D. B. J. COLLEGE, CHIPLUN

Page No. : _____

DEPARTMENT OF COMPUTER SCIENCE

Expt. No.

Name : Piyush Pandurang Burate Class : TYCS Roll No.: 523

Title of Experiment : Data Acquisition

Date

Sub titles : Assignment/ Problem Solution, Flow chart/Algorithm, Problem Listing, Input Screen, Output Screen, Comments (If any)

Aim :- To study about Acquisition :-

- Perform data acquisition using
- USB write blocker + encase imager
- SATA write blocker + encase imager
- Falcon imaging device.

Software / Hardware Requirements :-

FTK imager, regedit printer.

Theory :-

Data acquisition is the process of making a forensics image from computer media such as hard drive, thumb drives, servers and other media that stores electronic data including gaming console and other devices.

The forensic image, not the original media, is used by the forensic examiner to conduct the examination.

The data acquisition process includes the recording of all serial numbers and other marking using a digital camera.

Remark

The forensic image is verified against the original to ensure the forensic image is an exact duplicate of the original media.

Signature

Creating Forensic imager using S/W and H/W write blocker.

Both S/W and H/W write blockers are available software write blockers are versatile and come in two flavours. One is module that 'Plugs' ~~in to~~ into the Forensic S/W ~~dot~~ and can generally be used to write block any port on the computer. The other method of software write blocking is to use a forensic boot disk. This will boot the computer system from the HD. Developing checklists that can be repeatable procedure is an ideal way to ensure solid result in any investigation.

Conclusion :-

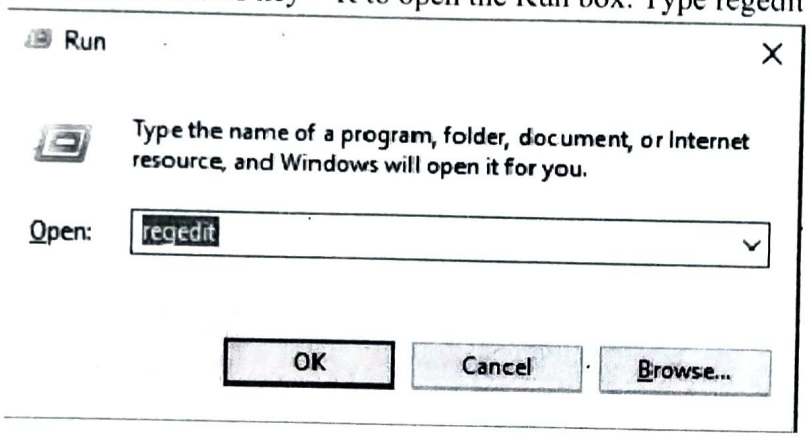
By using FTK imager we perform data acquisition.

Practical 2: Data Acquisition:

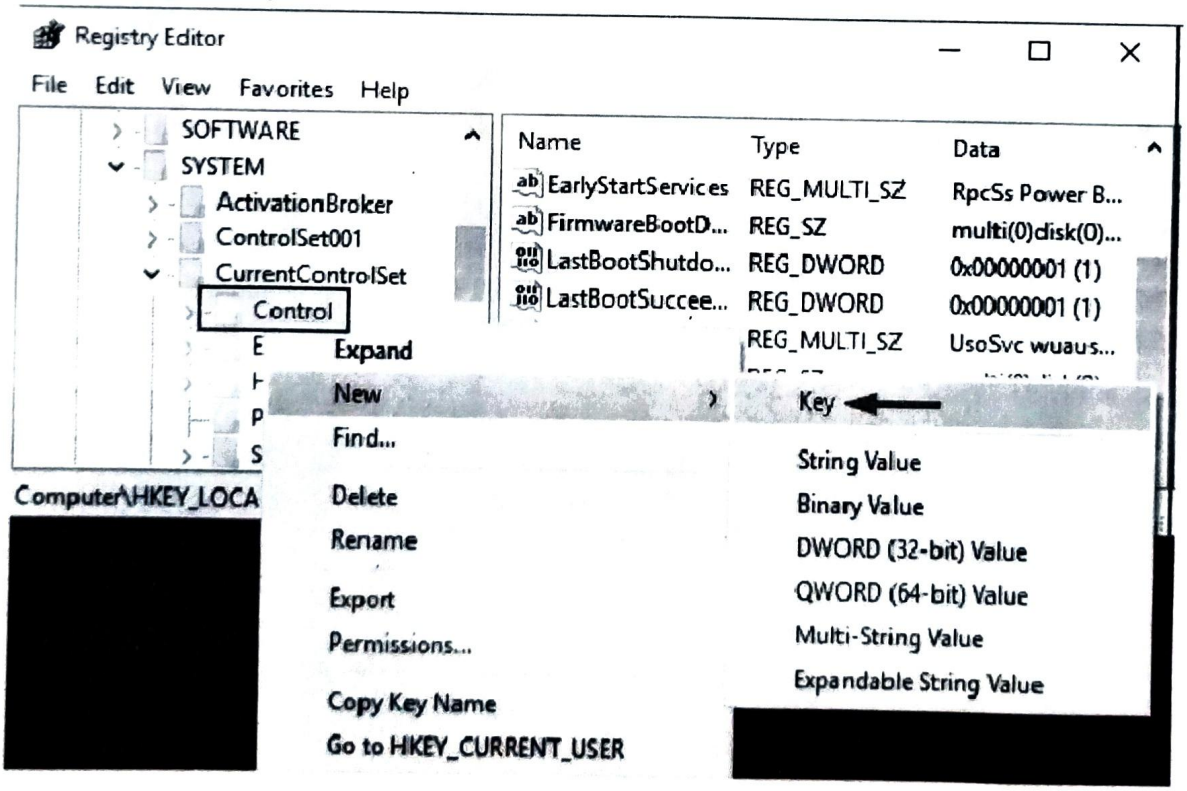
Steps:

Enable USB Write Block in Windows 10, 8 and 7 using registry

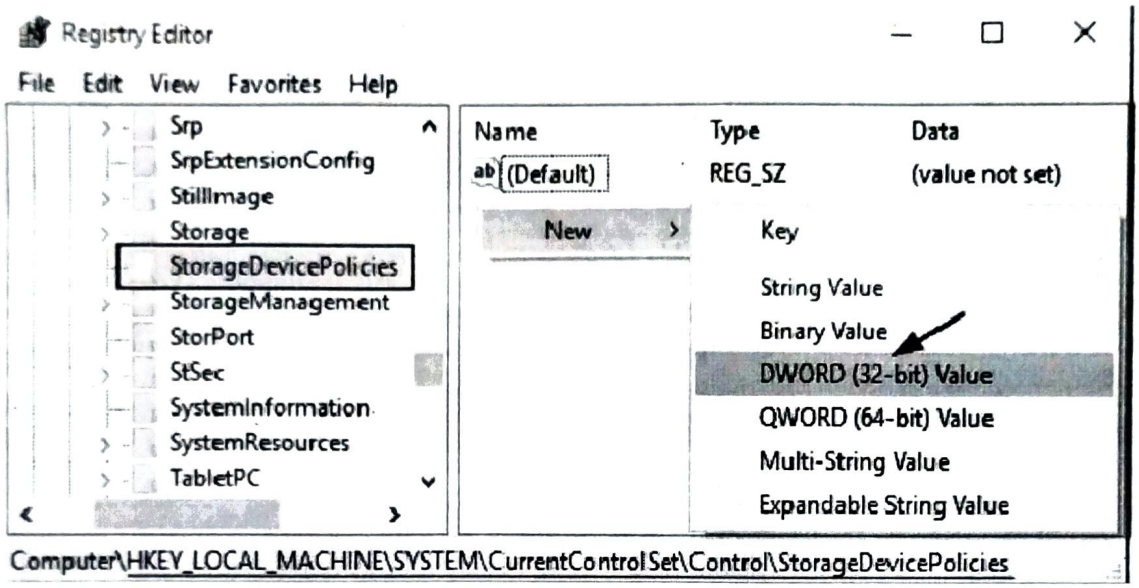
1. Press the Windows key + R to open the Run box. Type regedit and press Enter.



