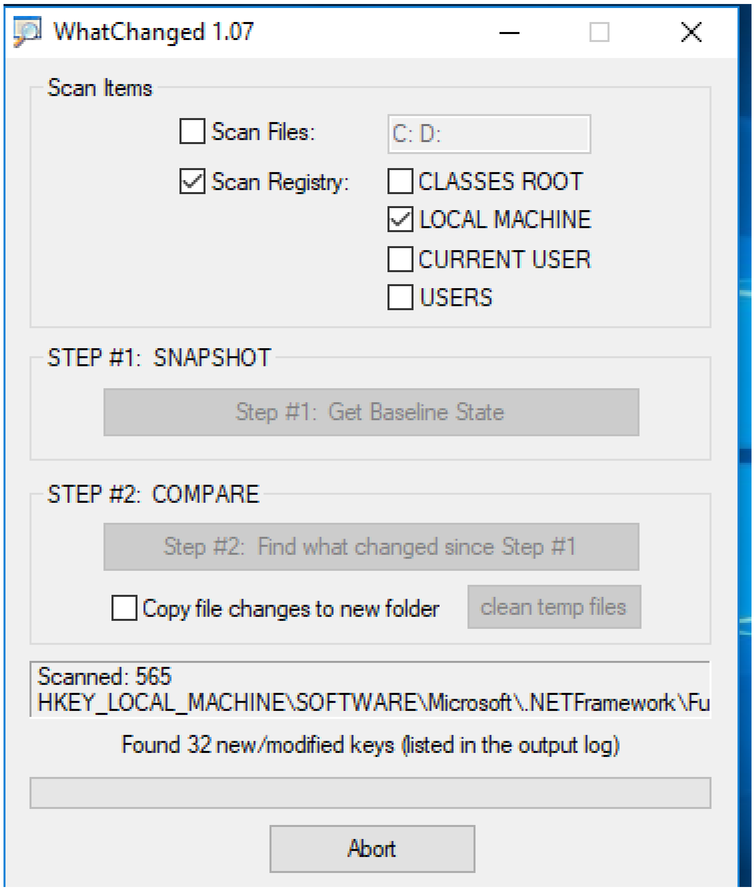


- **A text file with all changes listed on it generated by disk pulse.**


Disk Change Monitor Report 25-Nov-2023 231646 - Notepad
File Edit Format View Help

```
GENERATOR: Disk Pulse v8.7.26 - http://www.diskpulse.com
WARNING:   This report was generated by the free product version and it cannot be used for

Disk Change Monitoring Report

Summary:

Date             2023/11/25
Time             23:13:09
Host Name        windows10
Total Changes    11136
Current Changes  2000
Excluded Files   0
Change Rate      305 CH/Min
Process Time     36 Mins, 31 Secs
File Filter      Off


------------------------------------------------------------------------------------------

Top 10 File Categories

  NOEXT Files                                  515.26 MB          5659 Files      50.82 %
  TMP Files                                    236.64 MB          1870 Files      16.79 %
  DLL Files                                    504.03 MB          1032 Files      9.27 %
```

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



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

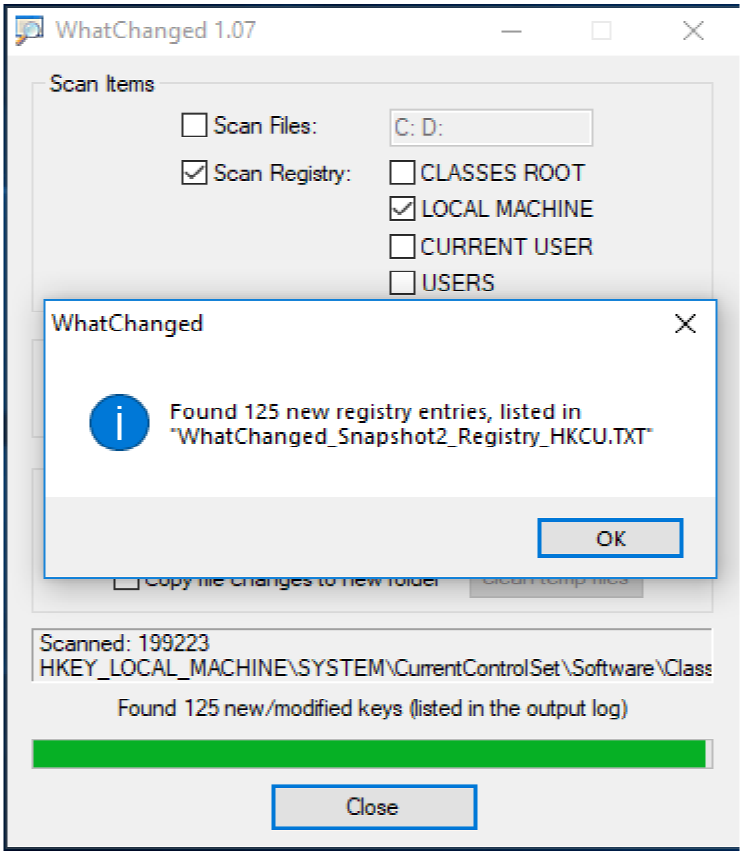
clean temp files

```
Scanned: 565
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Fu
```

Found 32 new/modified keys (listed in the output log)

Abort

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



WhatChanged 1.07

Scan Items

□ Scan Files: C: D:

☑ Scan Registry: □ CLASSES ROOT
☑ LOCAL MACHINE
□ CURRENT USER
□ USERS

WhatChanged

Found 125 new registry entries, listed in "WhatChanged_Snapshot2_Registry_HKCU.TXT"

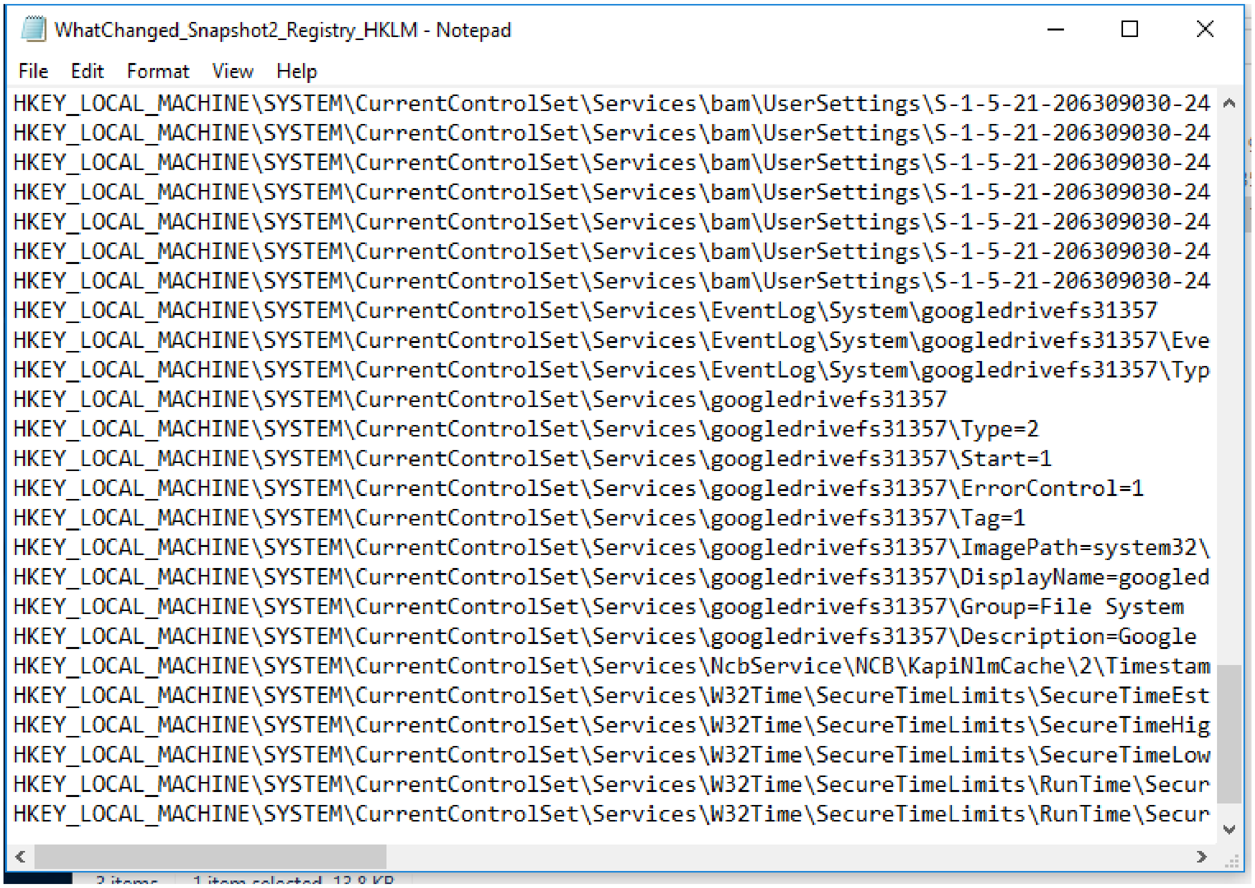
OK

□ Copy file changes to new folder

Scanned: 199223
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Software\Class

