**Forensic Report:**

**Disk to Image Acquisition of a USB Pendrive(FAT 16 Format)**

Assignment Submitted By:

**Shanti Kumar Deepak**

**Roll No - 18704**

**Scope of Work**

Create a disk to image of a 1GB USB drive. This USB is suspected to use for exploiting a system and compromising the organization’s sensitive information. The purpose for creating an image is to analyze all the files in this USB drive. The Software based write blocker is being used to make the device write blocked while capturing the image.

**Abstract**

In a reputed Organization, there is an incident of sensitive data leak. A system in the Finance Department office containing sensitive information was compromised using this USB. Investigation purpose is to identify all the leaked files and/or the malicious code (if any) present in the USB for this incidence by gathering and analyzing all the files, folders and other information available on this USB drive.

**Acquisition Details**

To acquire disk to image for the suspected USB drive we are using **EnCase v7.09.02** tool by the Guidance Software. The result is an image file(s) that can be saved in several formats, including **.E01**, **.Ex01**. The acquired data includes:

* **All the files available on the media**
* **Unallocated Space**
* **Removed or Deleted Files if not overwritten**

We will then analyze the acquired data using FTK Manager. We also calculate the hash of each file at the end of this process.

**Chain of Custody**

**CASE NO:** C18704

|  |  |  |
| --- | --- | --- |
| **DESCRIPTION OF EVIDENCE** | | |
| **DEVICE TYPE** | **DEVICE NAME** | **STATE** |
| USB | USB1 GB | Okay |

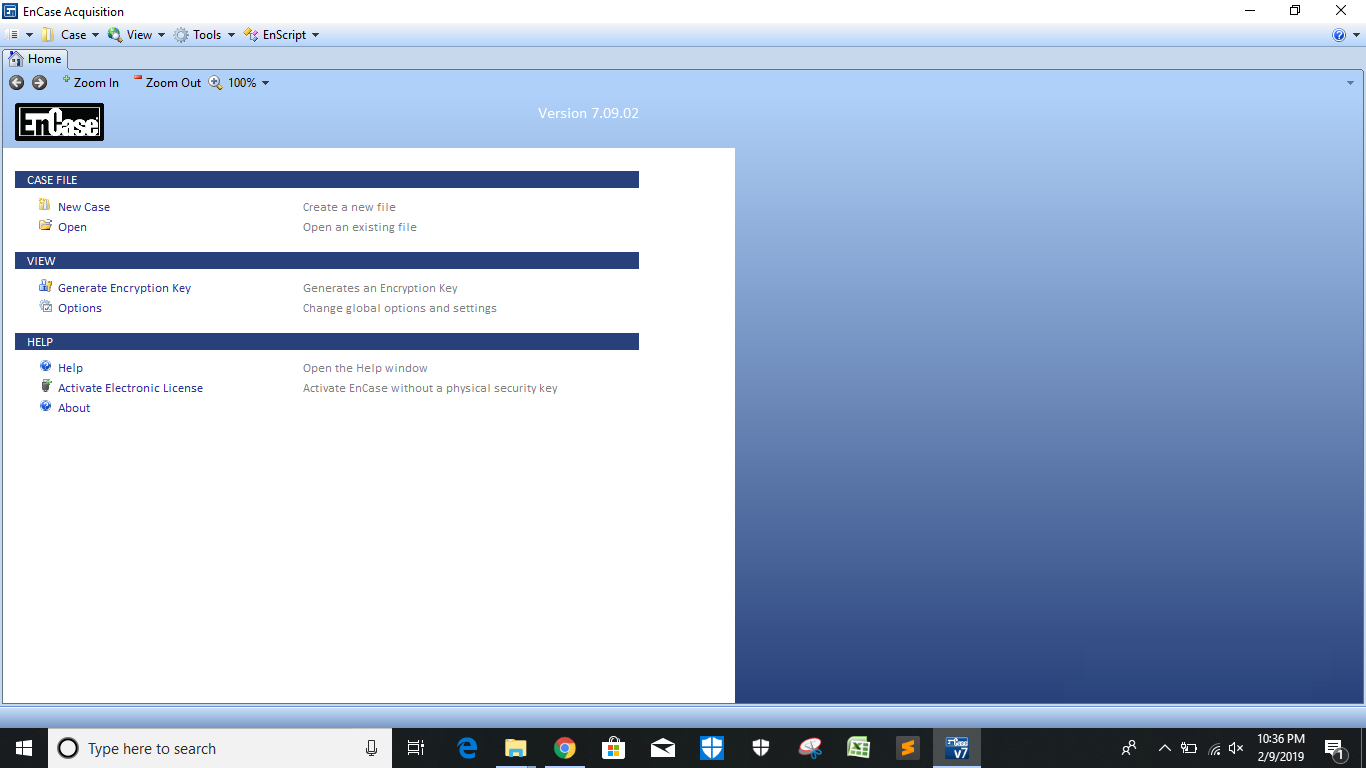
|  |  |  |
| --- | --- | --- |
| **DESCRIPTION OF DEVICE** | | |
| **LABEL#** | **MANUFACTURER** | **CAPACITY** |
| 1 | Custom | 1 GB |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Chain of Custody** | | | | |
| **LABEL #** | **Date/Time** | **Releasedby** (ID#) | **Received by** (ID#) | **Comments/Location** |
| 1 | 10-2-2019  2:05 PM | Deepak  18714 | Pascal  Sr. IO | At Technodata  Office, Delhi |

**Mode of Operation**

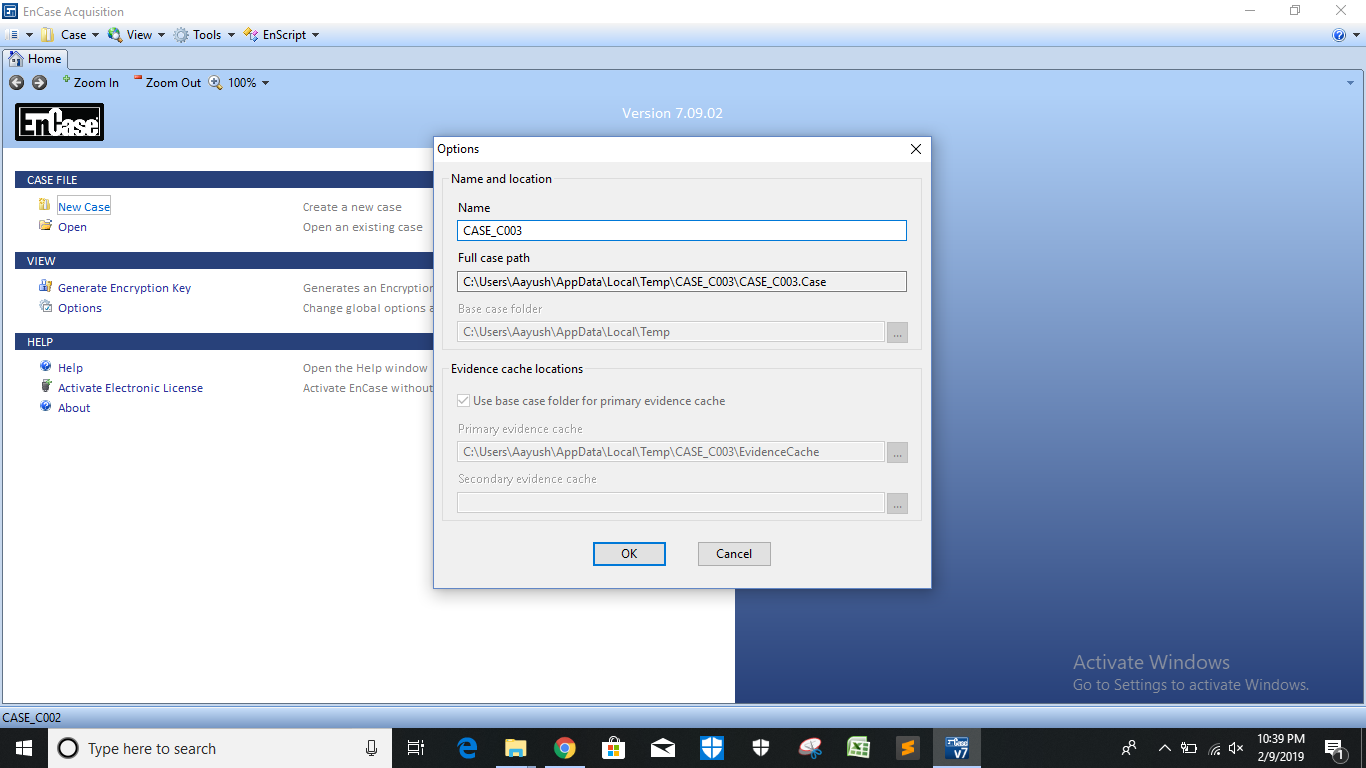
Investigator followed the SOP defined, and stayed compliant to the policies followed by Data Owner Institute. Following are the steps underwent:

**Step 1**: Launch EnCase Acquisition Tool on the workstation the investigator’s machine.

****

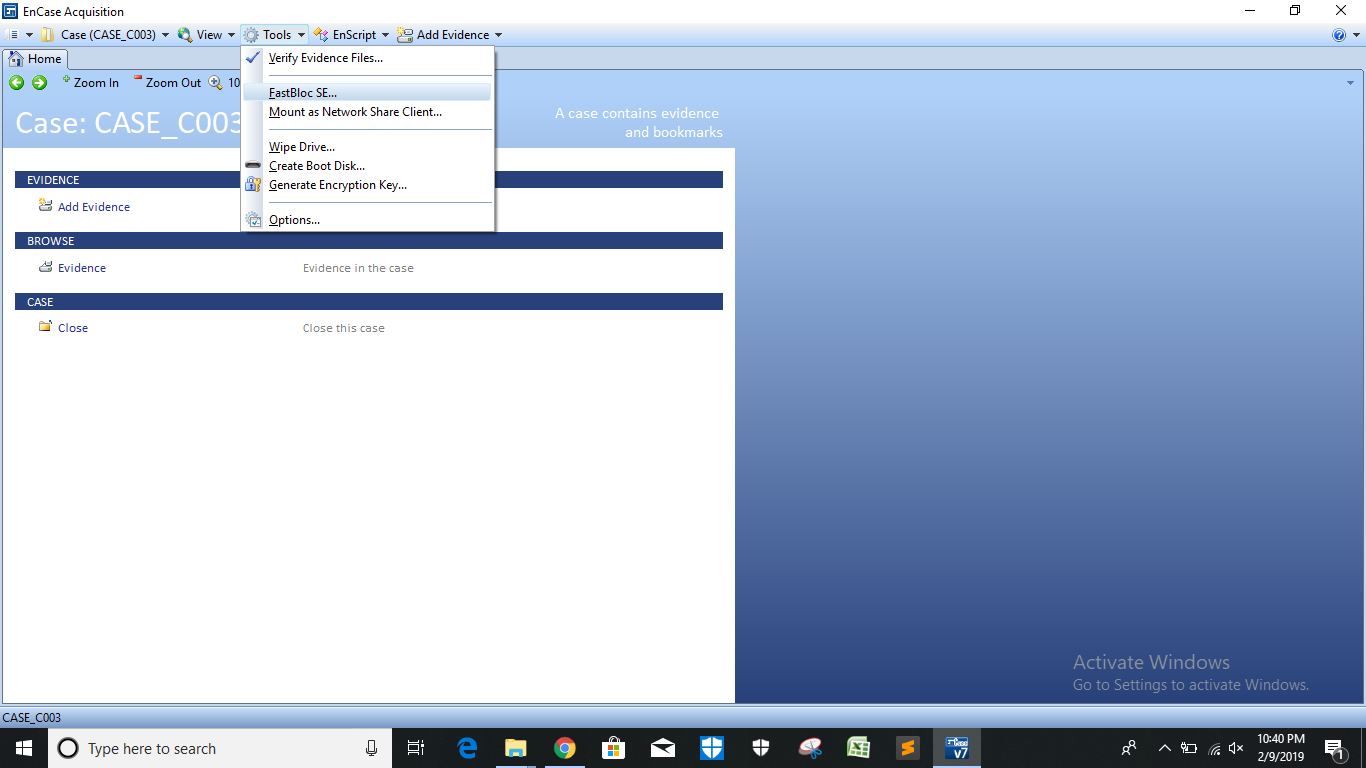
***Fig-1: Launch EnCase Acquisition***

**Step 2**: Create a new Case **Case\_C003:**

****

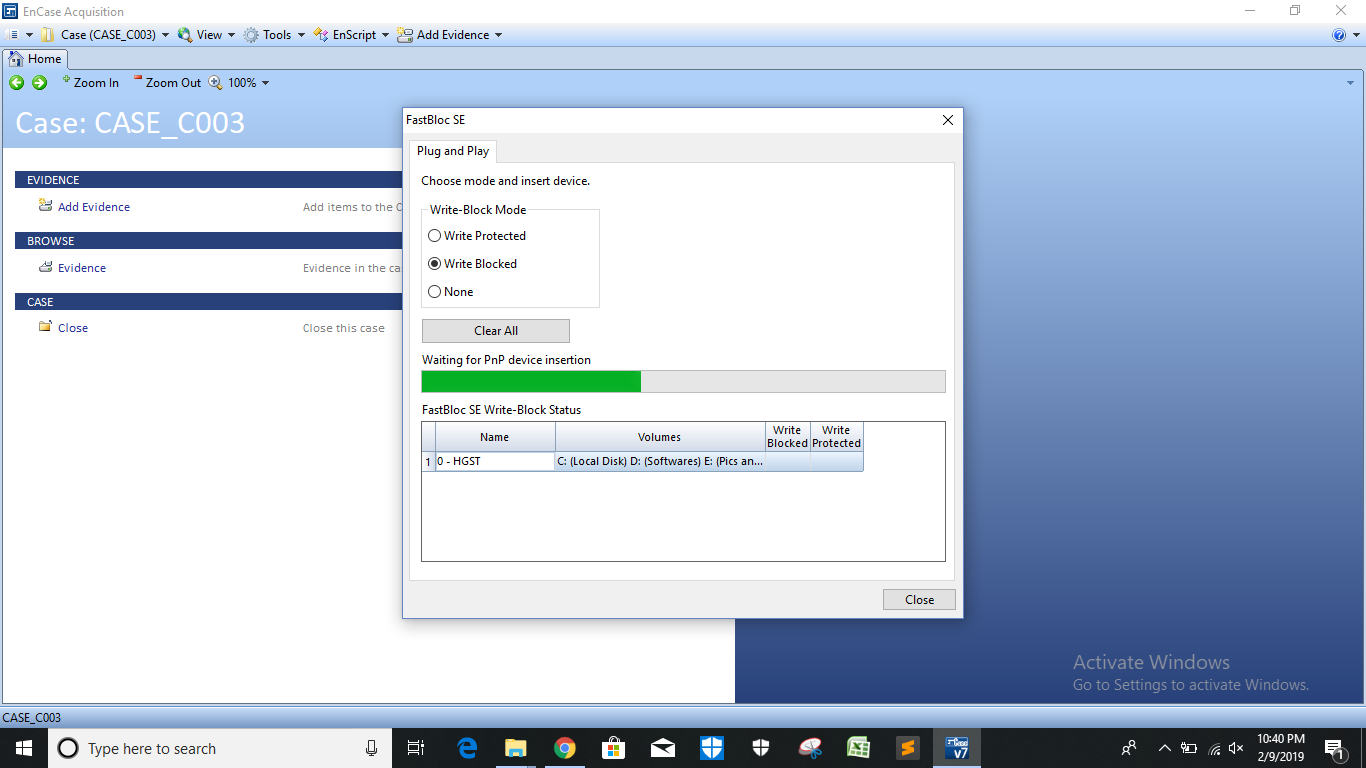
***Fig-2: Create a new Case***

**Step 3**: Enable Software based write blocker **FastBlock SE** from **tools** option as shown below:



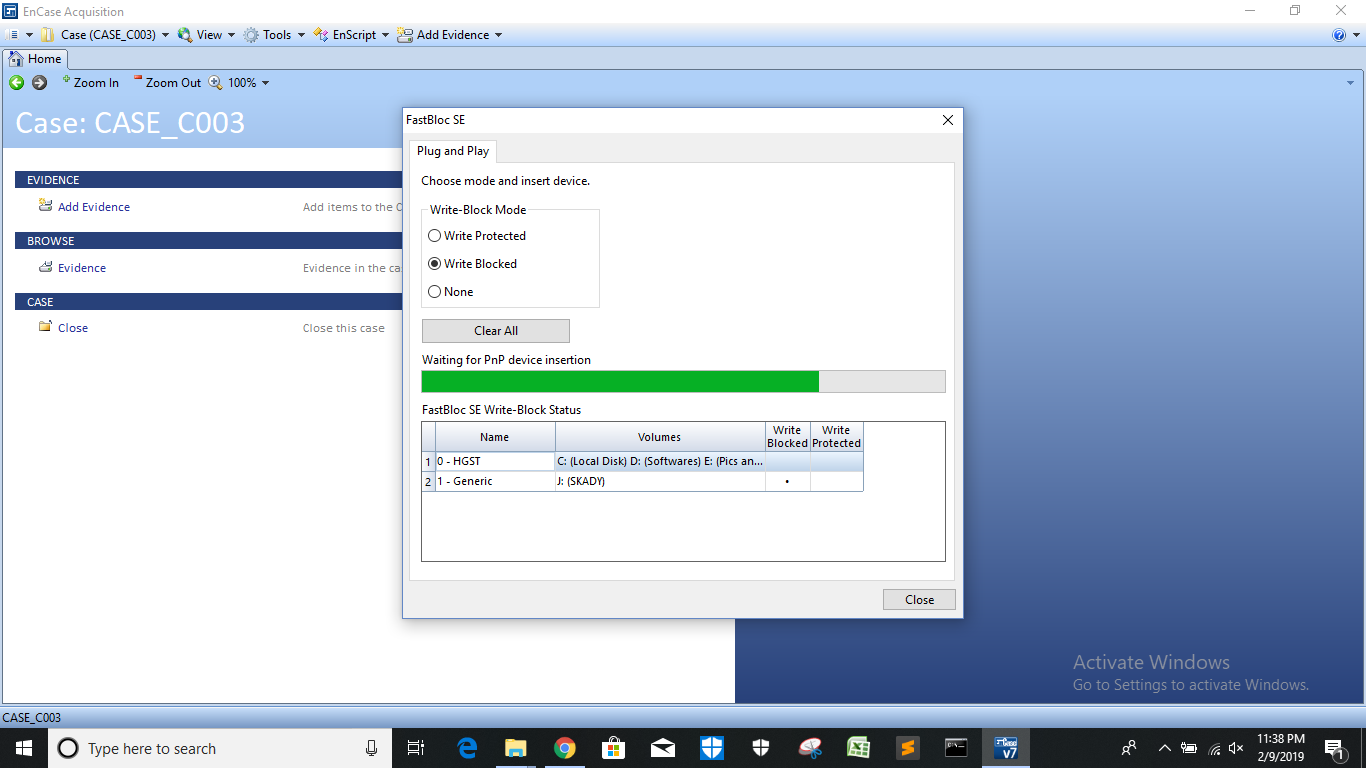
