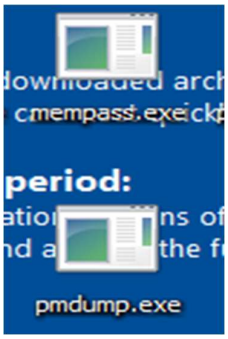
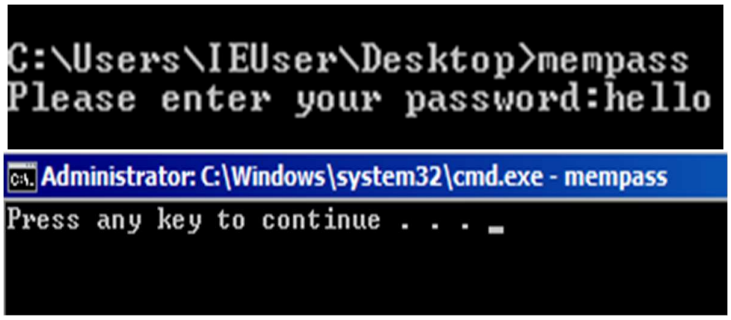
PRACTICAL NO. 06

Dump Memory contents using PMdump

1. Here we will use program name mempass, and we will see how by using combination of pmdump and strings, we are able to dump the password in memory.

Let start the mempass





2. Now open new terminal and run PMdump, pmdump –list will list the running program currently.

```
C:\Users\IEUser\Desktop>pmdump

pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
             - http://ntsecurity.nu/toolbox/pmdump/

Usage:  pmdump (pid) (filename)

          - dumps the process memory contents to a file

        pmdump -list

          - lists all running processes and their PID's
```

```
C:\Users\IEUser\Desktop>pmdump -list

pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
             - http://ntsecurity.nu/toolbox/pmdump/

    0 - System idle process
    4 - System
  252 - smss.exe
  328 - csrss.exe
  364 - csrss.exe
  372 - wininit.exe
  400 - winlogon.exe
  460 - services.exe
  468 - lsass.exe
  476 - lsm.exe
  568 - svchost.exe
  624 - VBoxService.exe
  676 - svchost.exe
  780 - svchost.exe
  820 - svchost.exe
  848 - svchost.exe
  872 - svchost.exe
  996 - svchost.exe
 1148 - svchost.exe
 1256 - spoolsv.exe
 1292 - svchost.exe
 1384 - svchost.exe
 1424 - svchost.exe
 1584 - cygrunsrv.exe
 1660 - wlms.exe
 1696 - conhost.exe
 1720 - sshd.exe
 1932 - sppsvc.exe
  296 - svchost.exe
 1520 - taskhost.exe
 2280 - GoogleCrashHandler.exe
 2596 - svchost.exe
 2708 - SearchIndexer.exe
 2928 - dwm.exe
 2956 - explorer.exe
 3096 - VBoxTray.exe
 3560 - wuauclt.exe
 3104 - cmd.exe
 2700 - conhost.exe
 3808 - cmd.exe
 1992 - conhost.exe
```

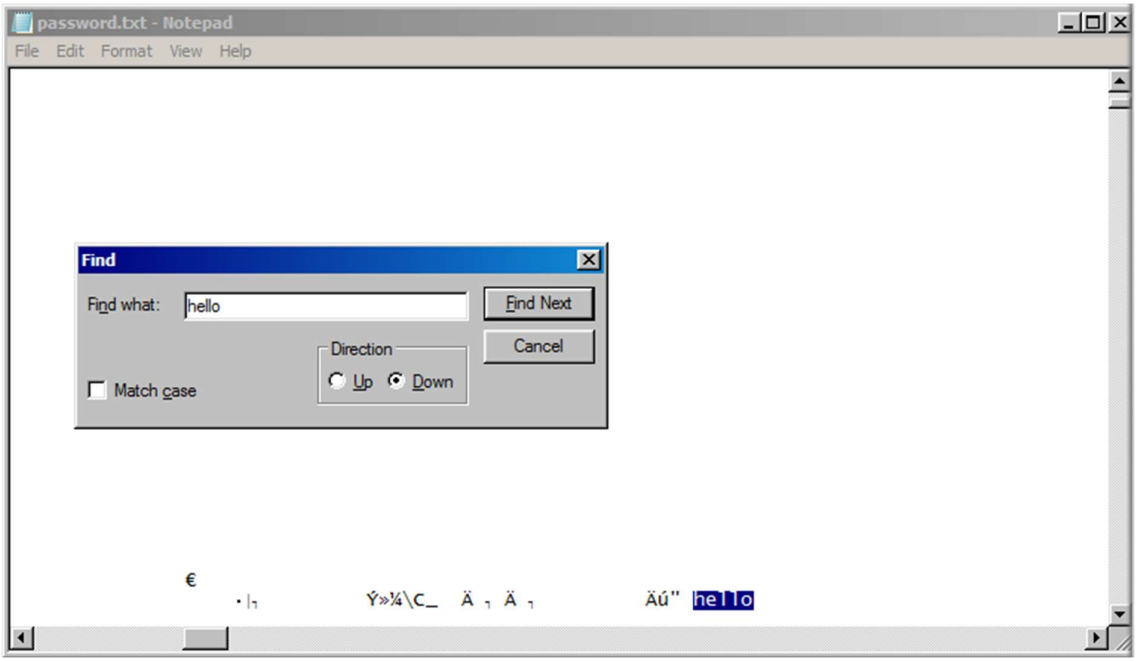
```
2076  - taskeng.exe
3456  - mempass.exe
 976  - cmd.exe
2120  - pmdump.exe

C:\Users\IEUser\Desktop>mempass 3456 paswd.txt
```