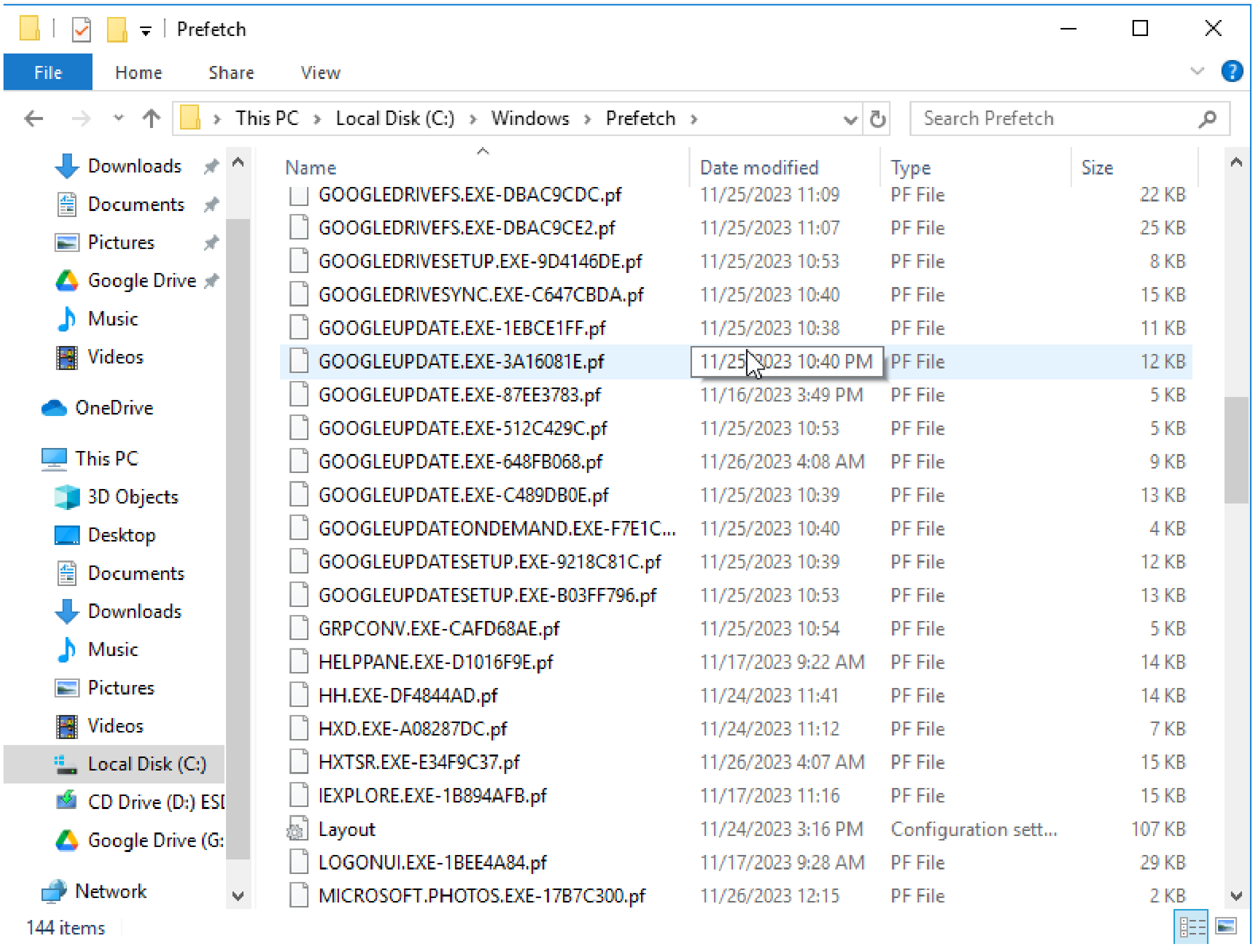
Found 125 new/modified keys (listed in the output log)