***Fig-3: Enable Write Blocker***

**Step 4**: FastBlock SE window observe the devices detected here:



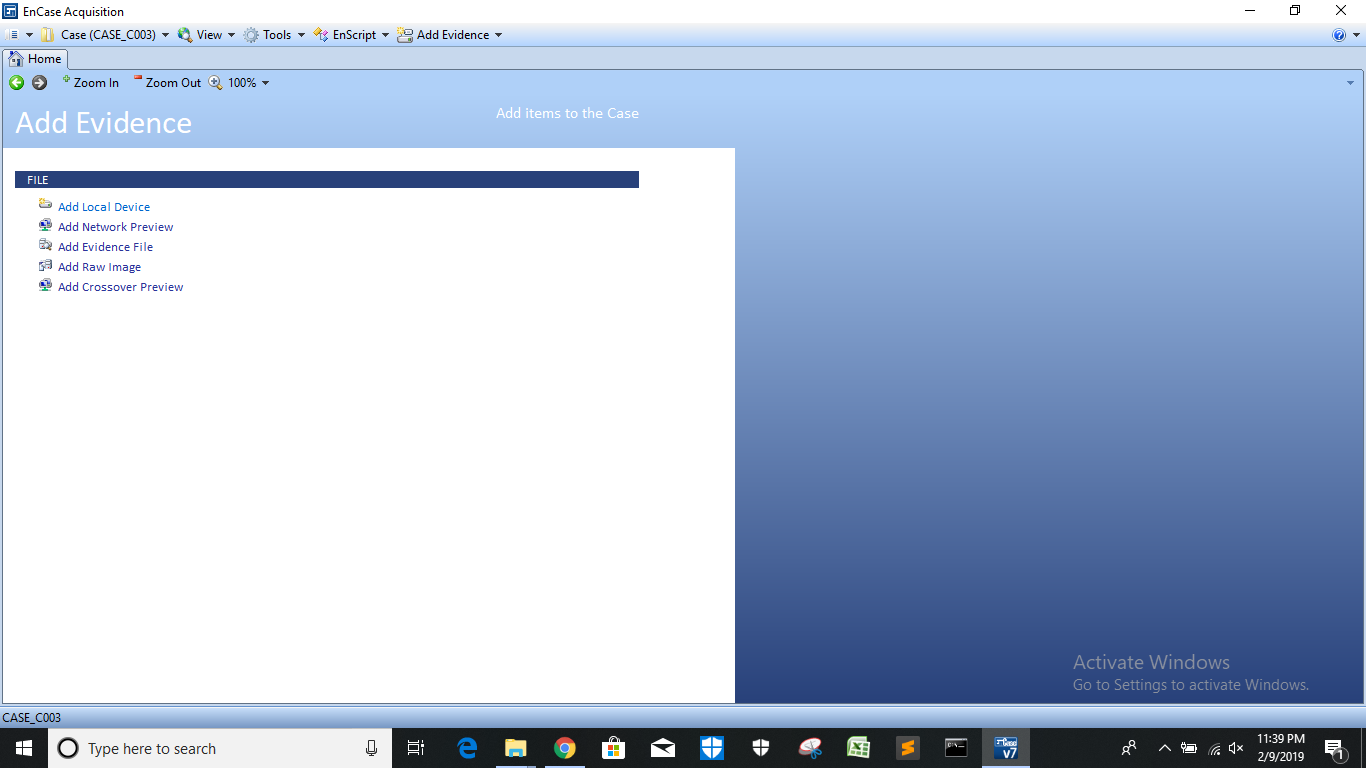
***Fig-4: FastBlock SE window detected the Internal HDD***

**Step 5**: Insert the USB HDD and observe the FastBlock SE window:



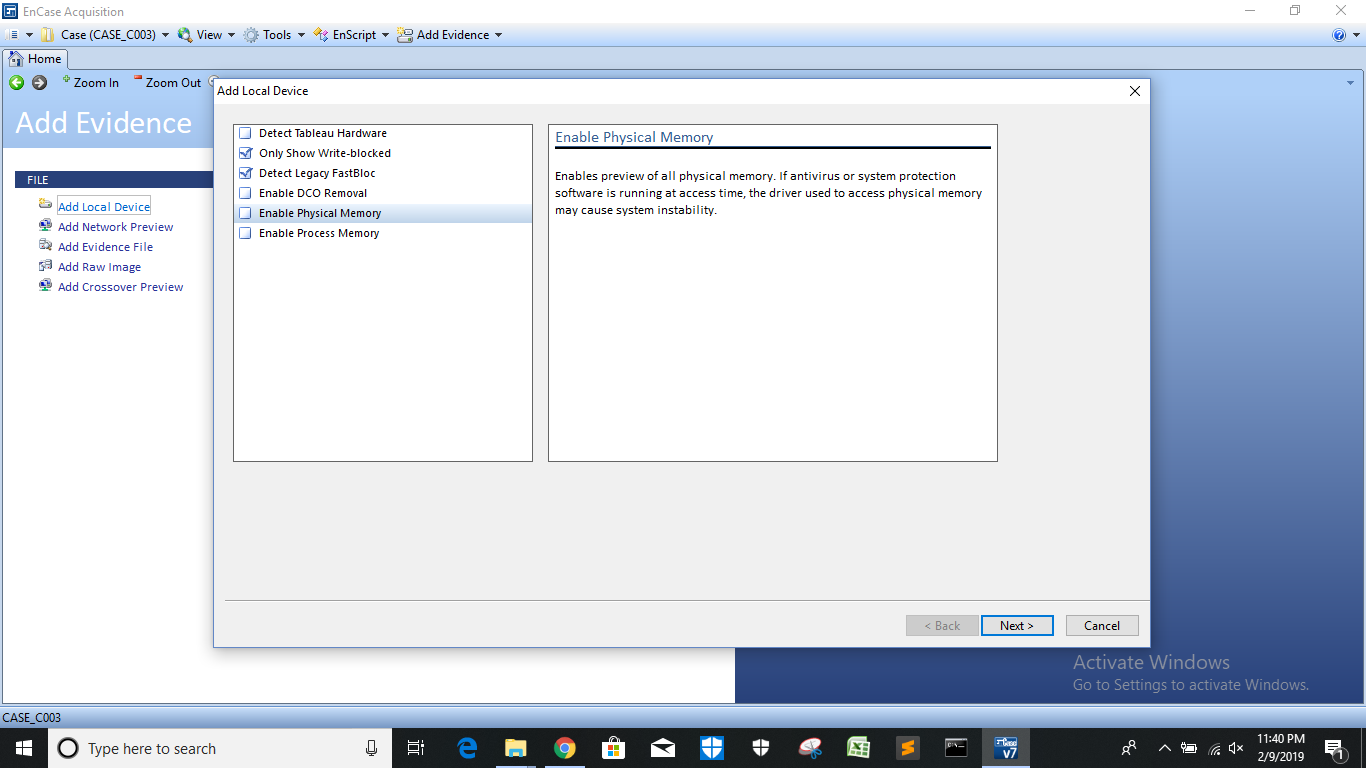
***Fig-5: FastBlock window detected the USB HDD and enabled the write block.***