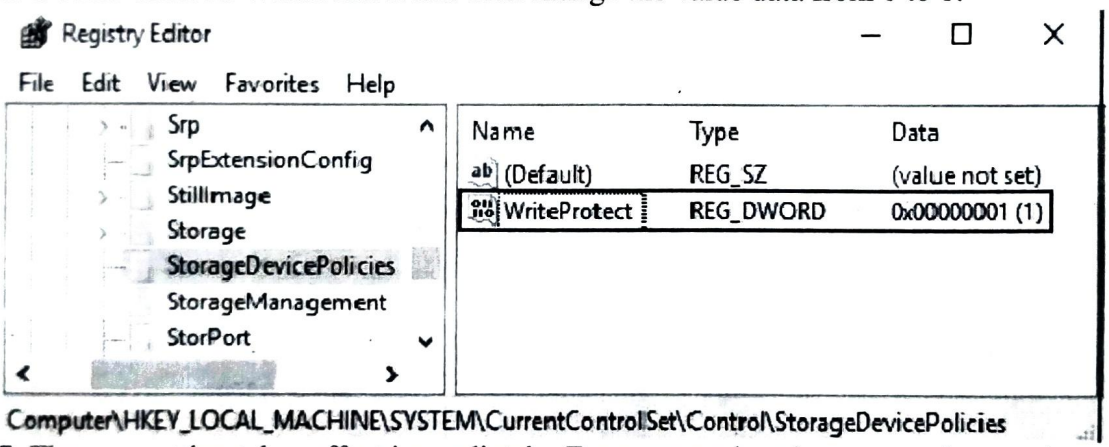
2. This will open the Registry Editor. Navigate to the following key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
3. Right-click on the Control key in the left pane, select New -> Key.
4. Name it as StorageDevicePolicies.



5. Select the StorageDevicePolicies key in the left pane, then right-click on any empty space in the right pane and select New -> DWORD (32-bit) Value. Name it WriteProtect.



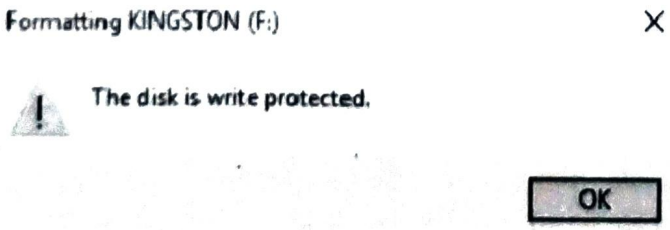
6. Double-click on WriteProtect and then change the value data from 0 to 1.



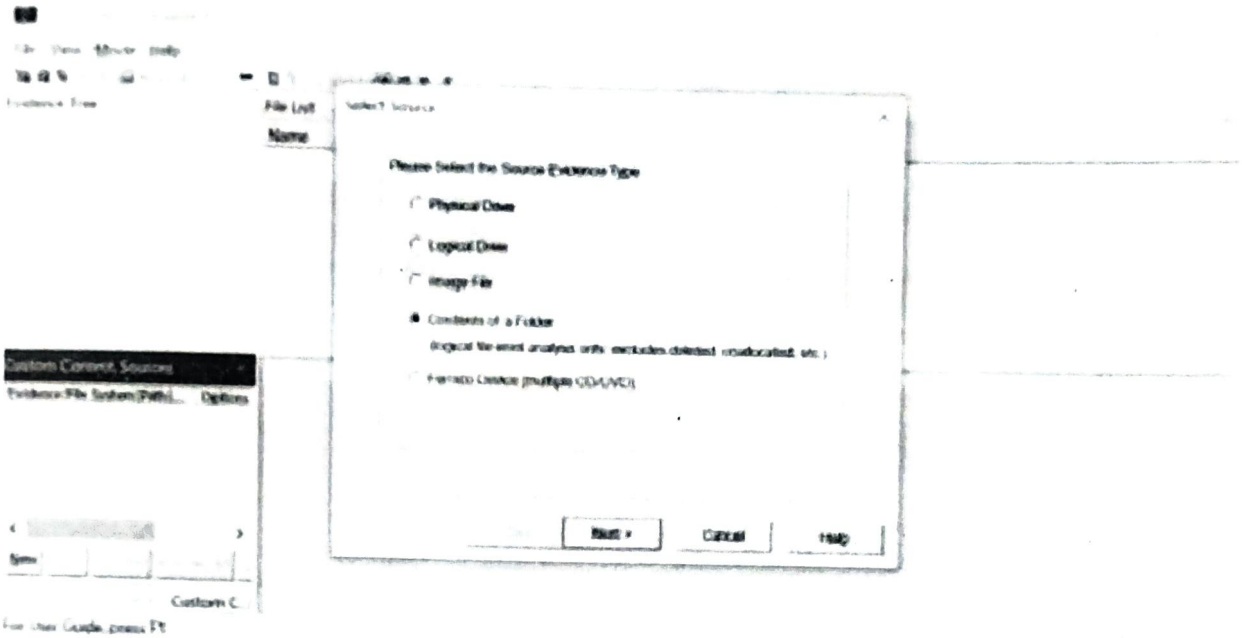
7. The new setting takes effect immediately. Every user who tries to copy / move data to USB devices or format USB drive will get the error message "*The disk is write-protected*".