3. Here we can see the pid of mempass i.e., 3456. We will dump the entire memory of mempass program in paswd.txt file

```
C:\Users\IEUser\Desktop>mempass 3456 paswd.txt
Please enter your password:hello_
```

4. File name paswd is created having direct memory of mempass program without tampering the running mempass program

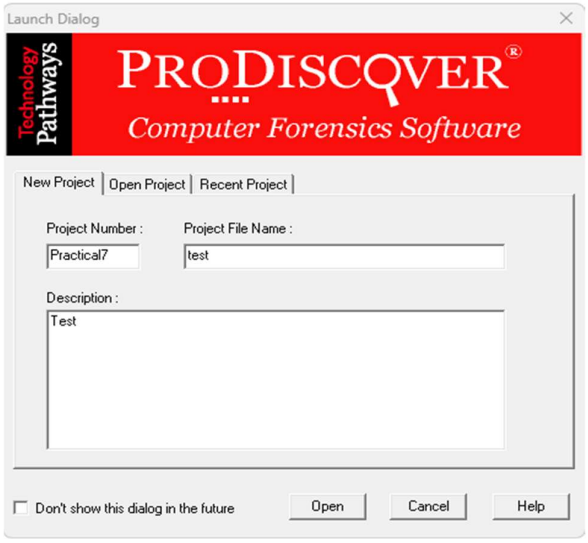


In this way, we can retrieve passwords from applications which store them in memory without any form of encryption.

PRACTICAL NO. 07

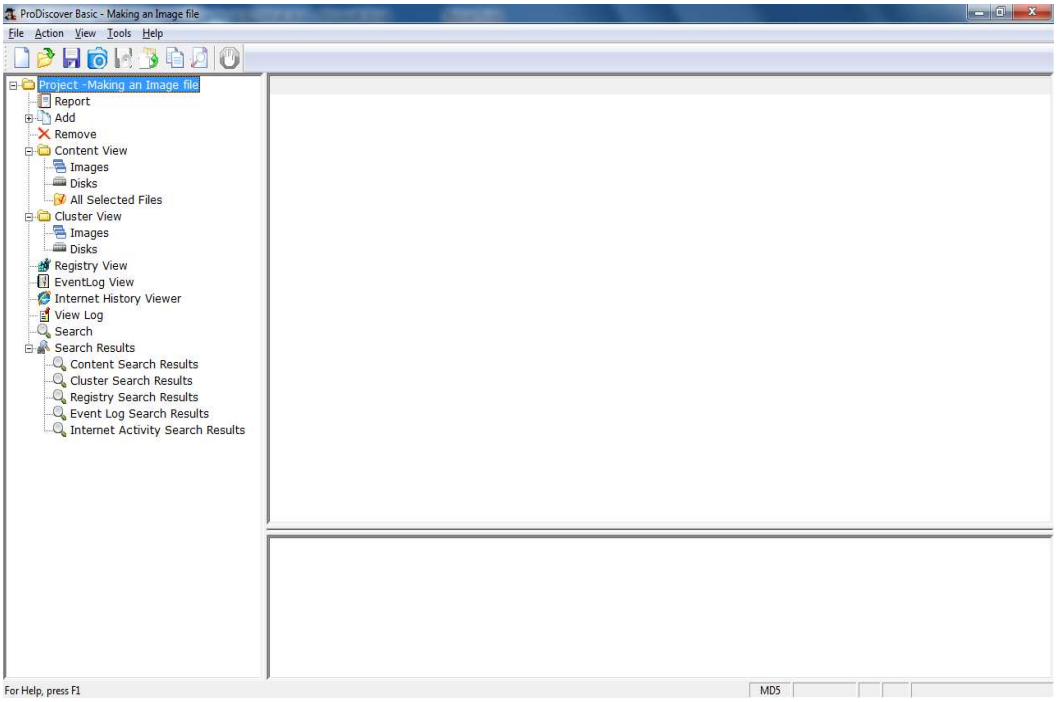
Using Data Acquisition Tools [ProDiscover Pro]

Step 1) Start ProDiscover. ProDiscover presents the launch dialog.



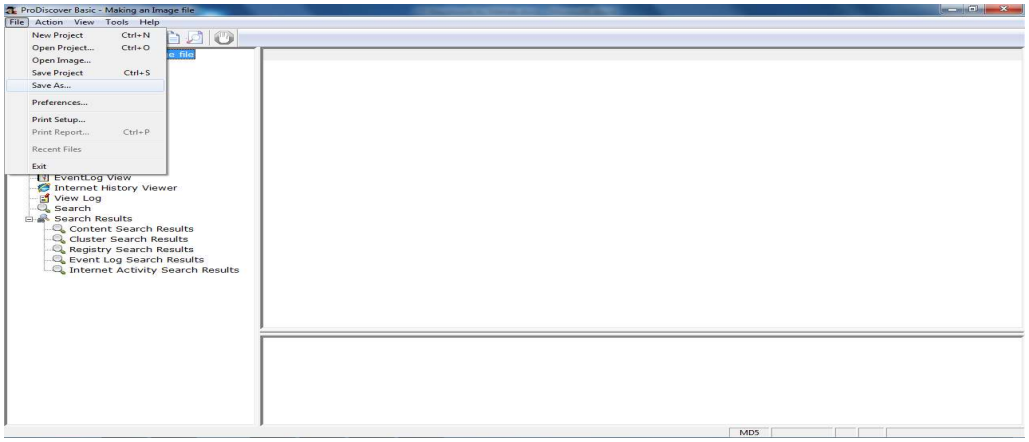
Step 2) Enter a project number, project name, and description of the project in the new project tab
option, and then click the Open button.