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



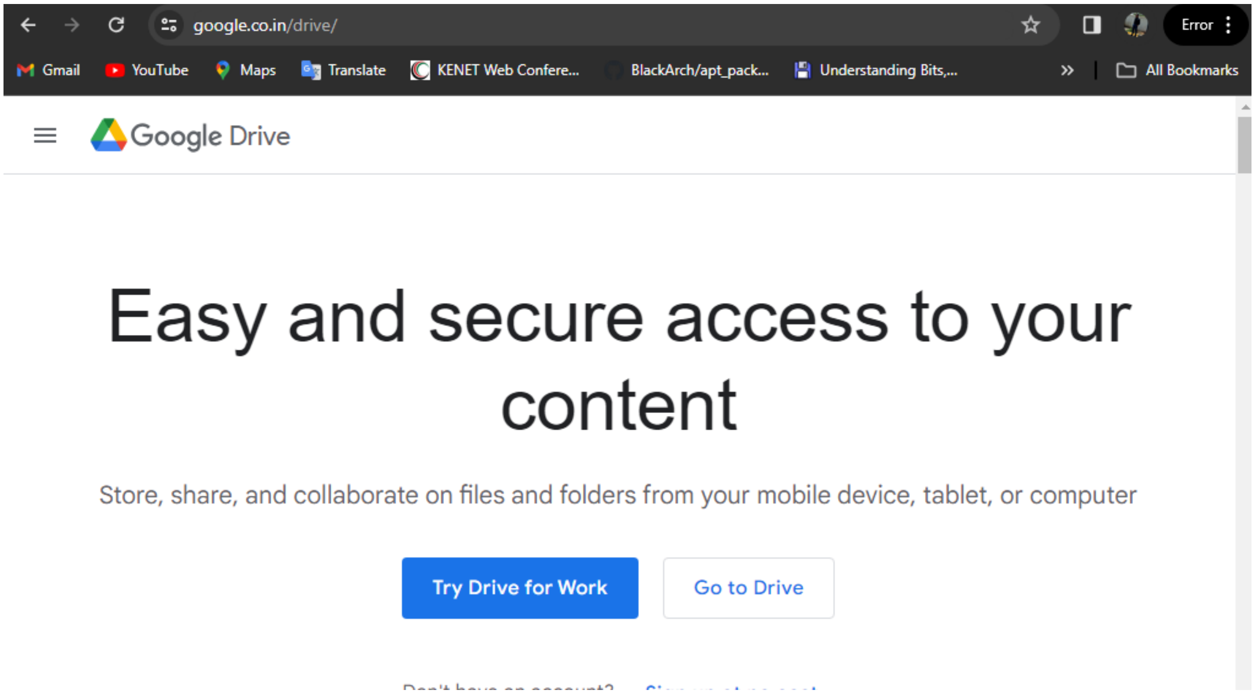
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-206309030-24
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-206309030-24
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-206309030-24
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-206309030-24
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
```

- **Other files created during installation by google drive.**



Name	Date modified	Type	Size
GOOGLEDRIVEFS.EXE-DBAC9CDC.pf	11/25/2023 11:09	PF File	22 KB
GOOGLEDRIVEFS.EXE-DBAC9CE2.pf	11/25/2023 11:07	PF File	25 KB
GOOGLEDRIVESETUP.EXE-9D4146DE.pf	11/25/2023 10:53	PF File	8 KB
GOOGLEDRIVESYNC.EXE-C647CBDA.pf	11/25/2023 10:40	PF File	15 KB
GOOGLEUPDATE.EXE-1EBCE1FF.pf	11/25/2023 10:38	PF File	11 KB
GOOGLEUPDATE.EXE-3A16081E.pf	11/25/2023 10:40 PM	PF File	12 KB
GOOGLEUPDATE.EXE-87EE3783.pf	11/16/2023 3:49 PM	PF File	5 KB
GOOGLEUPDATE.EXE-512C429C.pf	11/25/2023 10:53	PF File	5 KB
GOOGLEUPDATE.EXE-648FB068.pf	11/26/2023 4:08 AM	PF File	9 KB
GOOGLEUPDATE.EXE-C489DB0E.pf	11/25/2023 10:39	PF File	13 KB
GOOGLEUPDATEONDEMAND.EXE-F7E1C...	11/25/2023 10:40	PF File	4 KB
GOOGLEUPDATESETUP.EXE-9218C81C.pf	11/25/2023 10:39	PF File	12 KB
GOOGLEUPDATESETUP.EXE-B03FF796.pf	11/25/2023 10:53	PF File	13 KB
GRPCONV.EXE-CAFD68AE.pf	11/25/2023 10:54	PF File	5 KB
HELPPANE.EXE-D1016F9E.pf	11/17/2023 9:22 AM	PF File	14 KB
HH.EXE-DF4844AD.pf	11/24/2023 11:41	PF File	14 KB
HXD.EXE-A08287DC.pf	11/24/2023 11:12	PF File	7 KB
HXTSR.EXE-E34F9C37.pf	11/26/2023 4:07 AM	PF File	15 KB
IEXPLORE.EXE-1B894AFB.pf	11/17/2023 11:16	PF File	15 KB
Layout	11/24/2023 3:16 PM	Configuration sett...	107 KB
LOGONUI.EXE-1BEE4A84.pf	11/17/2023 9:28 AM	PF File	29 KB
MICROSOFT.PHOTOS.EXE-17B7C300.pf	11/26/2023 12:15	PF File	2 KB

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

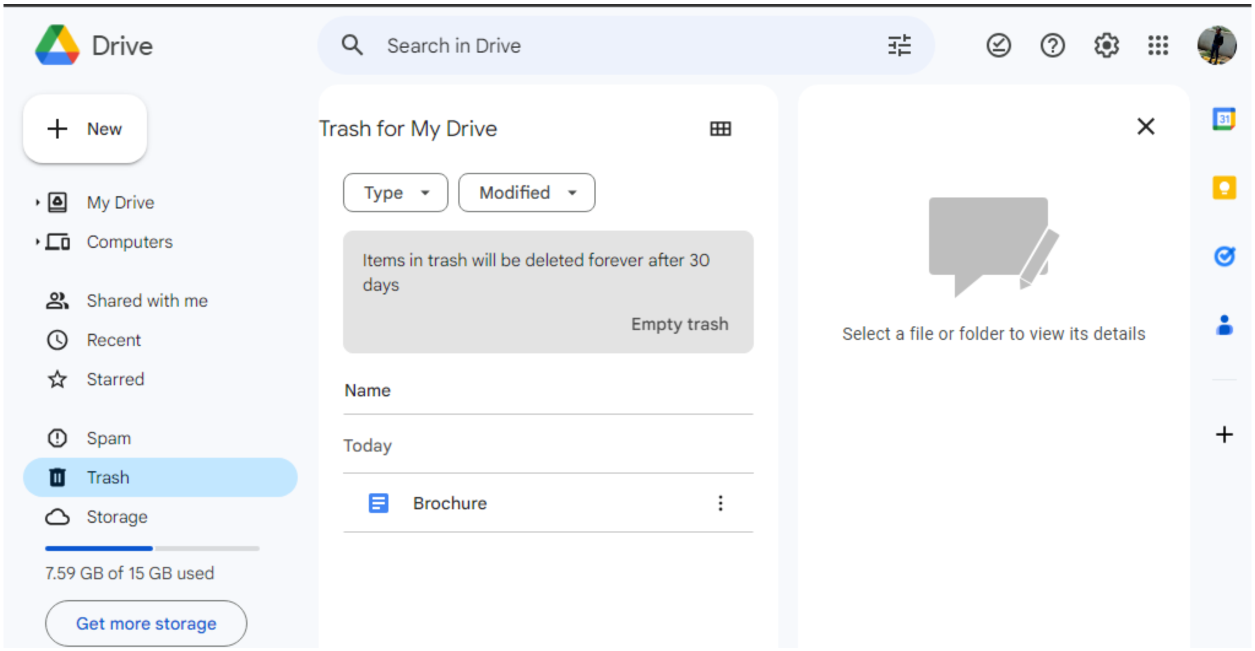


google.co.in/drive/

Easy and secure access to your content

Store, share, and collaborate on files and folders from your mobile device, tablet, or computer

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



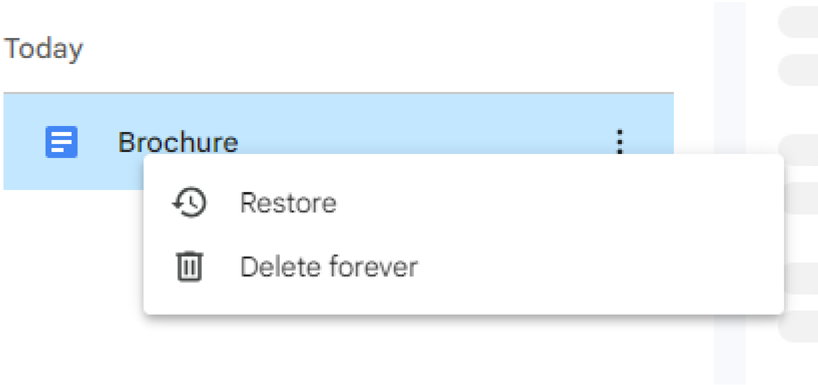
Trash for My Drive

Items in trash will be deleted forever after 30 days

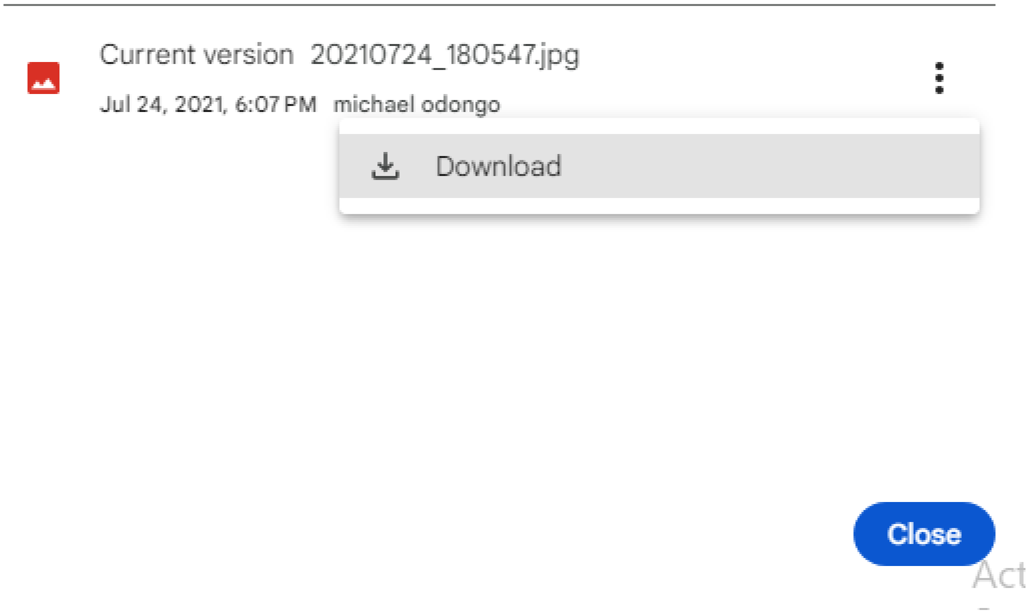
Select a file or folder to view its details

7.59 GB of 15 GB used

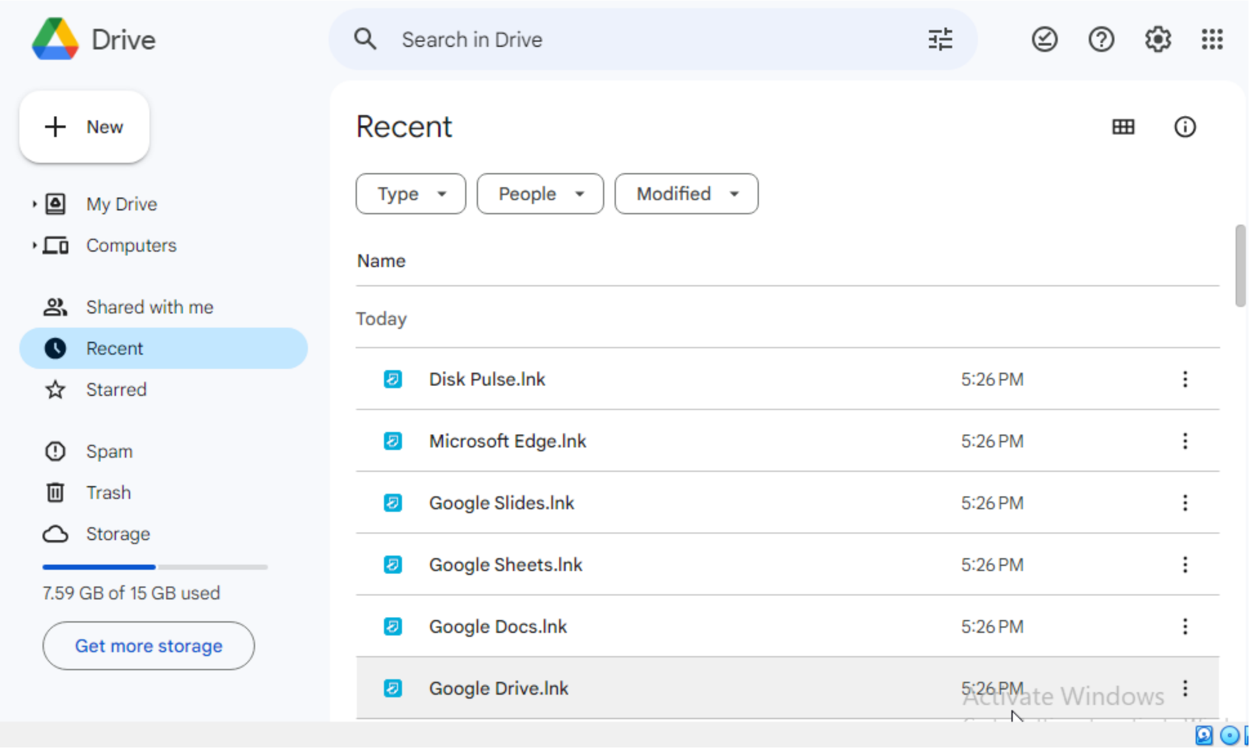
- **In the trash section, right click on any image to see options such as: Restore and Delete Forever.**



- **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.**


Current version 20210724_180547.jpg
Jul 24, 2021, 6:07 PM michael odongo
Download
Close
Act

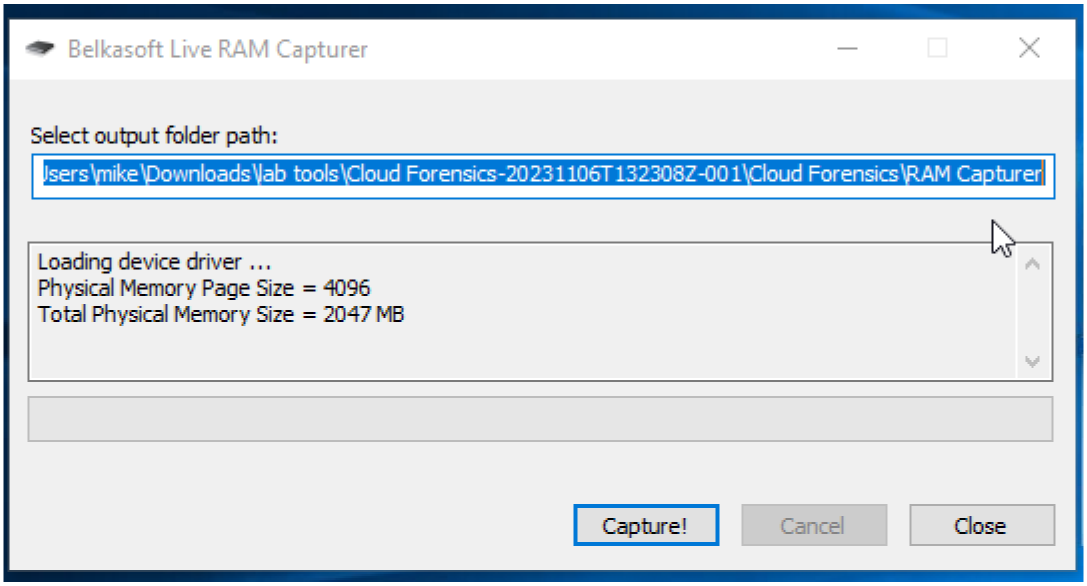
- **Click on the recent in the left pane to view the recently accessed files.**



Recent

Name	
Today	
Disk Pulse.lnk	5:26 PM
Microsoft Edge.lnk	5:26 PM
Google Slides.lnk	5:26 PM
Google Sheets.lnk	5:26 PM
Google Docs.lnk	5:26 PM
Google Drive.lnk	5:26 PM

- **Launch the RAM capturer.**

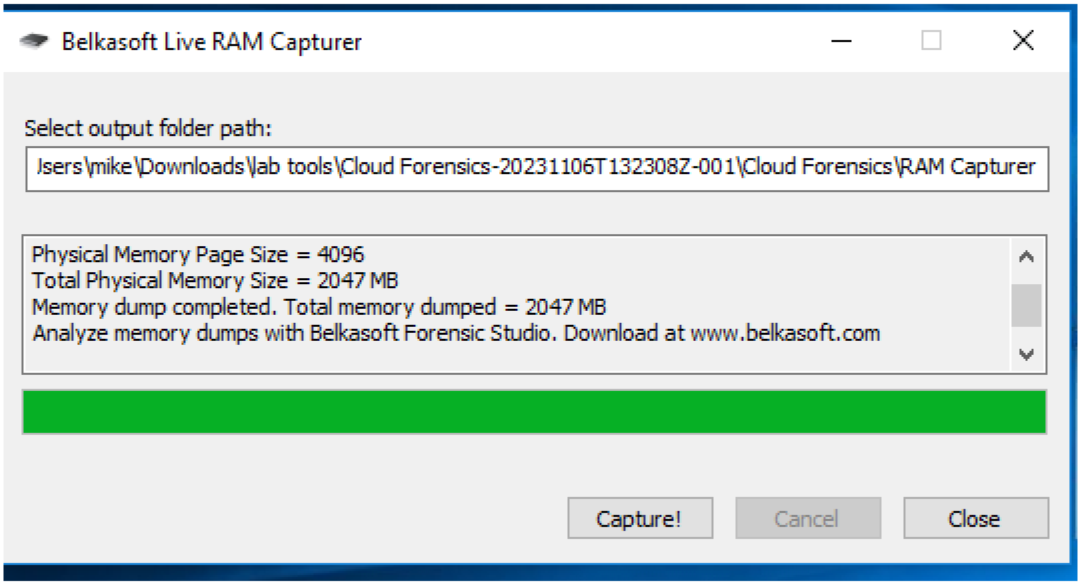


Select output folder path:

Jsers\mike\Downloads\lab tools\Cloud Forensics-20231106T132308Z-001\Cloud Forensics\RAM Capturer