**Step 6**: Add Evidence:



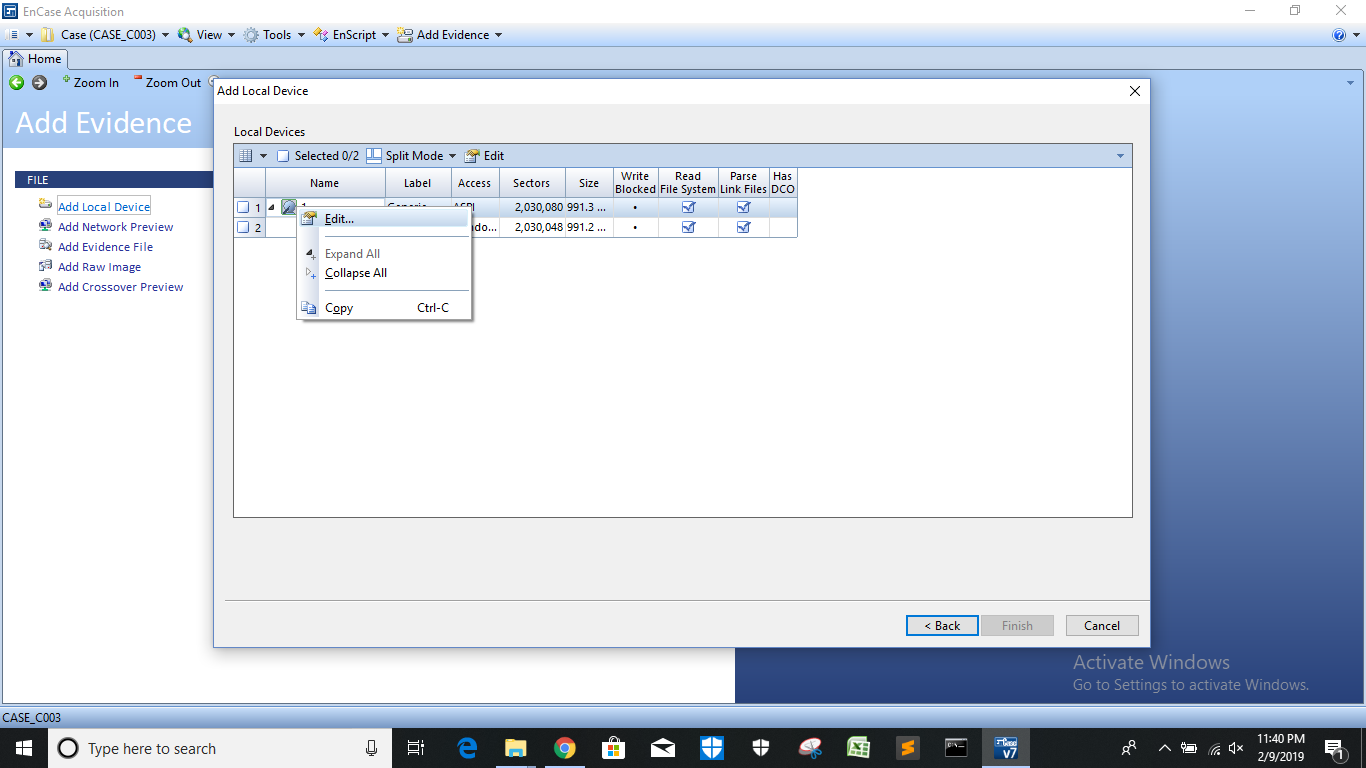
***Fig-6: Add Evidence Section***

**Step 7**: Add Local Device:

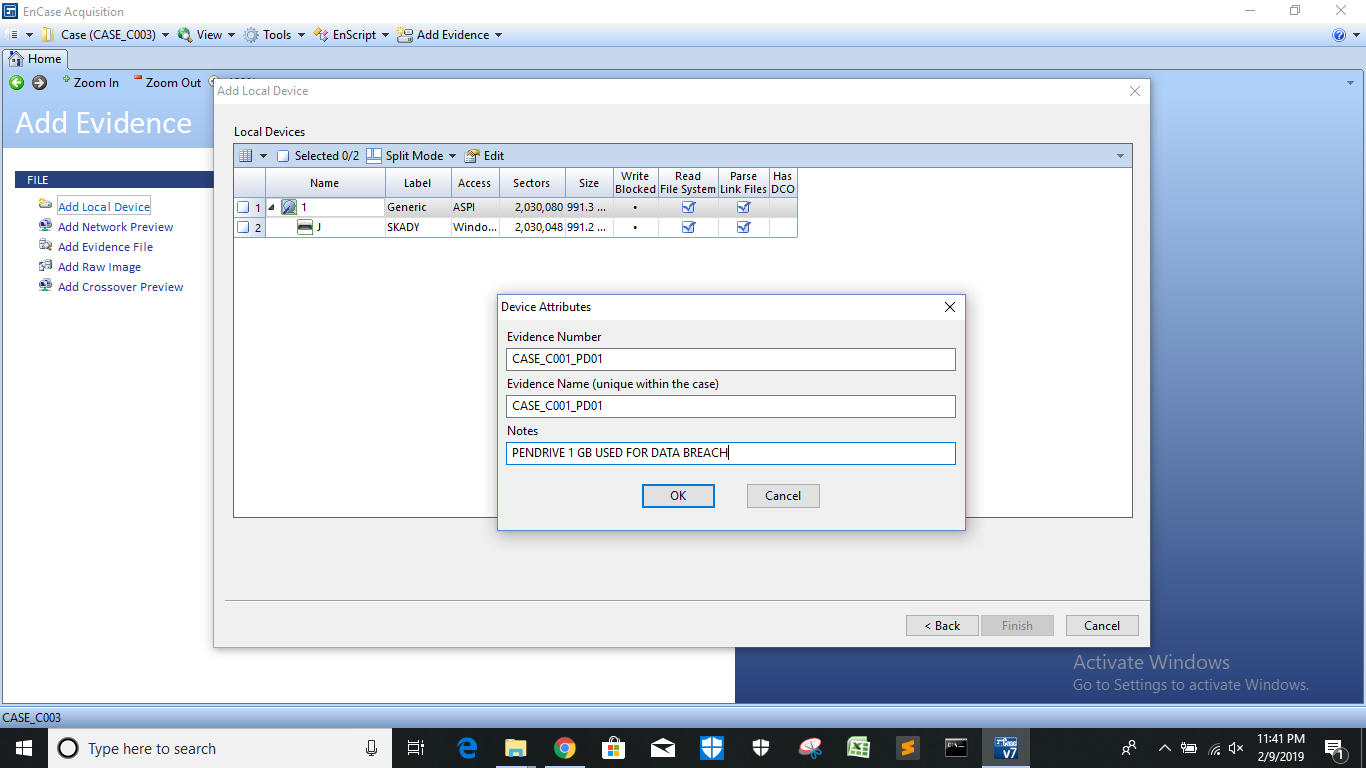


***Fig-7: Add Local Device***

**Step 8**: Naming of the detected local device which is write blocked:

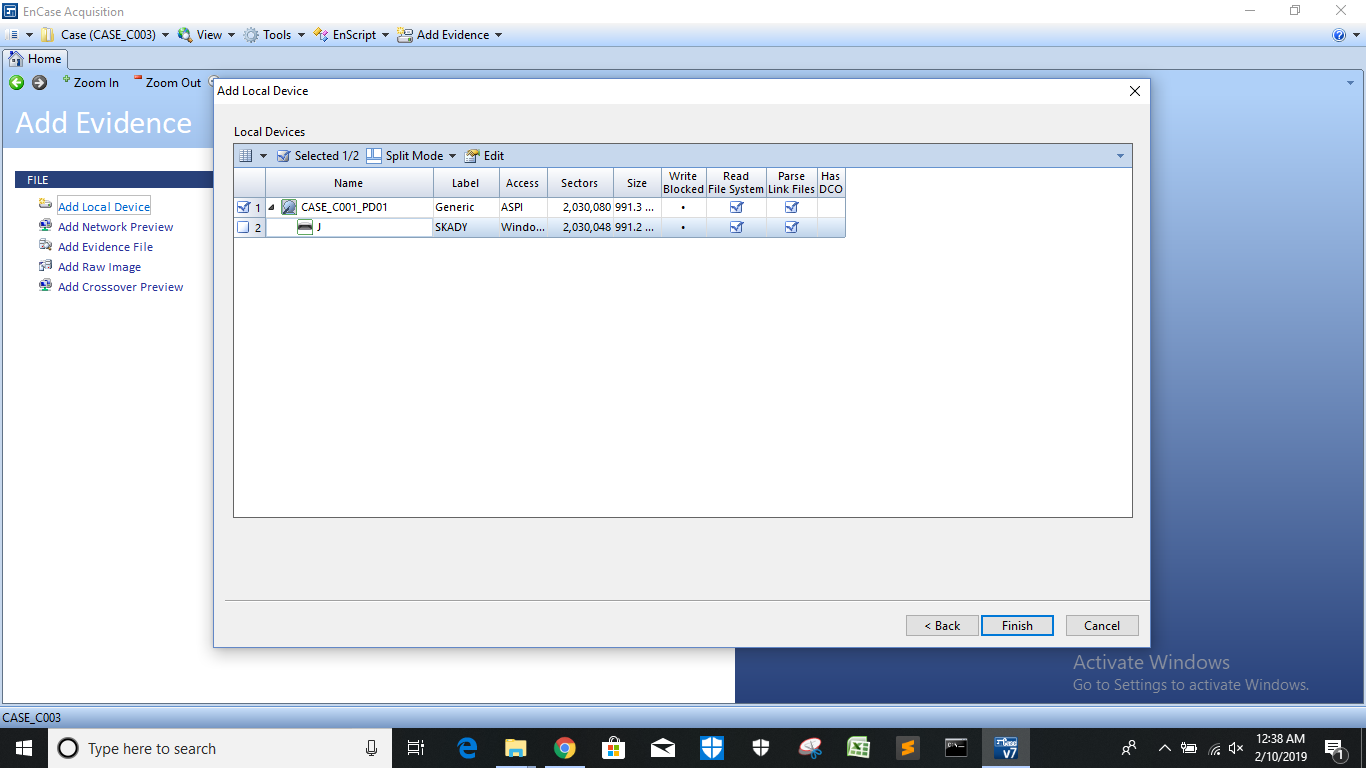