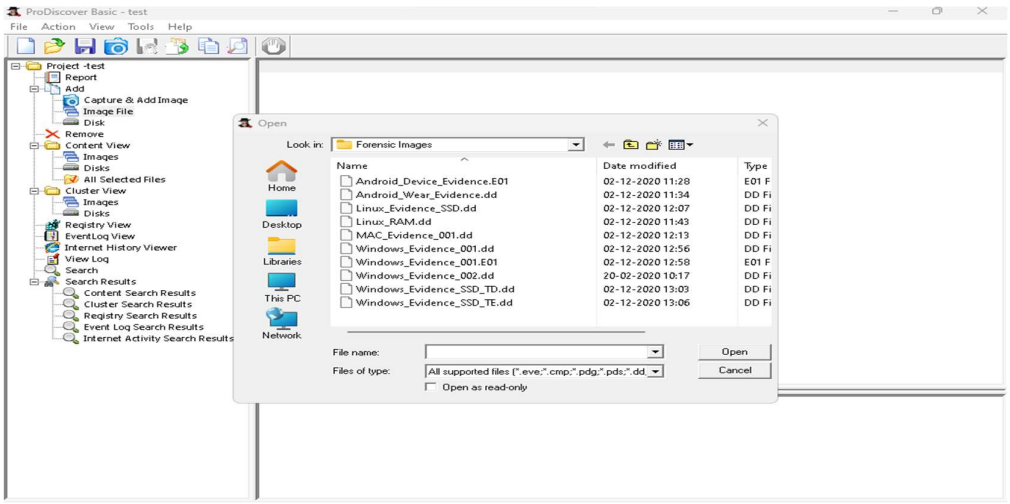
ProDiscover will then create a project and generate a template report in the work area.

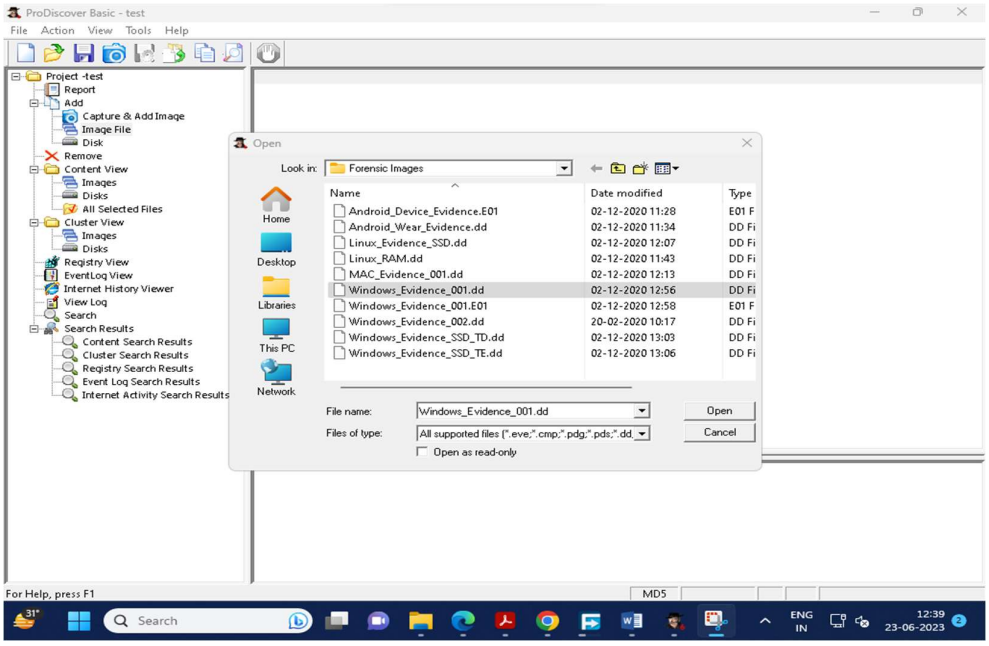


Step 3) Open Image:

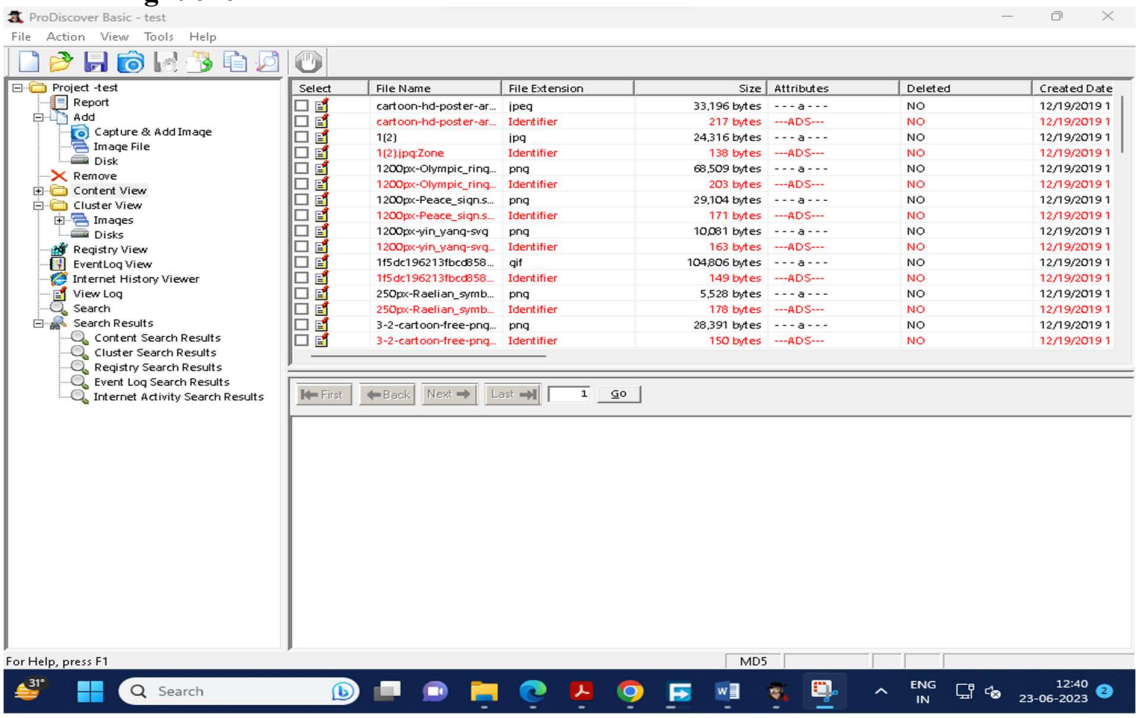
1] Select save project option from the file menu, or button bar and Open Image option.