```
Loading device driver ...
Physical Memory Page Size = 4096
Total Physical Memory Size = 2047 MB
```

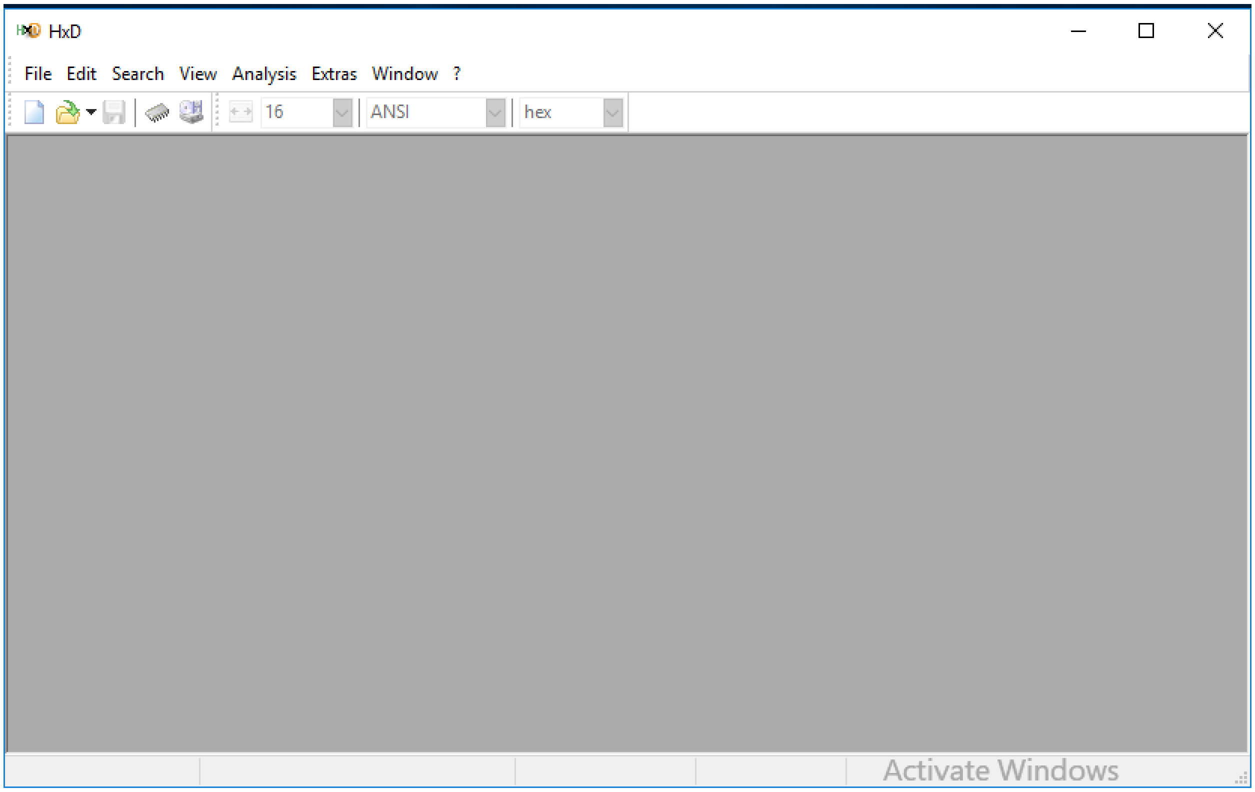
- **Click on the capture button and once done click on close.**



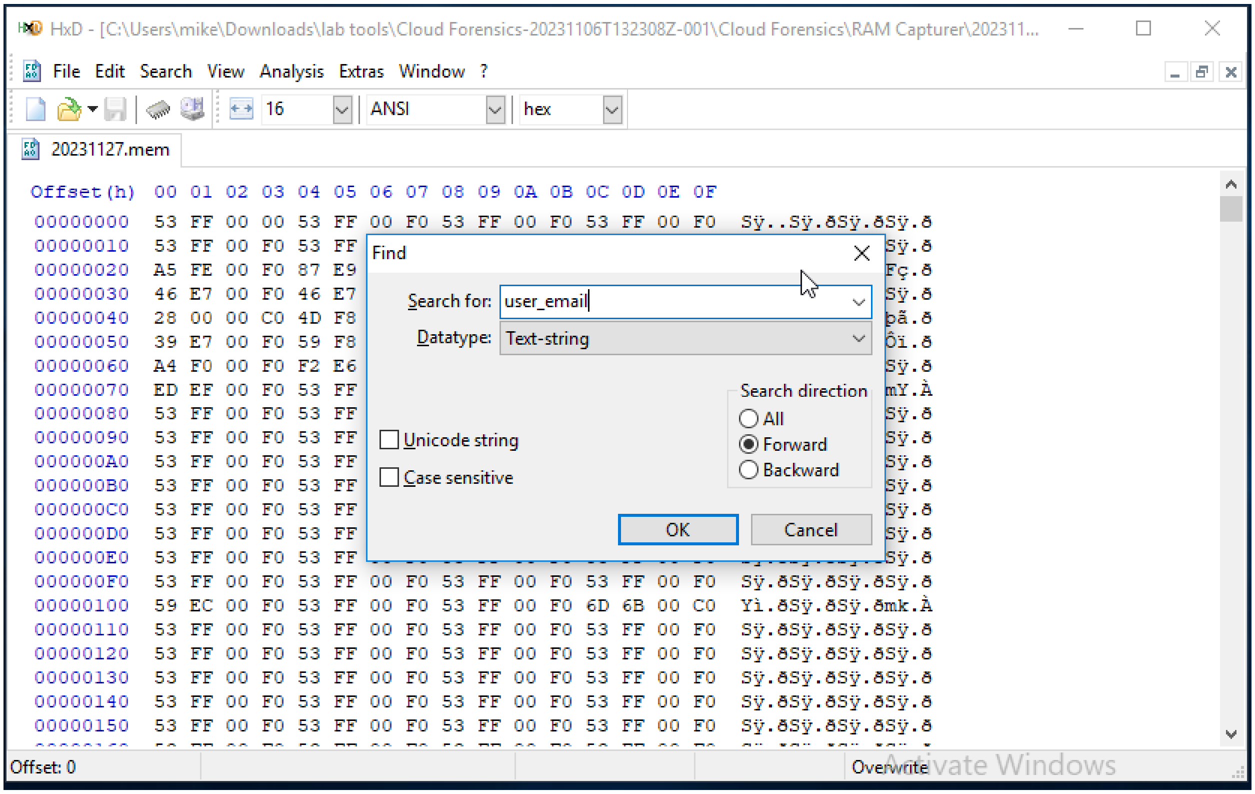
Select output folder path:
Jsers\mike\Downloads\lab tools\Cloud Forensics-20231106T132308Z-001\Cloud Forensics\RAM Capturer