***Fig-8: Name the Detected device***

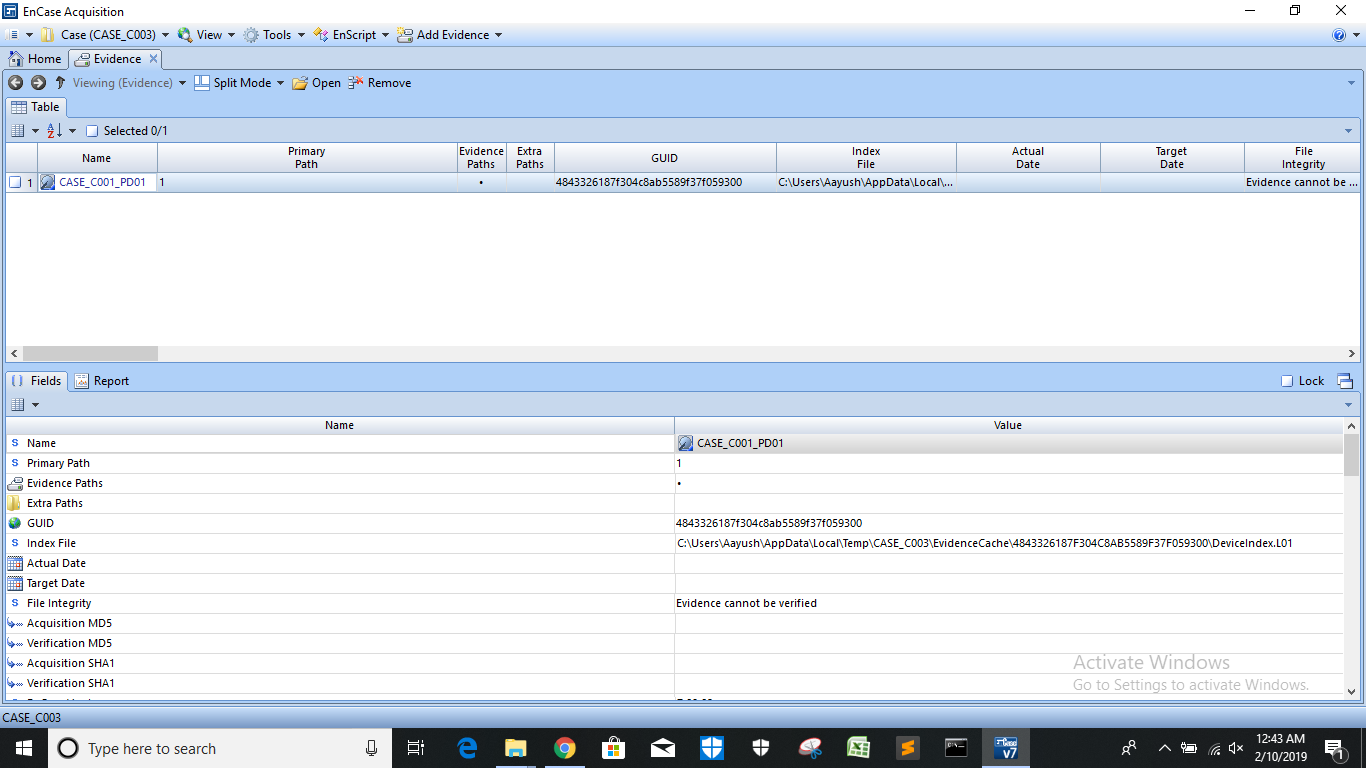
******

***Fig-9: Set Device Attributes***

**Step 9**: Finish attributes naming and observe the Case details:

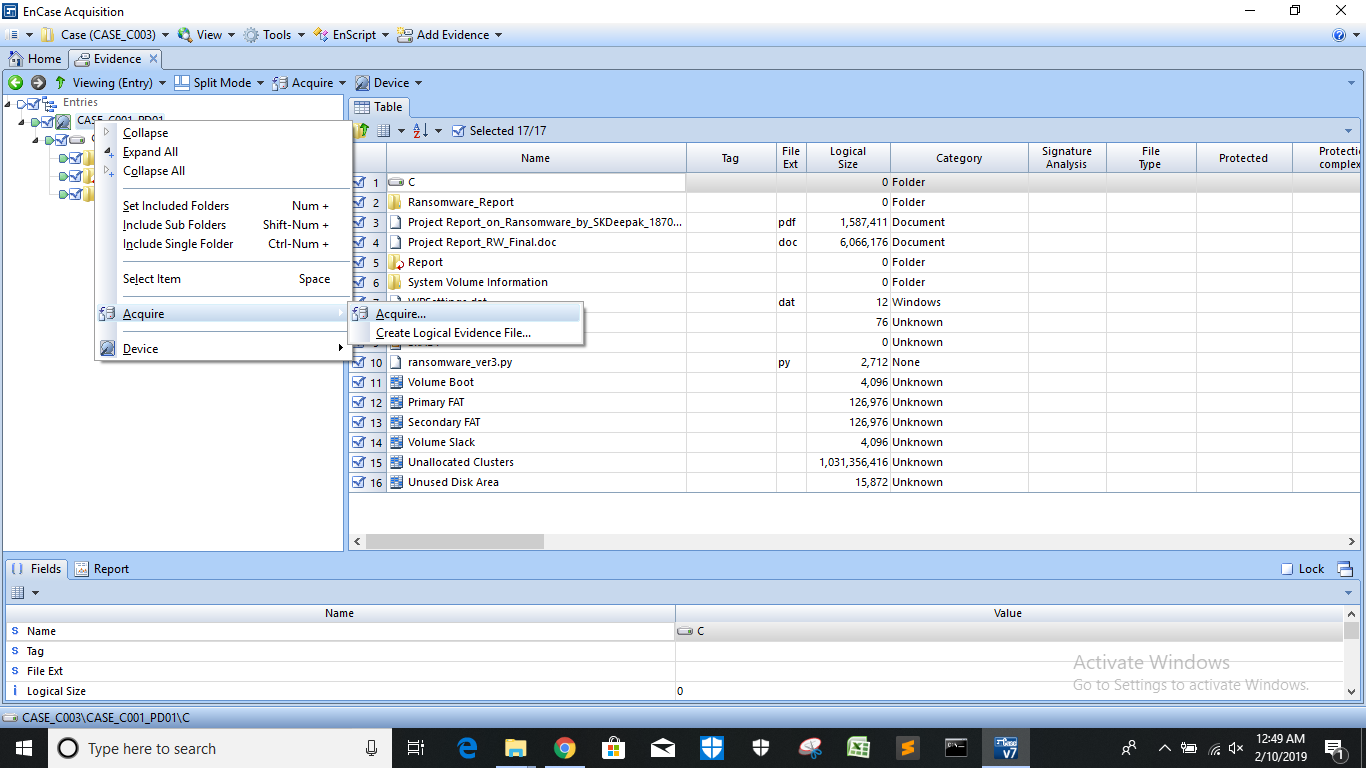