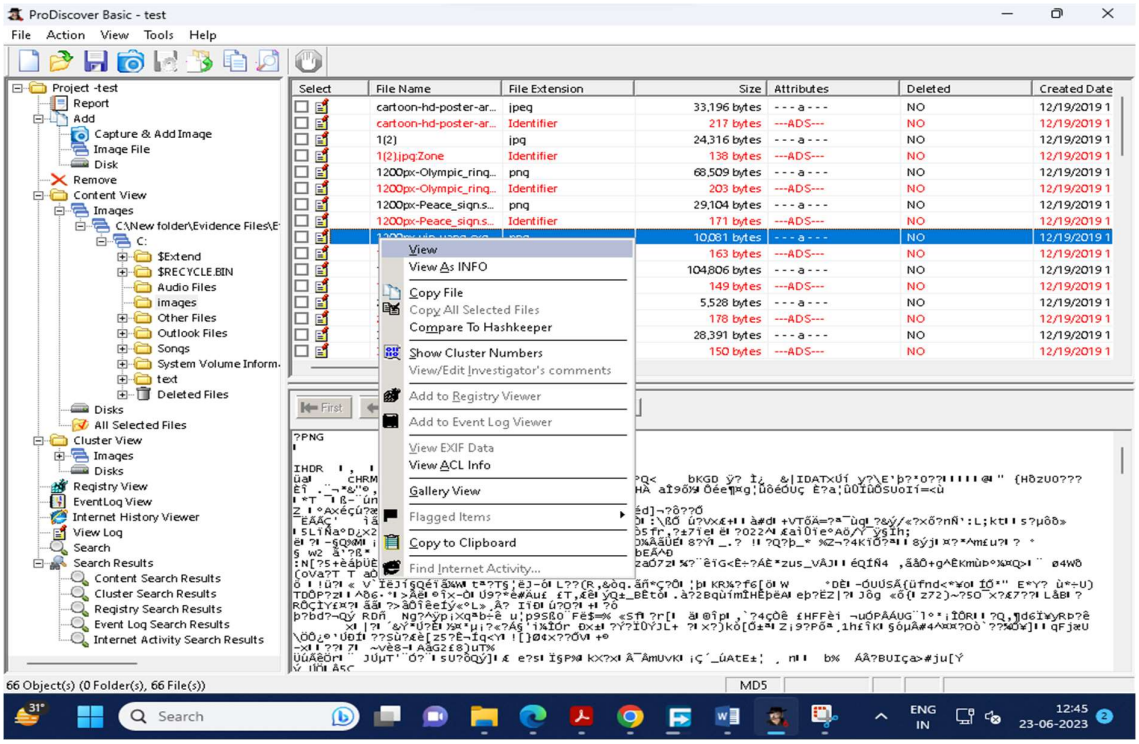




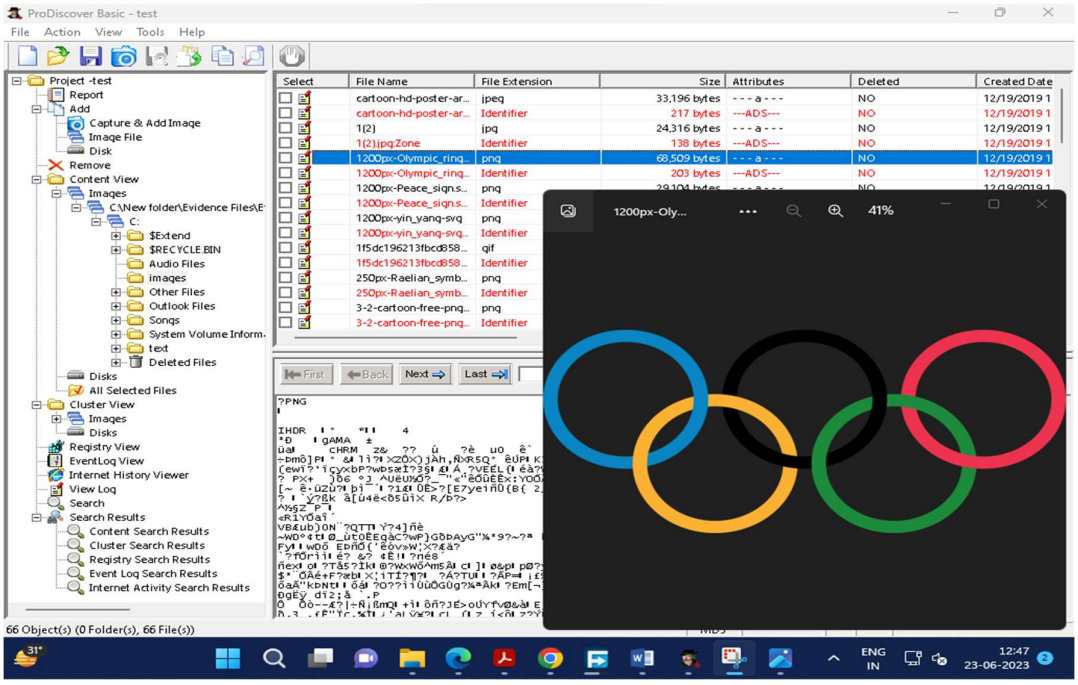
Step 4) ProDiscover displays the contents of the selected file at the bottom of the main window. **Right click** on a file.