```
Physical Memory Page Size = 4096
Total Physical Memory Size = 2047 MB
Memory dump completed. Total memory dumped = 2047 MB
Analyze memory dumps with Belkasoft Forensic Studio. Download at www.belkasoft.com
```

- **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.**



HxD - [C:\Users\mike\Downloads\lab tools\Cloud Forensics-20231106T132308Z-001\Cloud Forensics\RAM Capturer\202311...
File Edit Search View Analysis Extras Window ?
20231127.mem

16 | ANSI | hex

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  53 FF 00 00 53 FF 00 F0 53 FF 00 F0 53 FF 00 F0  Sÿ..Sÿ.ðSÿ.ðSÿ.ð
00000010  53 FF 00 F0 53 FF                                Sÿ.ð
00000020  A5 FE 00 F0 87 E9                                Fç.ð
00000030  46 E7 00 F0 46 E7                                Sÿ.ð
00000040  28 00 00 C0 4D F8                                þã.ð
00000050  39 E7 00 F0 59 F8                                Ôì.ð
00000060  A4 F0 00 F0 F2 E6                                Sÿ.ð
00000070  ED EF 00 F0 53 FF                                mY.À
00000080  53 FF 00 F0 53 FF                                Sÿ.ð
00000090  53 FF 00 F0 53 FF                                Sÿ.ð
000000A0  53 FF 00 F0 53 FF                                Sÿ.ð
000000B0  53 FF 00 F0 53 FF                                Sÿ.ð
000000C0  53 FF 00 F0 53 FF                                Sÿ.ð
000000D0  53 FF 00 F0 53 FF                                Sÿ.ð
000000E0  53 FF 00 F0 53 FF                                Sÿ.ð
000000F0  53 FF 00 F0 53 FF 00 F0 53 FF 00 F0 53 FF 00 F0  Sÿ.ðSÿ.ðSÿ.ðSÿ.ð
00000100  59 EC 00 F0 53 FF 00 F0 53 FF 00 F0 6D 6B 00 C0  Yì.ðSÿ.ðSÿ.ðmk.À
00000110  53 FF 00 F0 53 FF 00 F0 53 FF 00 F0 53 FF 00 F0  Sÿ.ðSÿ.ðSÿ.ðSÿ.ð
00000120  53 FF 00 F0 53 FF 00 F0 53 FF 00 F0 53 FF 00 F0  Sÿ.ðSÿ.ðSÿ.ðSÿ.ð
00000130  53 FF 00 F0 53 FF 00 F0 53 FF 00 F0 53 FF 00 F0  Sÿ.ðSÿ.ðSÿ.ðSÿ.ð
00000140  53 FF 00 F0 53 FF 00 F0 53 FF 00 F0 53 FF 00 F0  Sÿ.ðSÿ.ðSÿ.ðSÿ.ð
00000150  53 FF 00 F0 53 FF 00 F0 53 FF 00 F0 53 FF 00 F0  Sÿ.ðSÿ.ðSÿ.ðSÿ.ð
```

Find

Search for: user_email

Datatype: Text-string

□ Unicode string

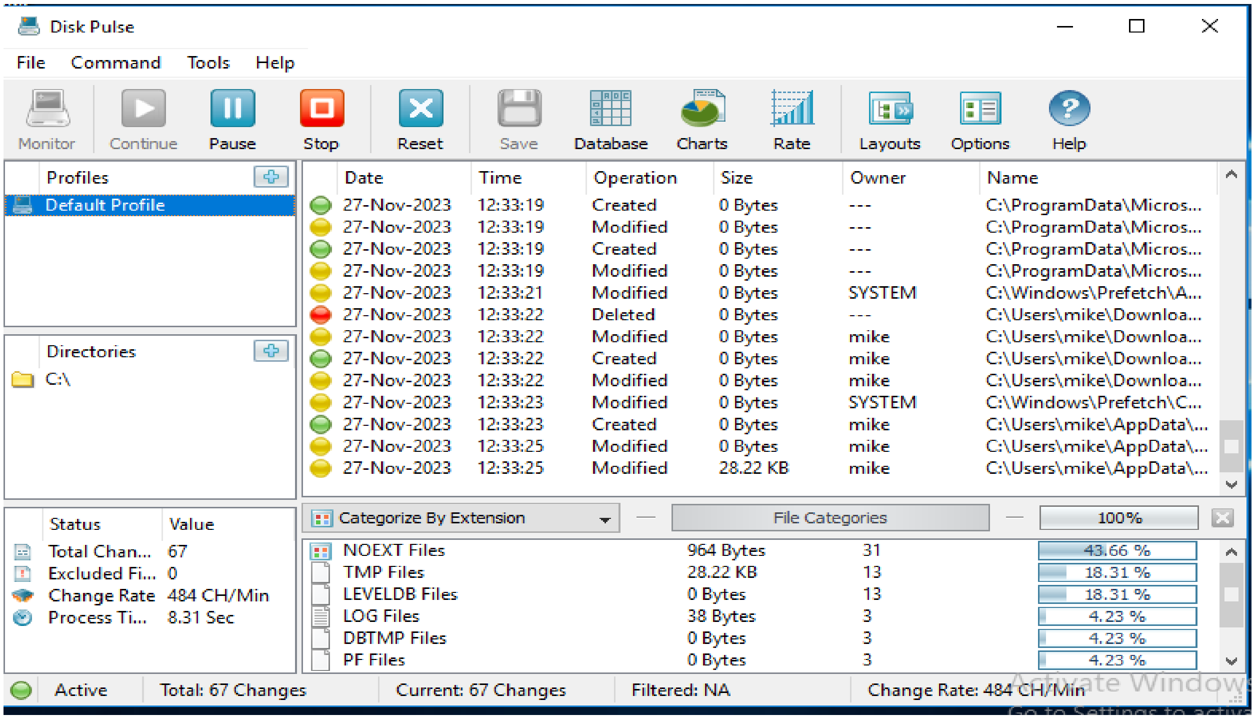
□ Case sensitive

Search direction

○ All
● Forward
○ Backward

Offset: 0 | Overwrite

- **Launch disk pulse and click on monitor.**



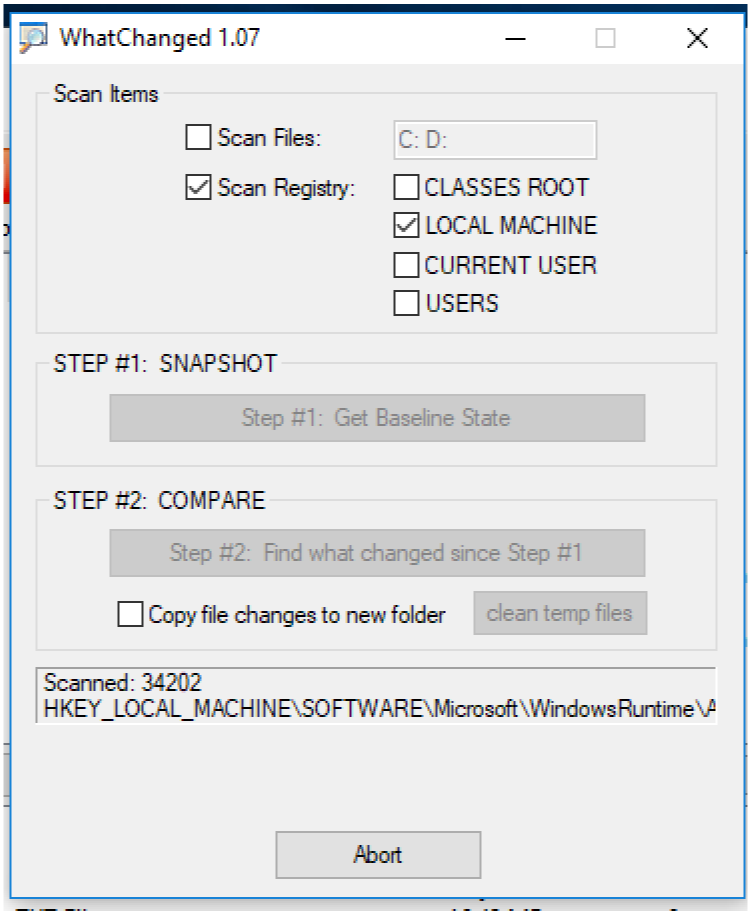
	Date	Time	Operation	Size	Owner	Name
🟢	27-Nov-2023	12:33:19	Created	0 Bytes	---	C:\ProgramData\Micros...
🟡	27-Nov-2023	12:33:19	Modified	0 Bytes	---	C:\ProgramData\Micros...
🟢	27-Nov-2023	12:33:19	Created	0 Bytes	---	C:\ProgramData\Micros...
🟡	27-Nov-2023	12:33:19	Modified	0 Bytes	---	C:\ProgramData\Micros...
🟡	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\...