***Fig-10: Finish attributes naming***



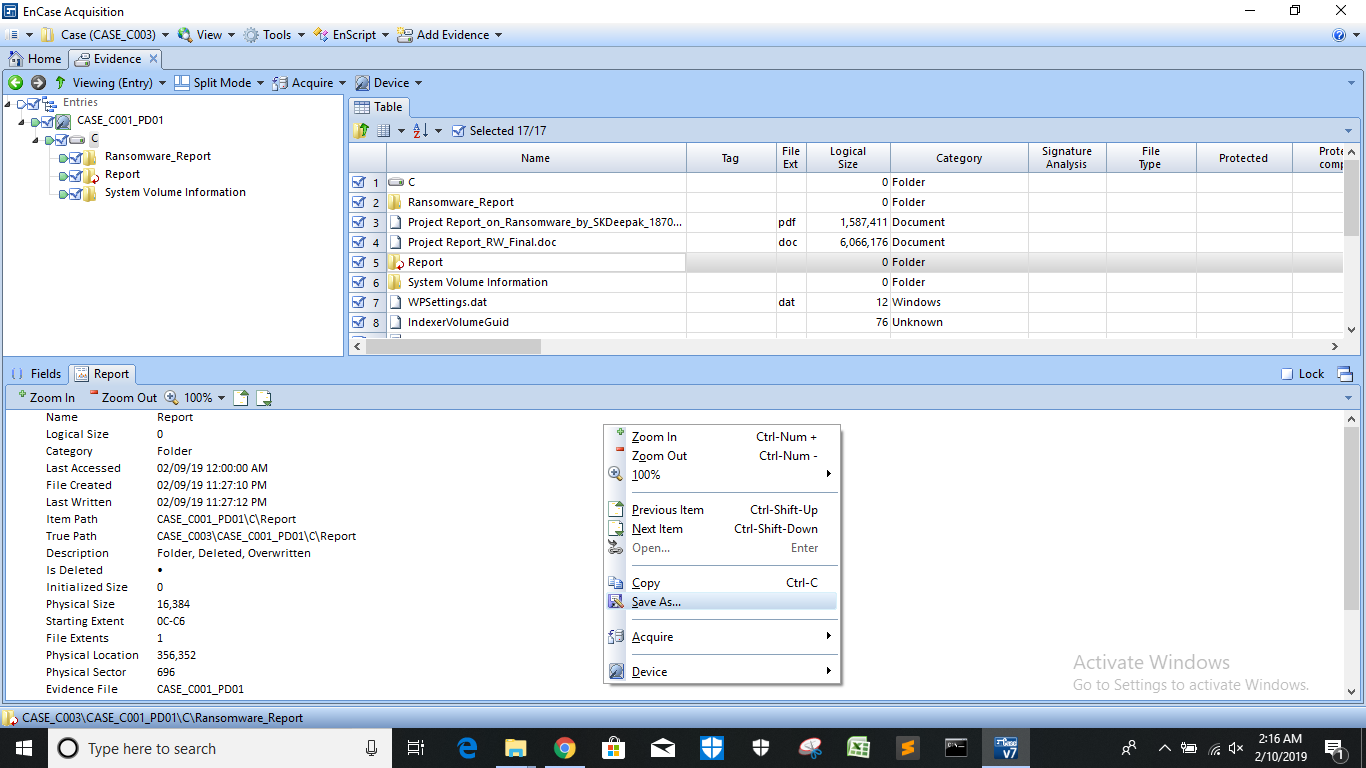
***Fig-11: Case Details***

**Step 10**: Double click on case and select all the data and then right click on case and Acquire:



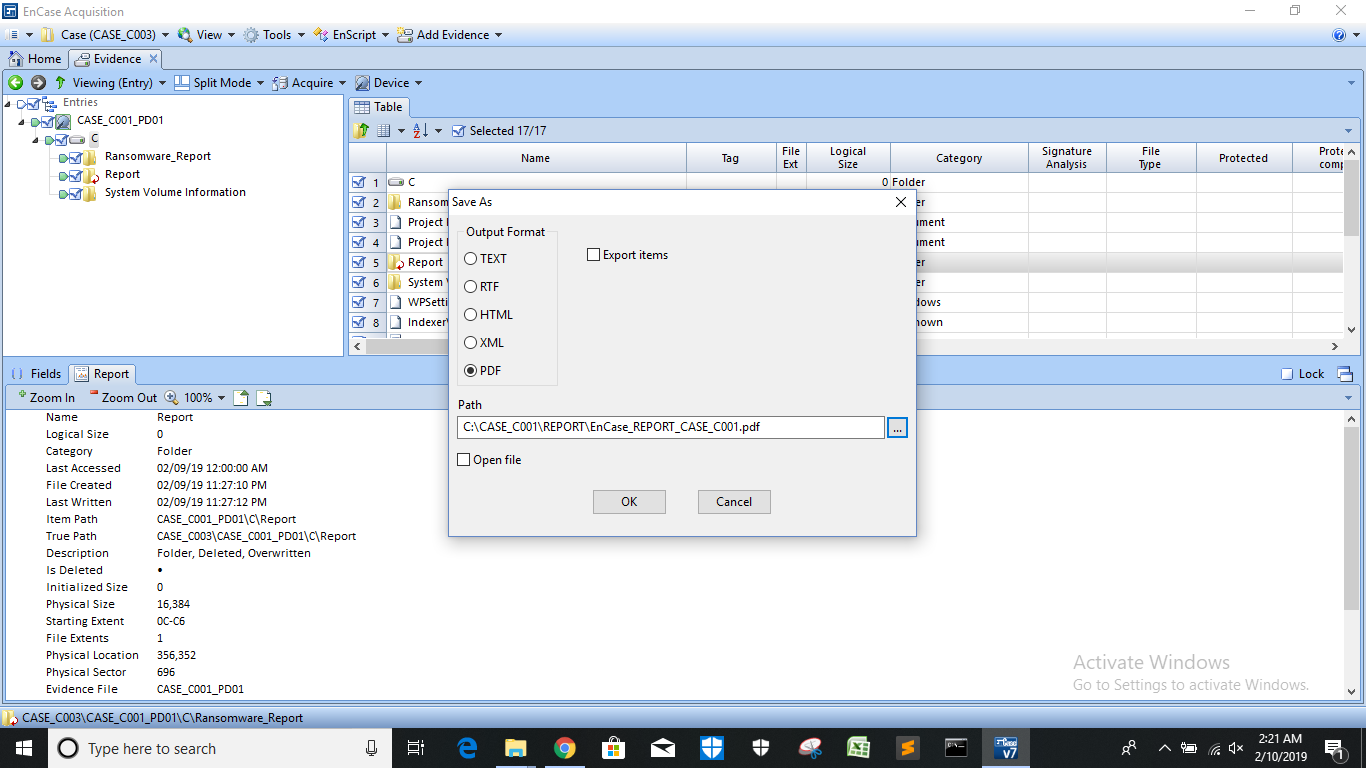
***Fig-12: Acquire Data***

**Step 11**: Wait for the process to complete the