Step 5) In ProDiscover a pop-up dialog with the choice to View or Recover the selected file. Select **View**



Step 6)For further study, we can also copy the file at desired location

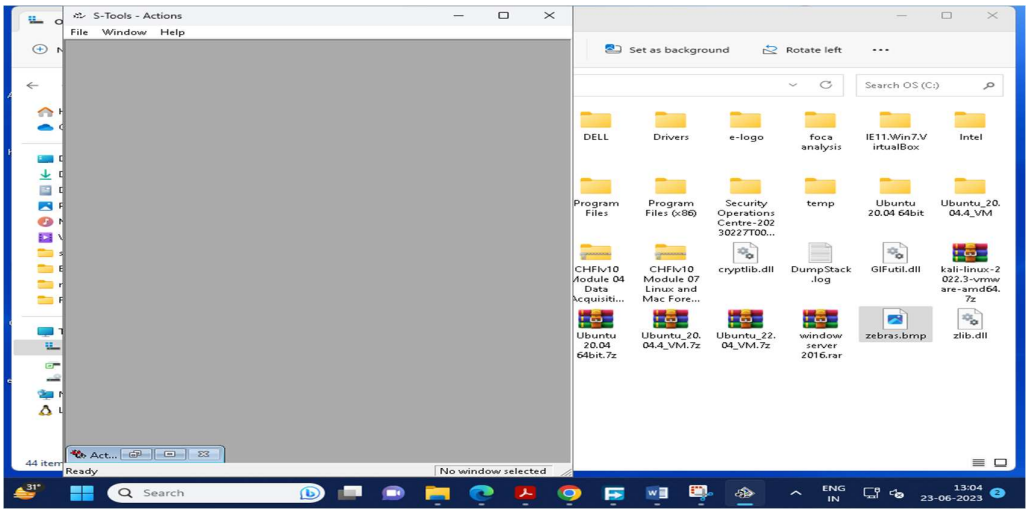


PRACTICAL NO. 08

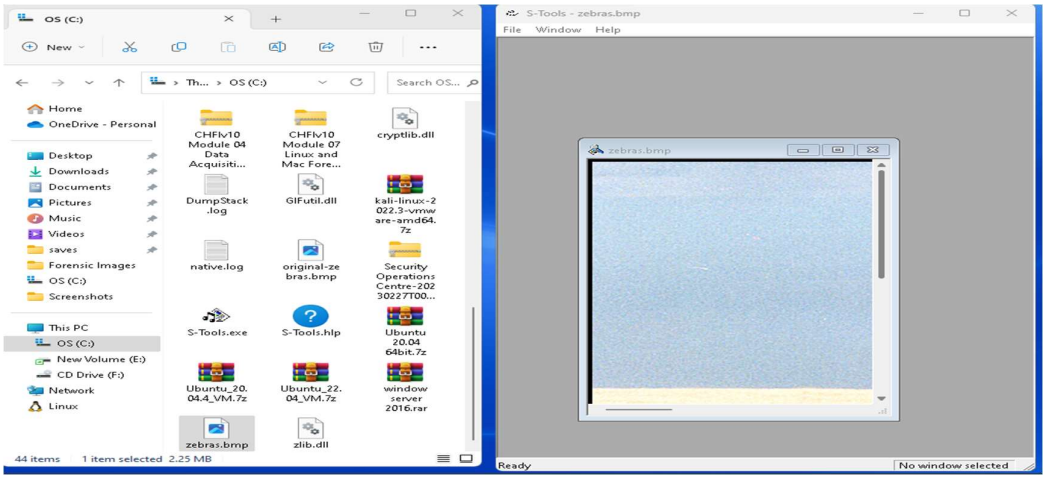
a. Using Steganography Tools [S-Tools]

Following steps Show how to use freeware S-Tools utility to hide and reveal files inside pictures

Step 1) Select the S-Tools.exe file and open the steganography software tool.



Step 2) With both the working directory and the S-Tools program open minimize both windows and place side-by-side.



The S-Tools program is a drag and drop software. The files used to create the steganography file can be dragged from the directory into the S-Tools program.

Step 3) Select the file from the directory and drag it over the S-Tools main window and release the
file.