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

NOEXT Files	964 Bytes	31	43.66 %
TMP Files	28.22 KB	13	18.31 %
LEVELDB Files	0 Bytes	13	18.31 %
LOG Files	38 Bytes	3	4.23 %
DBTMP Files	0 Bytes	3	4.23 %
PF Files	0 Bytes	3	4.23 %

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

- **Lauch WhatChanged and click on ‘Get Baseline state’.**



☐ Scan Files: C: D:

☑ Scan Registry:

☐ CLASSES ROOT

☑ LOCAL MACHINE

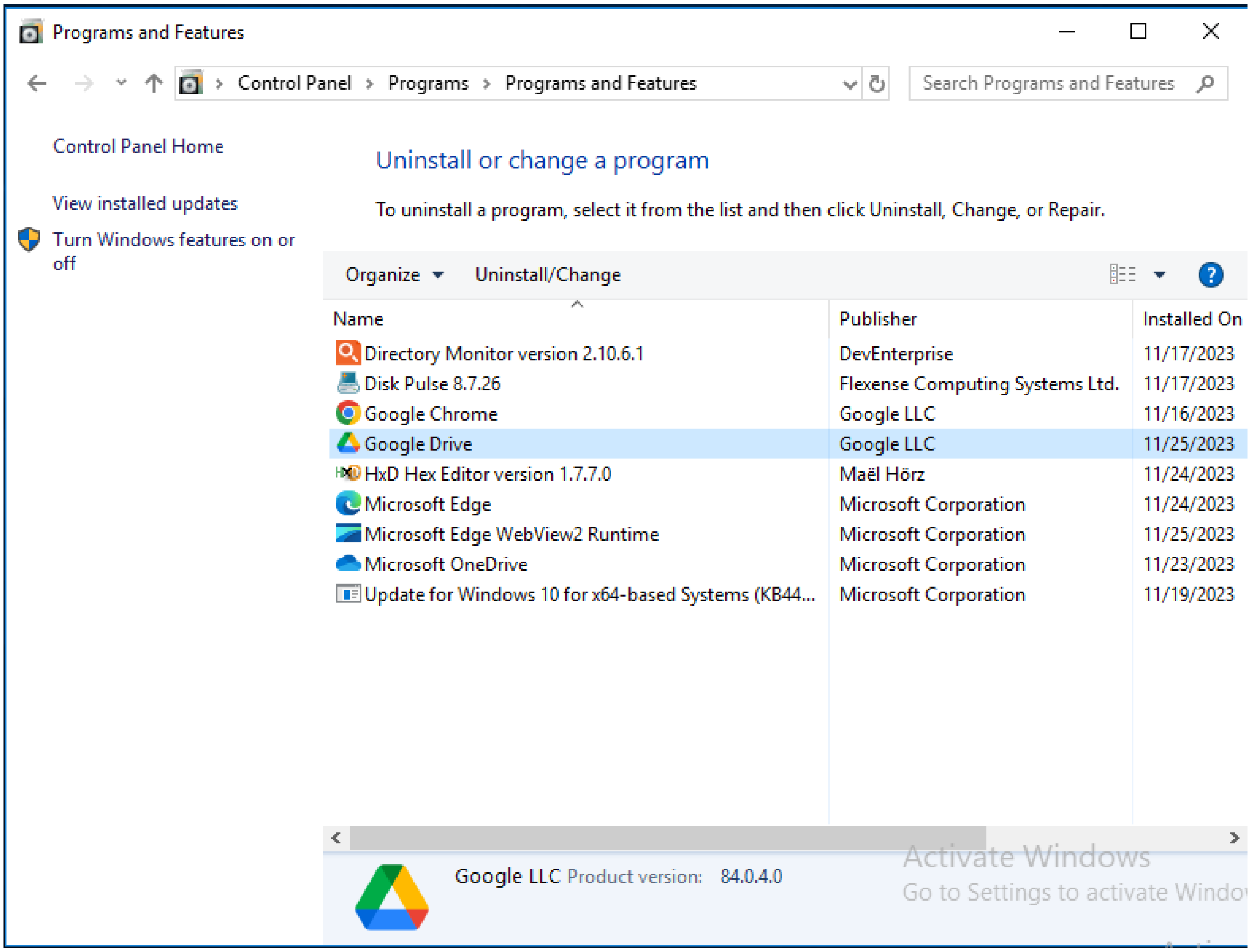
☐ CURRENT USER

☐ USERS

☐ Copy file changes to new folder

```
Scanned: 34202
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsRuntime\A
```

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

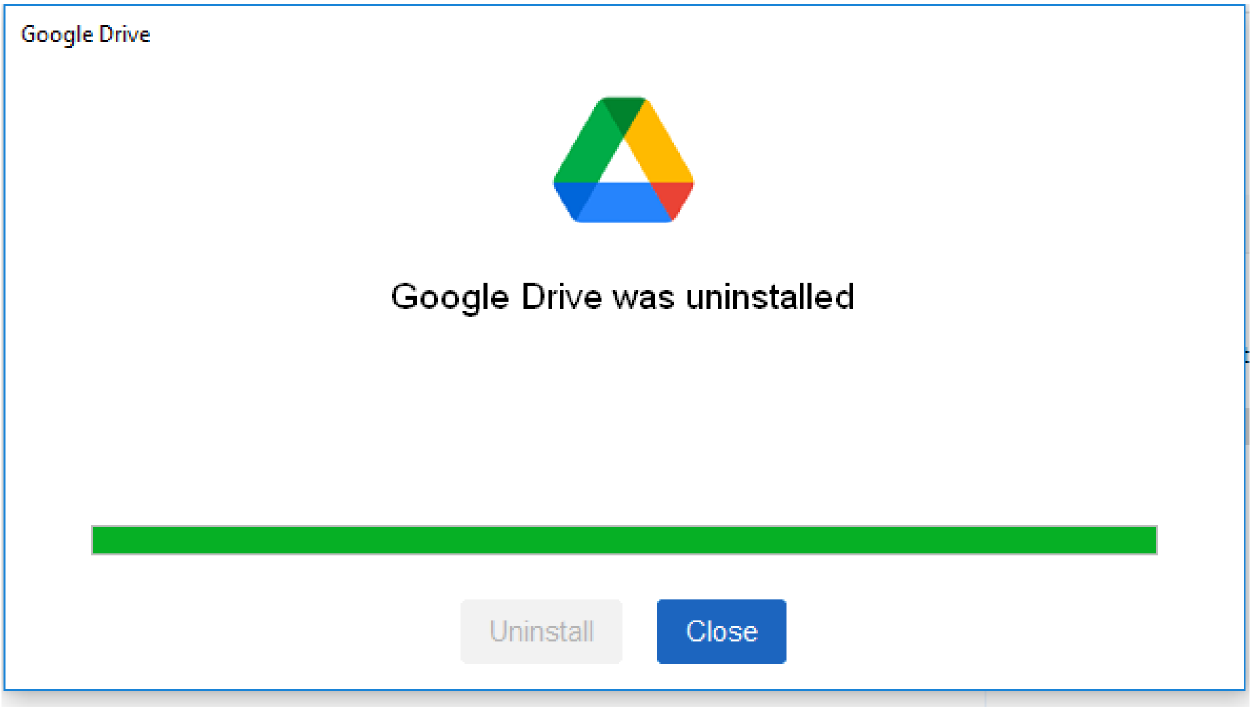

Programs and Features
Control Panel › Programs › Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾
Uninstall/Change
Activate Windows
Go to Settings to activate Windo