acquisition and then save the report:



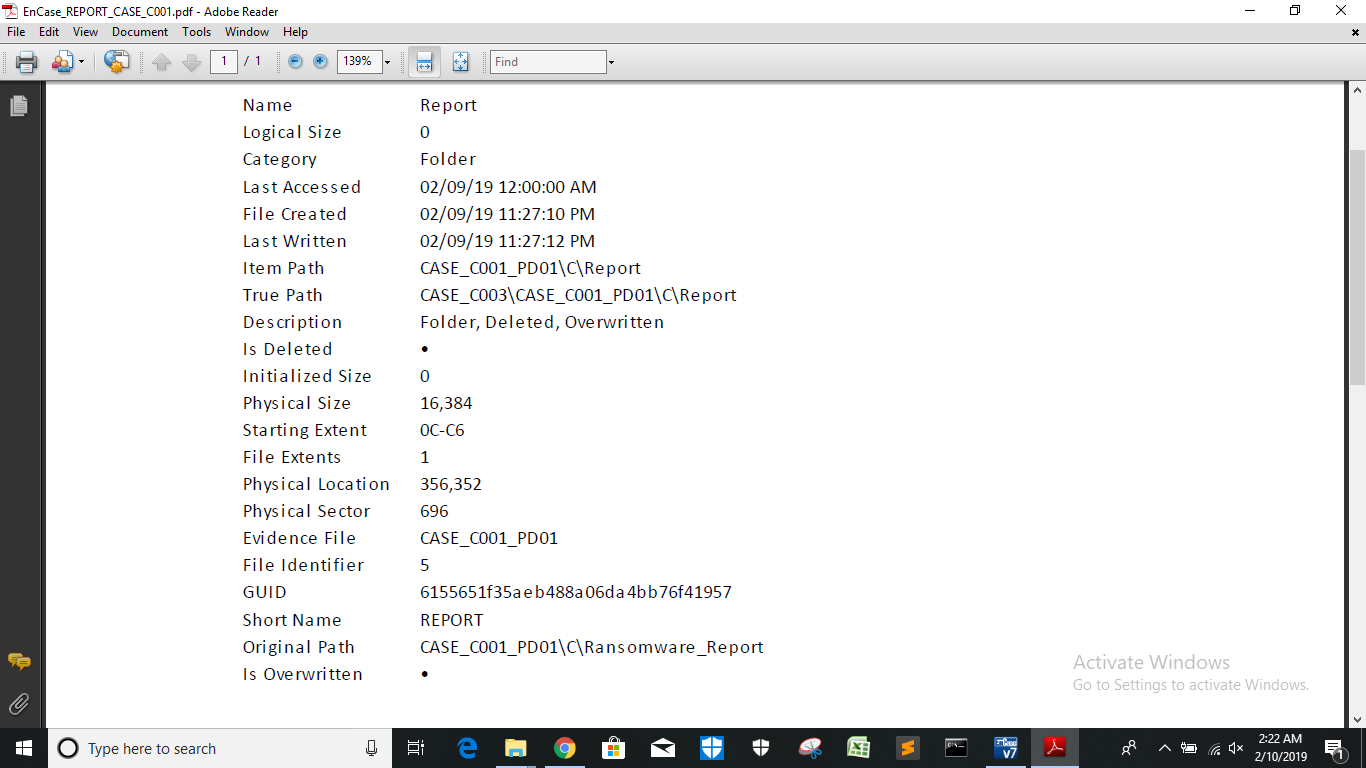
***Fig-13: Save the Report***

**Step 12**: Select the format and path to save the report:



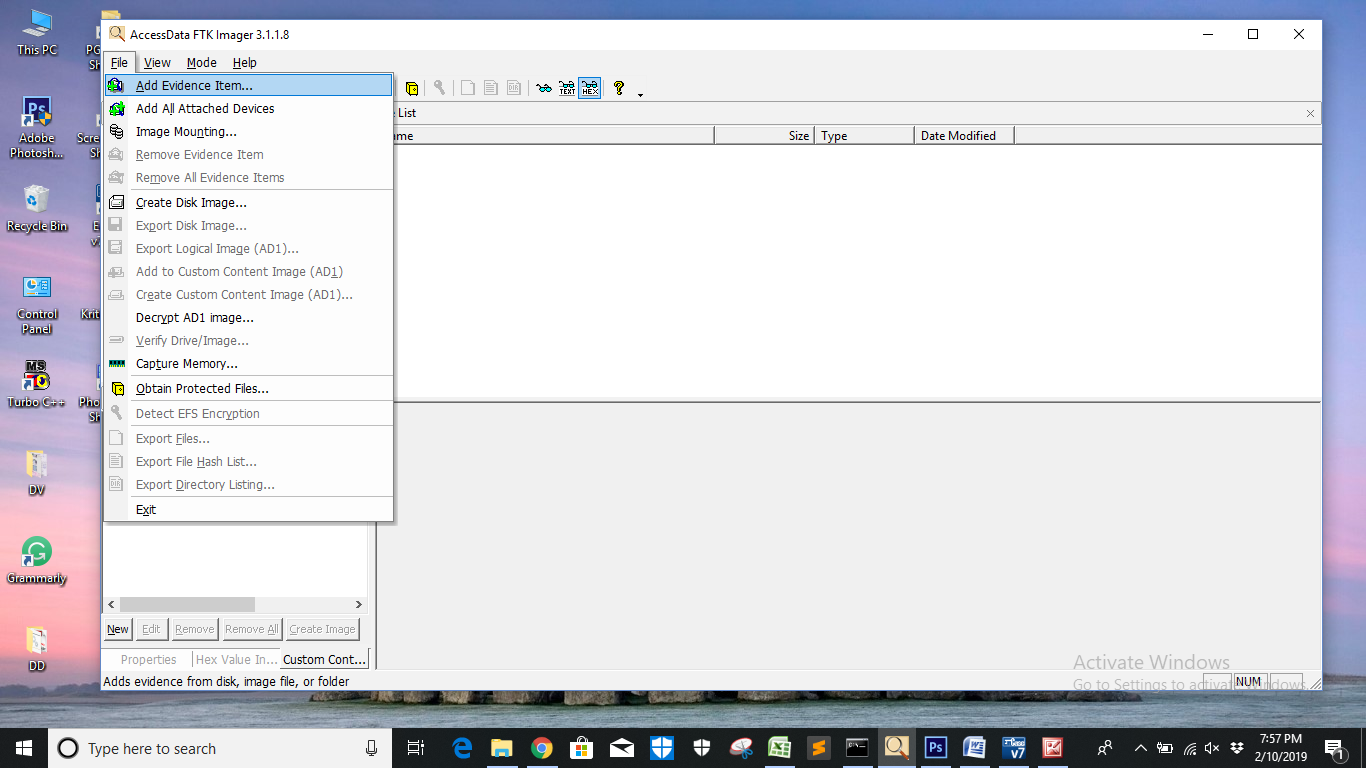
***Fig-14: Save Report in PDF format***

**Step 13**: View Report Content:

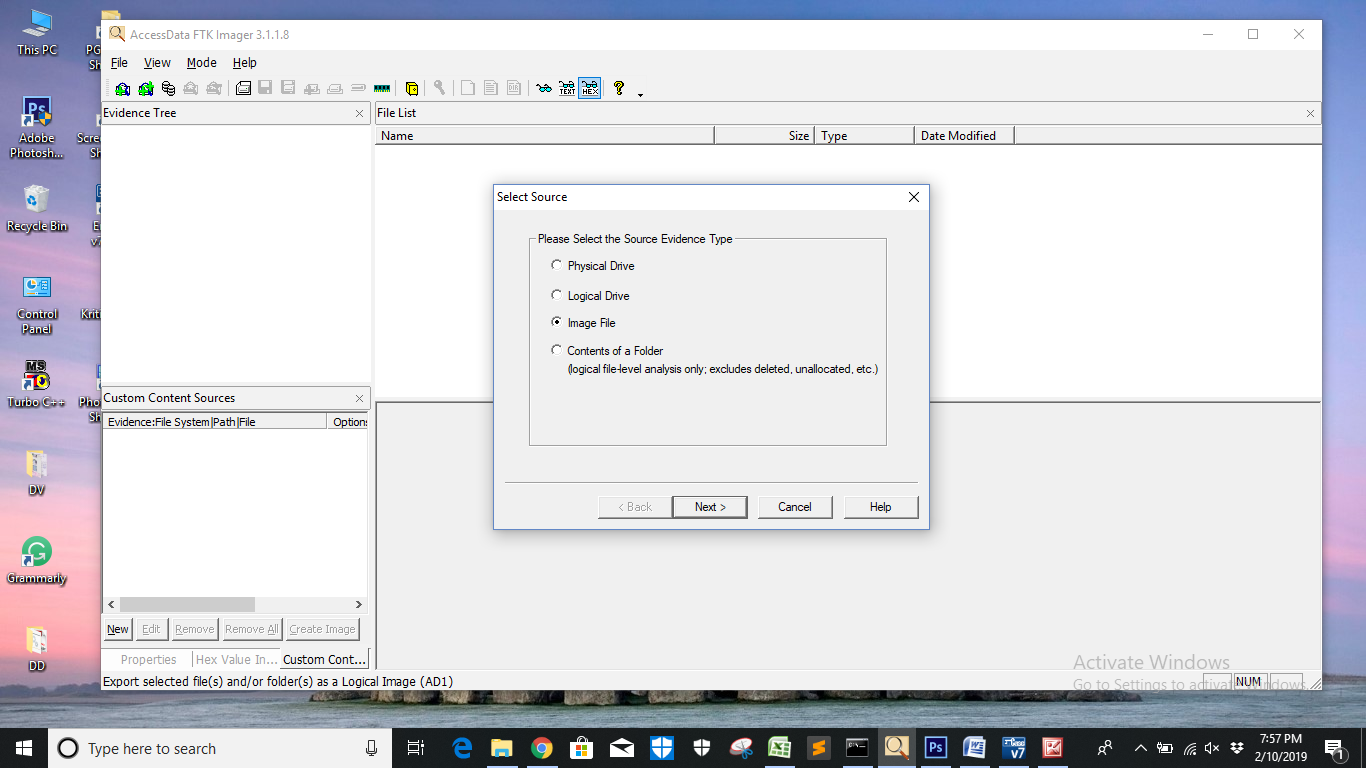