A dialogue box appears indicating that the file type is unknown. Supported file types for audio and image files are shown below:

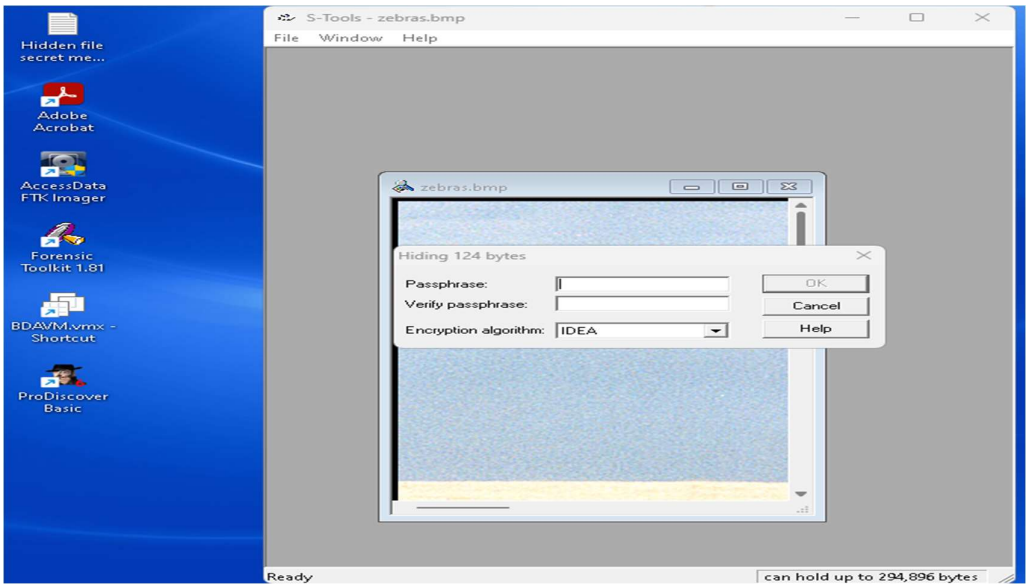
- Audio - *.wav
- Image - *.bmp and *.gif

If your image is in .jpg format, convert it to .bmp format.

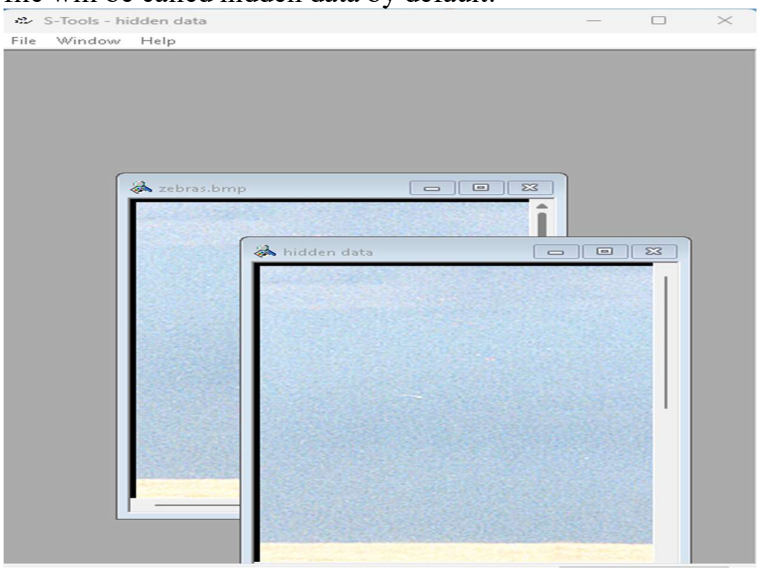
Step 4) Select a file to hide within the base file. If it's not there, create a txt file and save the file. Here we have created file name Hidden file
Step 5) The *.txt text file is selected and dragged on top of the base image. Release the file while the cursor is still on top of the base file.

Step 6) A dialogue box will appear asking the user to enter and verify a passphrase. Additionally, the user will have to select an encryption algorithm.

Step 7) Select the 'OK' button after entering a valid passphrase.



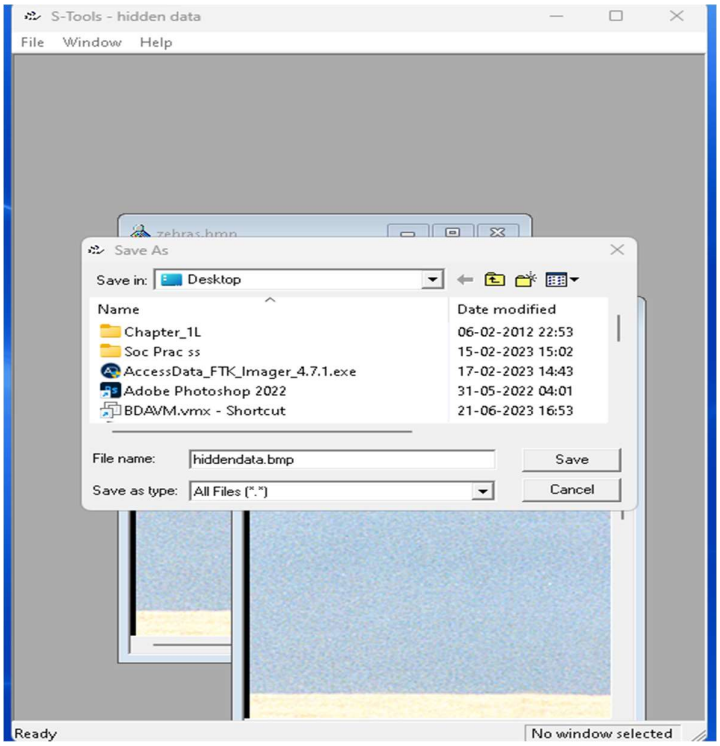
Step 8) The S-Tools main window will appear and a new file will be visible. The name of the file will be called hidden data by default.