8. We can only open the file in the USB drive for reading, but it's not allowed to modify and save the changes back to USB drive.

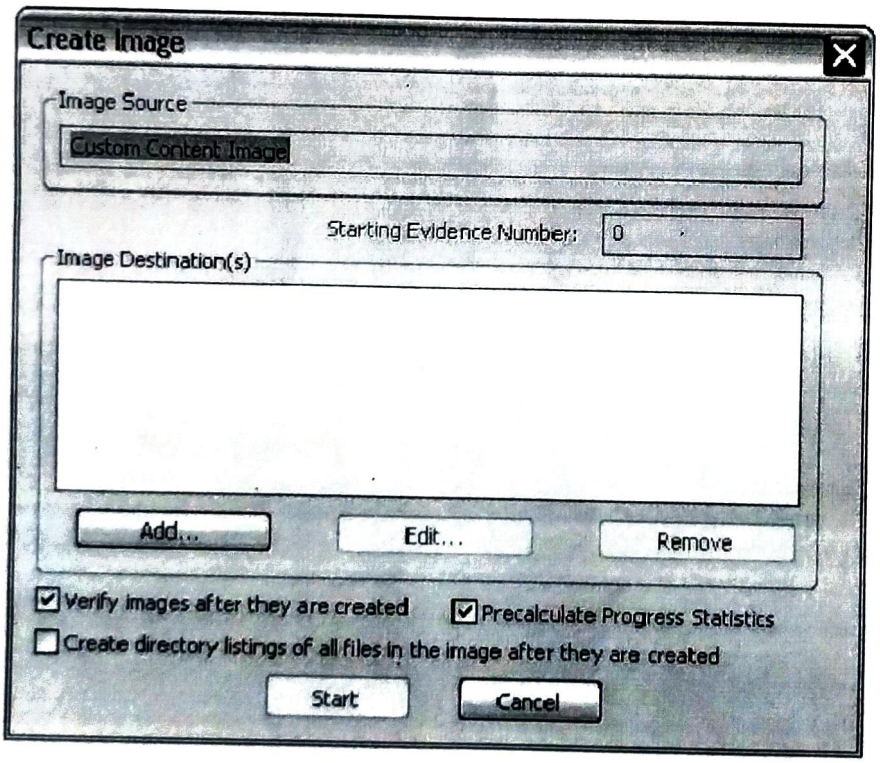
So this is how you can enable write protection to all connected USB drives. If you want to disable write protection at a later time, just open Registry Editor and set the WriteProtect value to 0.

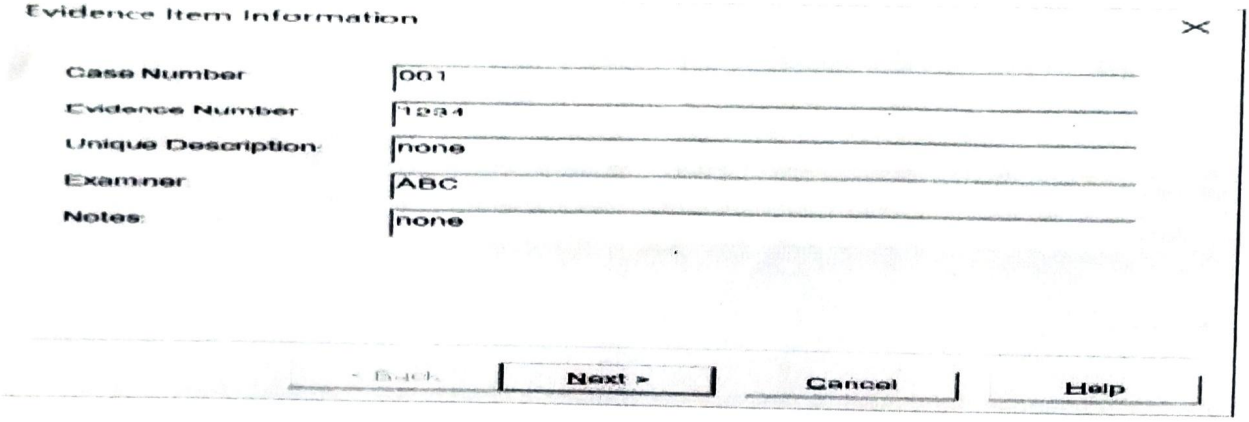


9. Now Create image of the USB drive using FTK imager



10. Select the USB drive folder by browsing and click next & Finish
11.In the Create Image dialog, click Add.





Select the type of image you want to create, and then click Next