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

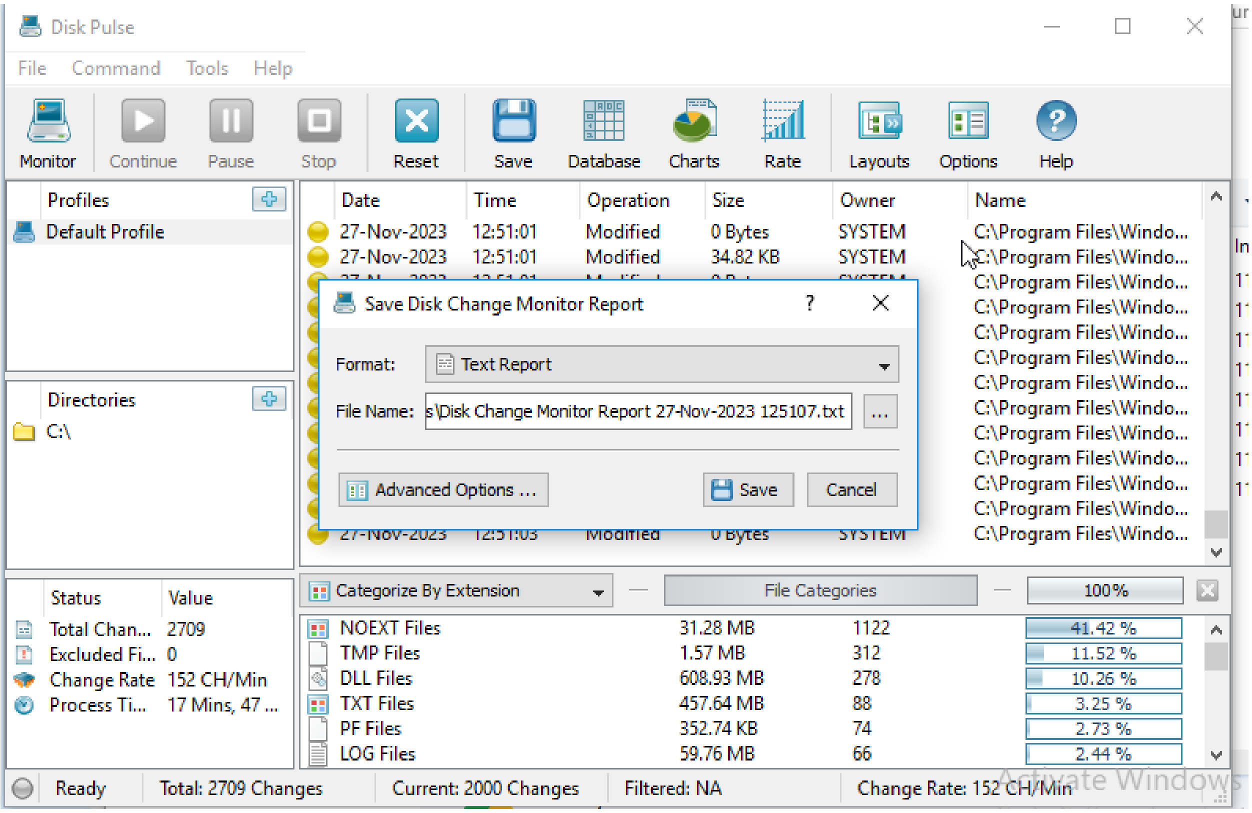
Name	Publisher	Installed On
Directory Monitor version 2.10.6.1	DevEnterprise	11/17/2023
Disk Pulse 8.7.26	Flexense Computing Systems Ltd.	11/17/2023
Google Chrome	Google LLC	11/16/2023
Google Drive	Google LLC	11/25/2023
HxD Hex Editor version 1.7.7.0	Maël Hörz	11/24/2023
Microsoft Edge	Microsoft Corporation	11/24/2023
Microsoft Edge WebView2 Runtime	Microsoft Corporation	11/25/2023
Microsoft OneDrive	Microsoft Corporation	11/23/2023
Update for Windows 10 for x64-based Systems (KB44...	Microsoft Corporation	11/19/2023

Google LLC Product version: 84.0.4.0



Google Drive was uninstalled

- **After uninstalling google drive, navigate to disk pulse and click on stop and save to save all changes.**



Date	Time	Operation	Size	Owner	Name
27-Nov-2023	12:51:01	Modified	0 Bytes	SYSTEM	C:\Program Files\Windo...
27-Nov-2023	12:51:01	Modified	34.82 KB	SYSTEM	C:\Program Files\Windo...
					C:\Program Files\Windo...
					C:\Program Files\Windo...
					C:\Program Files\Windo...
					C:\Program Files\Windo...
					C:\Program Files\Windo...
					C:\Program Files\Windo...
					C:\Program Files\Windo...
					C:\Program Files\Windo...
					C:\Program Files\Windo...
					C:\Program Files\Windo...
27-Nov-2023	12:51:03	Modified	0 Bytes	SYSTEM	C:\Program Files\Windo...

Save Disk Change Monitor Report

Format: Text Report

File Name: s\Disk Change Monitor Report 27-Nov-2023 125107.txt

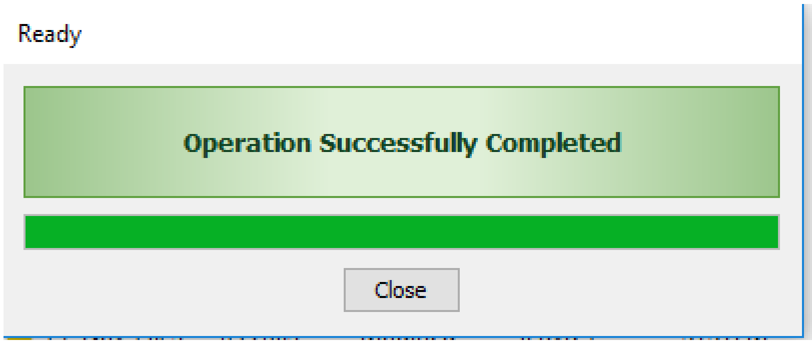
Advanced Options ... | Save | Cancel

Status	Value
Total Chan...	2709
Excluded Fi...	0
Change Rate	152 CH/Min
Process Ti...	17 Mins, 47 ...

Categorize By Extension — File Categories — 100%

NOEXT Files	31.28 MB	1122	41.42 %
TMP Files	1.57 MB	312	11.52 %
DLL Files	608.93 MB	278	10.26 %
TXT Files	457.64 MB	88	3.25 %
PF Files	352.74 KB	74	2.73 %
LOG Files	59.76 MB	66	2.44 %

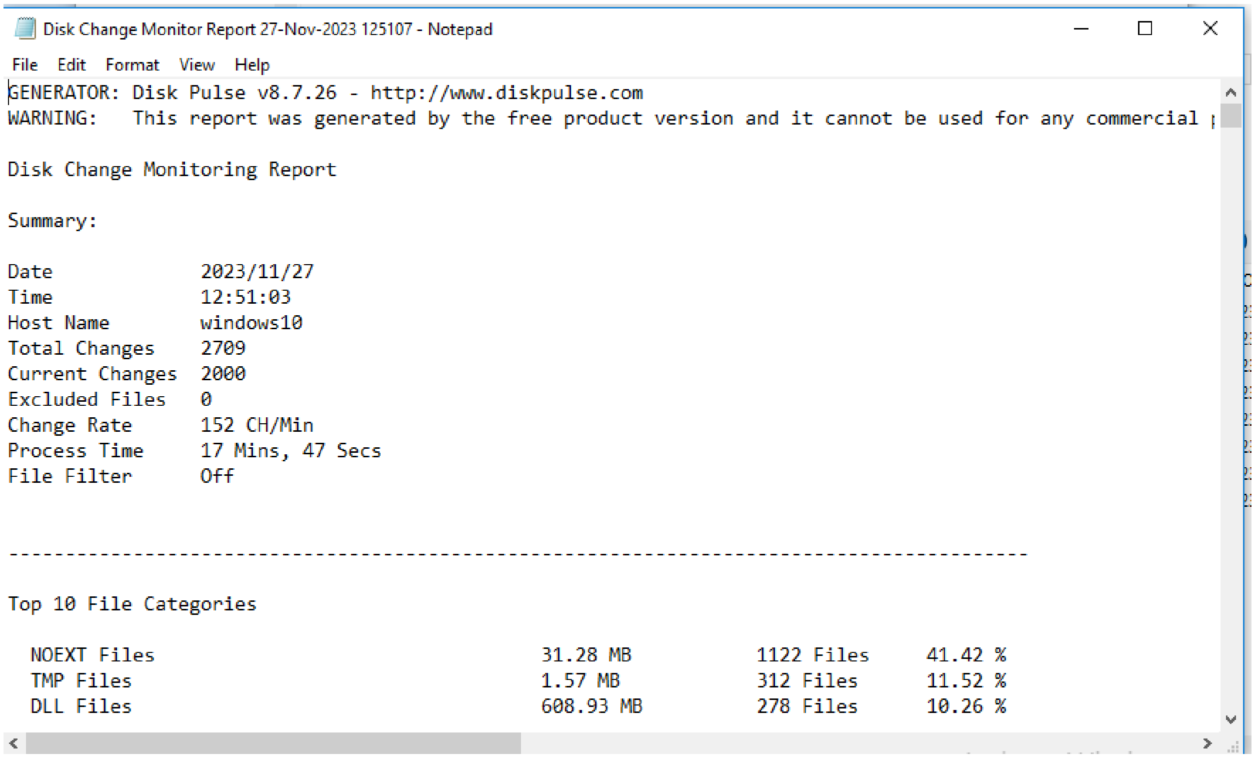
Ready | Total: 2709 Changes | Current: 2000 Changes | Filtered: NA | Change Rate: 152 CH/Min