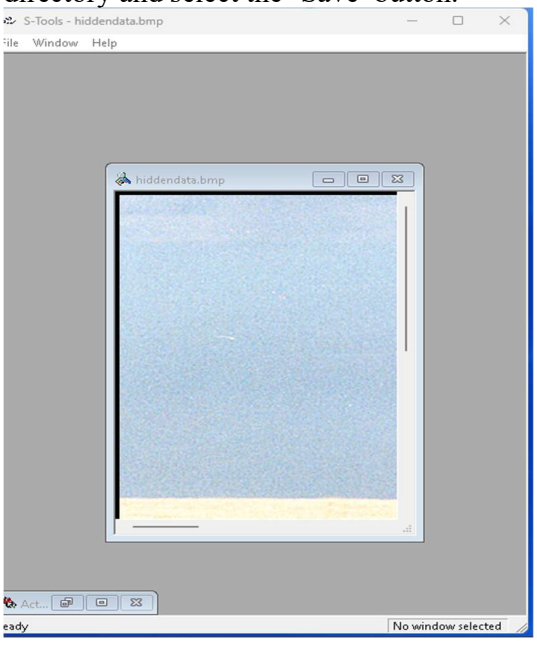
Step 9) Place the cursor on top of the hidden data image and select the right mouse button. The user will
have four options available to them:

- Save
- Save As
- Properties
- Reveal

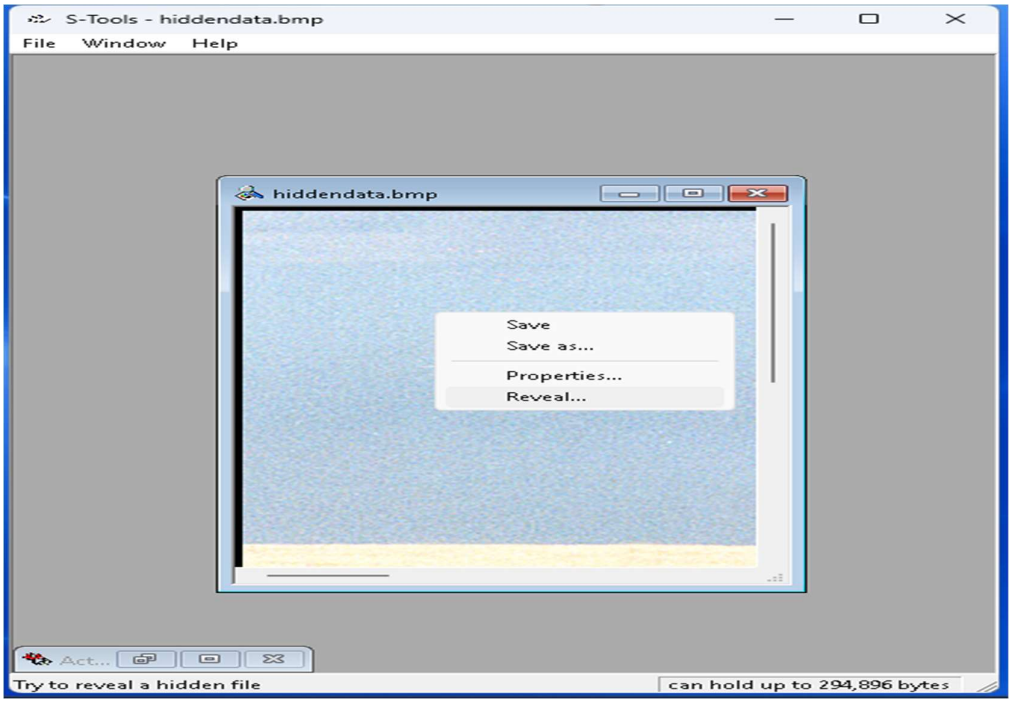
Select the ‘Save As’ button.



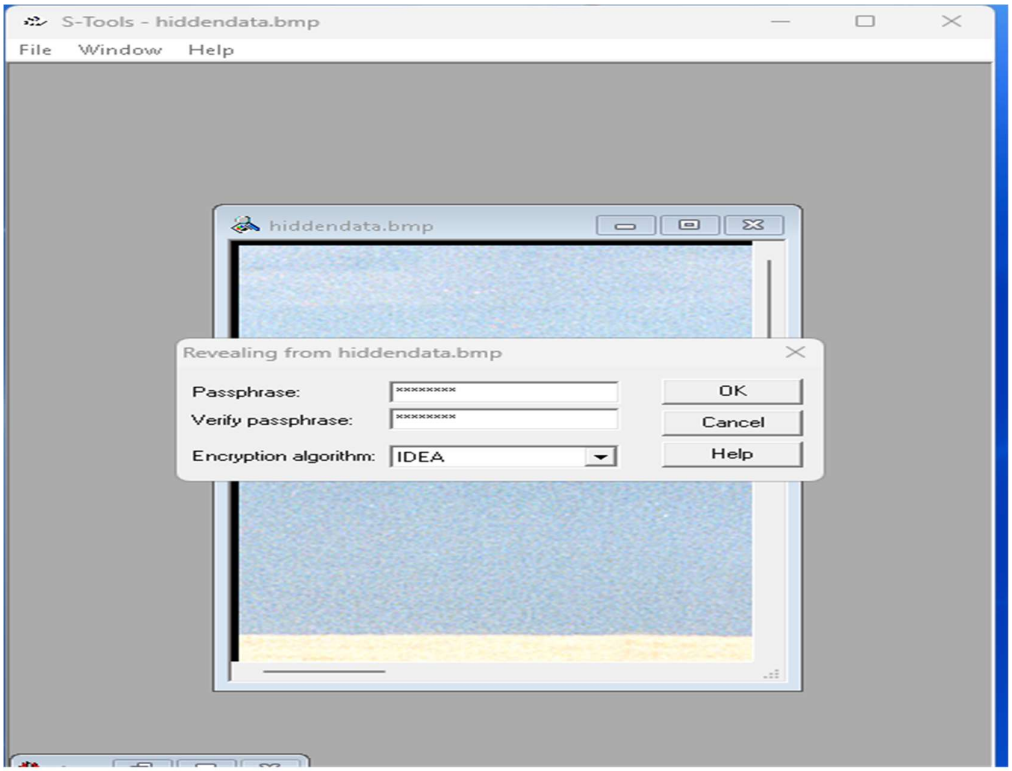
Step 10) A ‘Save As’ dialogue box will appear. Enter a valid file name, select the working directory and select the ‘Save’ button.



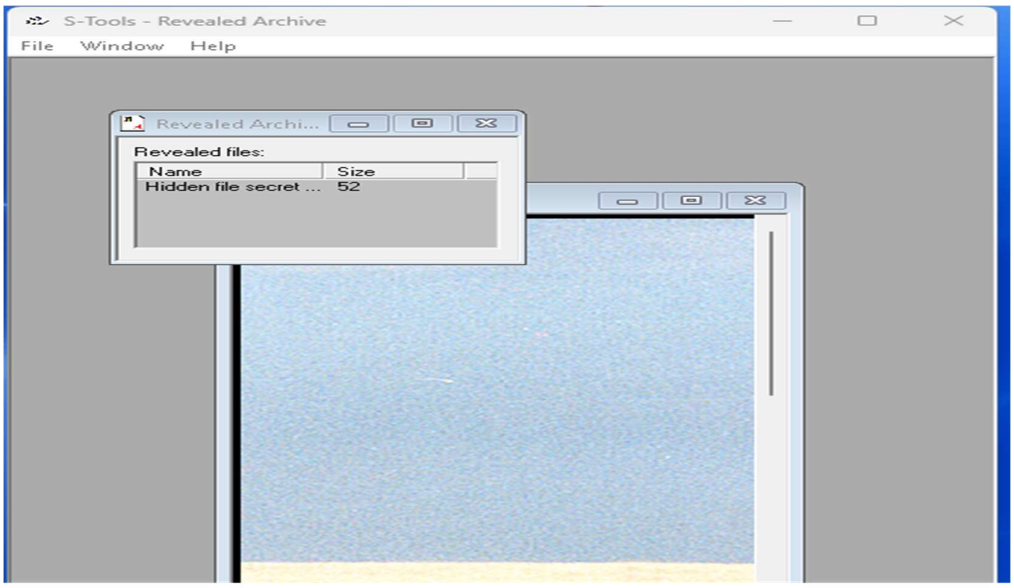
Step 11) Selecting the ‘Reveal’ button will display a passphrase dialogue box. A passphrase must be entered twice in the dialogue box and the correct encryption algorithm must be selected.



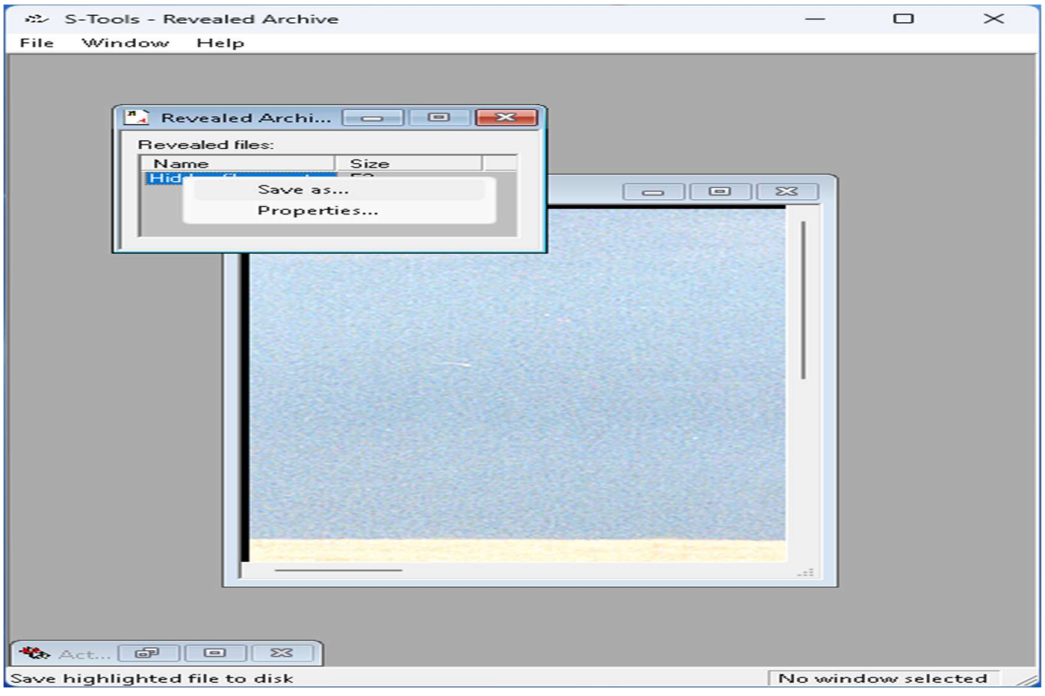
Step 12) Enter a passphrase twice, select the encryption algorithm, and select the ‘OK’ button.



Step 13) A ‘Revealed Archive’ dialogue box will display which contains the file name and size of the hidden file.



Step 14) Select the ‘Save As’ button.



Step 15) The Revealed data is saved in revealfile.txt