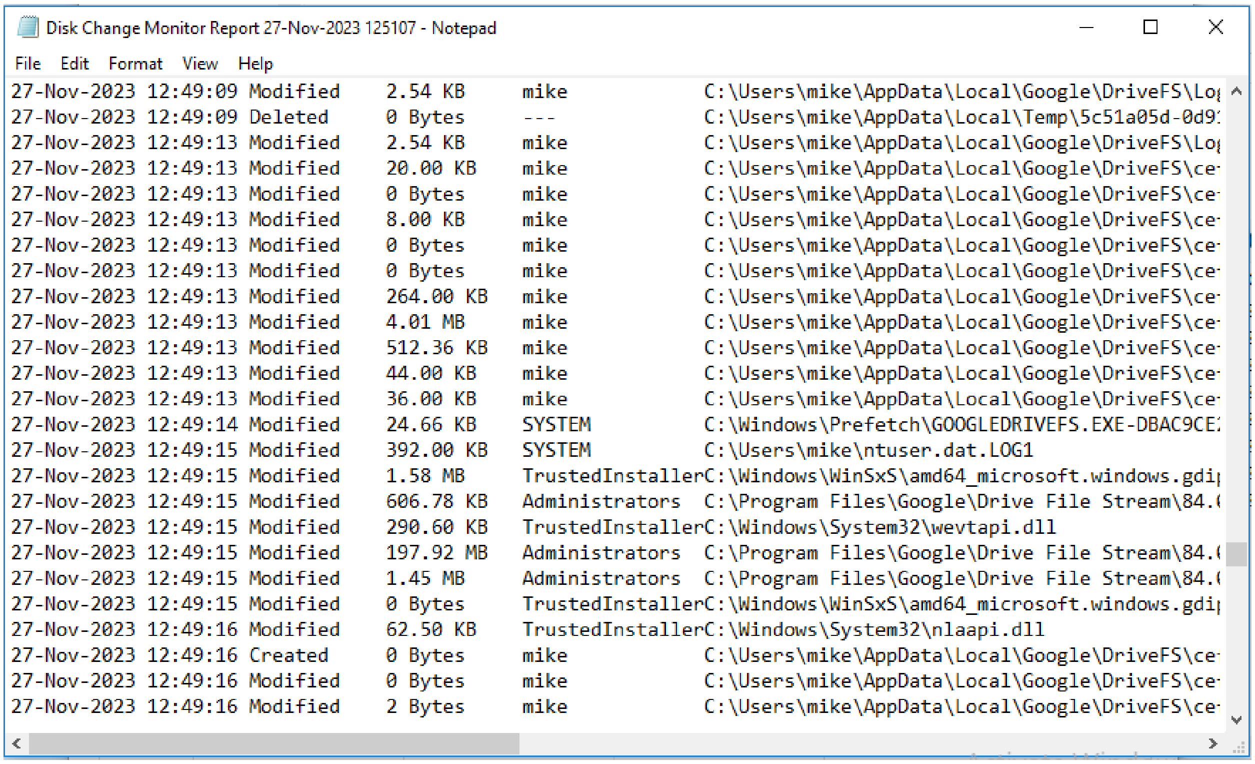
Ready

Operation Successfully Completed

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



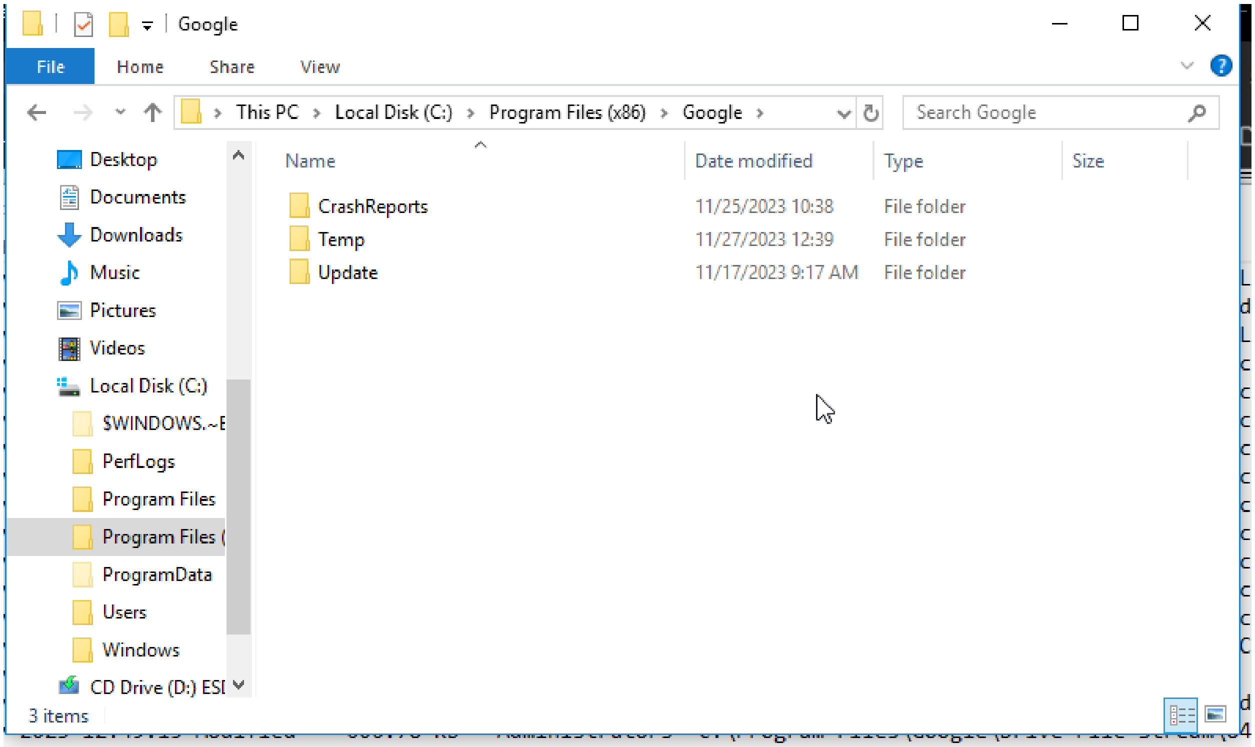
```
GENERATOR: Disk Pulse v8.7.26 - http://www.diskpulse.com
WARNING:   This report was generated by the free product version and it cannot be used for any commercial

Disk Change Monitoring Report

Summary:

Date              2023/11/27
Time              12:51:03
Host Name         windows10
Total Changes     2709
Current Changes   2000
Excluded Files    0
Change Rate       152 CH/Min
Process Time      17 Mins, 47 Secs
File Filter       Off


------------------------------------------------------------------------------------------

Top 10 File Categories

  NOEXT Files                                   31.28 MB          1122 Files     41.42 %
  TMP Files                                     1.57 MB           312 Files      11.52 %
  DLL Files                                     608.93 MB         278 Files      10.26 %
```



Disk Change Monitor Report 27-Nov-2023 125107 - Notepad
File Edit Format View Help

```
27-Nov-2023 12:49:09 Modified    2.54 KB     mike            C:\Users\mike\AppData\Local\Google\DriveFS\Log
27-Nov-2023 12:49:09 Deleted     0 Bytes     ---             C:\Users\mike\AppData\Local\Temp\5c51a05d-0d9
27-Nov-2023 12:49:13 Modified    2.54 KB     mike            C:\Users\mike\AppData\Local\Google\DriveFS\Log
27-Nov-2023 12:49:13 Modified    20.00 KB    mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:13 Modified    0 Bytes     mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:13 Modified    8.00 KB     mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:13 Modified    0 Bytes     mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:13 Modified    0 Bytes     mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:13 Modified    264.00 KB   mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:13 Modified    4.01 MB     mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:13 Modified    512.36 KB   mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:13 Modified    44.00 KB    mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:13 Modified    36.00 KB    mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:14 Modified    24.66 KB    SYSTEM          C:\Windows\Prefetch\GOOGLEDRIVEFS.EXE-DBAC9CE
27-Nov-2023 12:49:15 Modified    392.00 KB   SYSTEM          C:\Users\mike\ntuser.dat.LOG1
27-Nov-2023 12:49:15 Modified    1.58 MB     TrustedInstallerC:\Windows\WinSxS\amd64_microsoft.windows.gdi
27-Nov-2023 12:49:15 Modified    606.78 KB   Administrators  C:\Program Files\Google\Drive File Stream\84.
27-Nov-2023 12:49:15 Modified    290.60 KB   TrustedInstallerC:\Windows\System32\wevtapi.dll
27-Nov-2023 12:49:15 Modified    197.92 MB   Administrators  C:\Program Files\Google\Drive File Stream\84.
27-Nov-2023 12:49:15 Modified    1.45 MB     Administrators  C:\Program Files\Google\Drive File Stream\84.
27-Nov-2023 12:49:15 Modified    0 Bytes     TrustedInstallerC:\Windows\WinSxS\amd64_microsoft.windows.gdi
27-Nov-2023 12:49:16 Modified    62.50 KB    TrustedInstallerC:\Windows\System32\nlaapi.dll
27-Nov-2023 12:49:16 Created     0 Bytes     mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:16 Modified    0 Bytes     mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
27-Nov-2023 12:49:16 Modified    2 Bytes     mike            C:\Users\mike\AppData\Local\Google\DriveFS\ce
```

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



Name	Date modified	Type	Size
CrashReports	11/25/2023 10:38	File folder	
Temp	11/27/2023 12:39	File folder	
Update	11/17/2023 9:17 AM	File folder	