***Fig-15: Report Content***

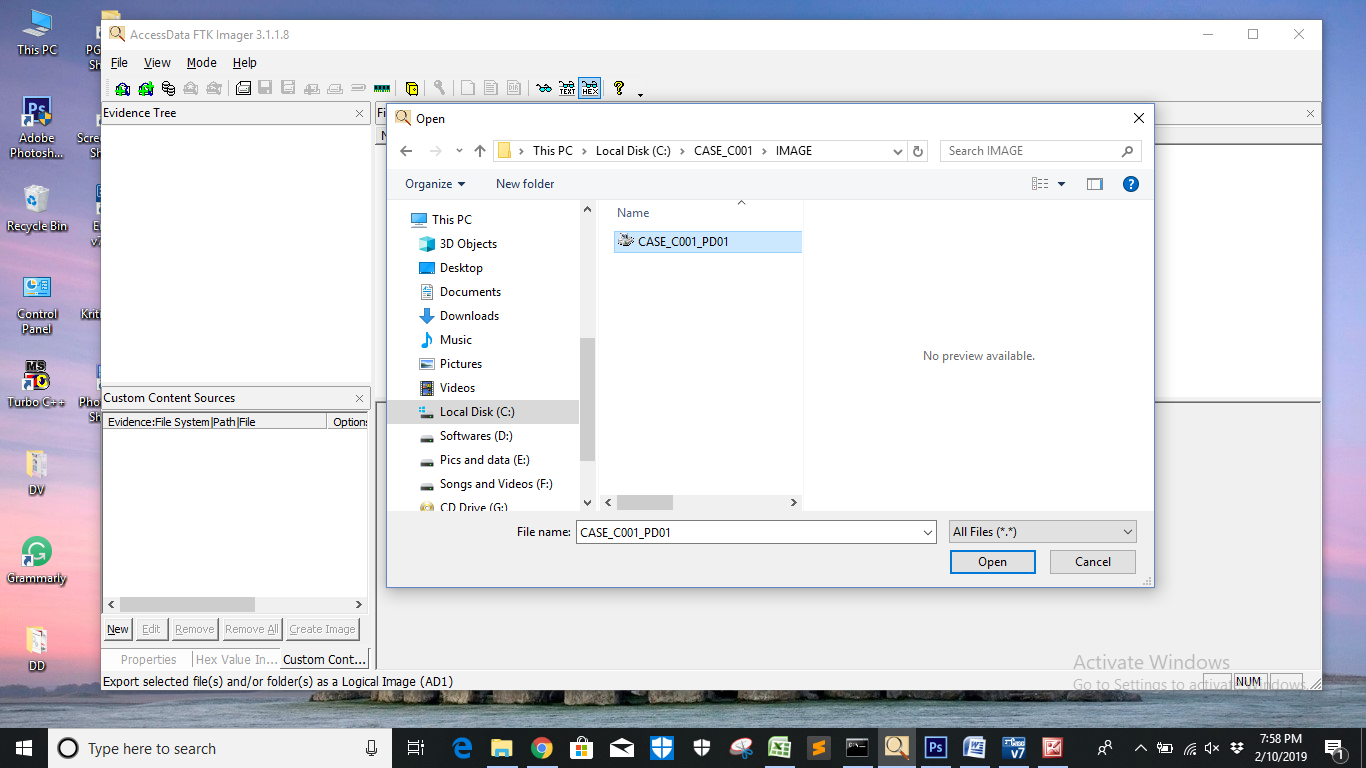
**Step 14**: Open CASE Image in FTK Manager:



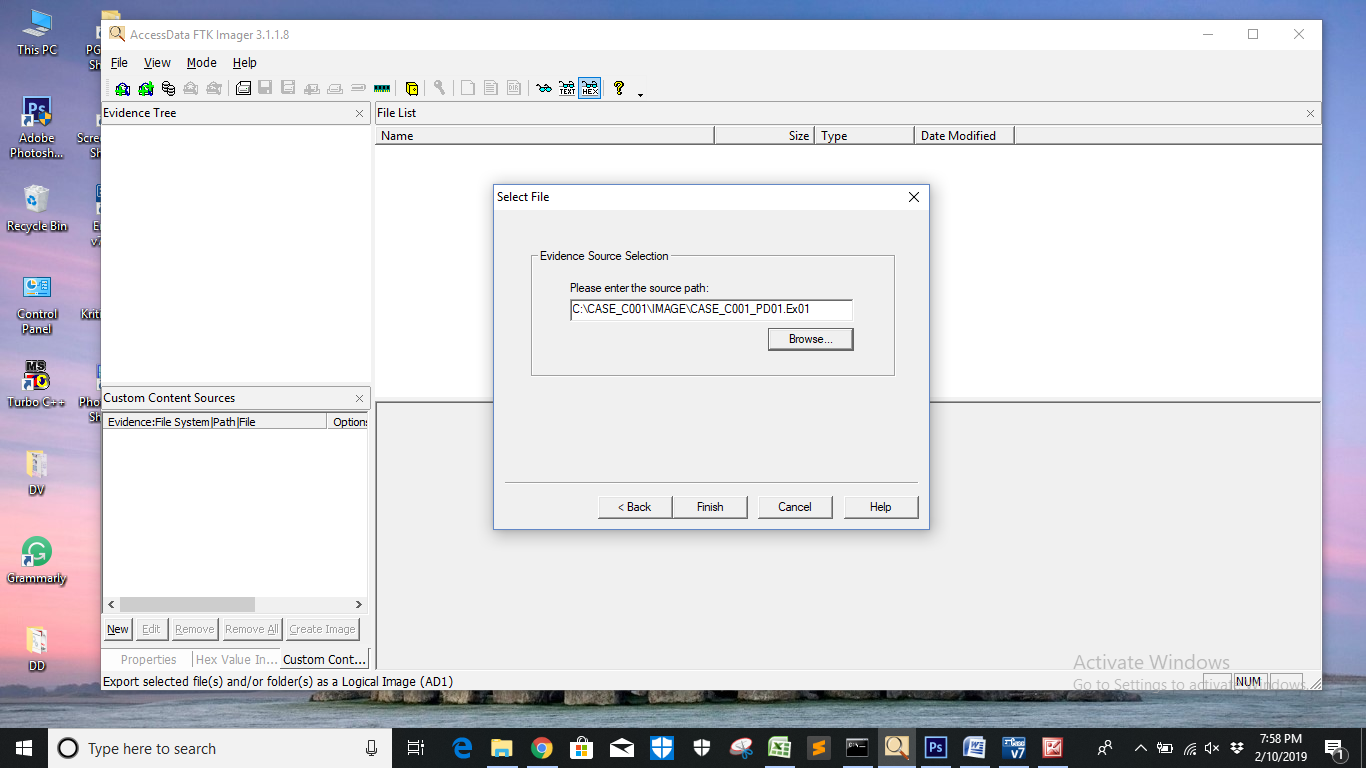
***Fig-16: Add Evidence Item in FTK Manager***

******

***Fig-17: Choose Image File option in Source***

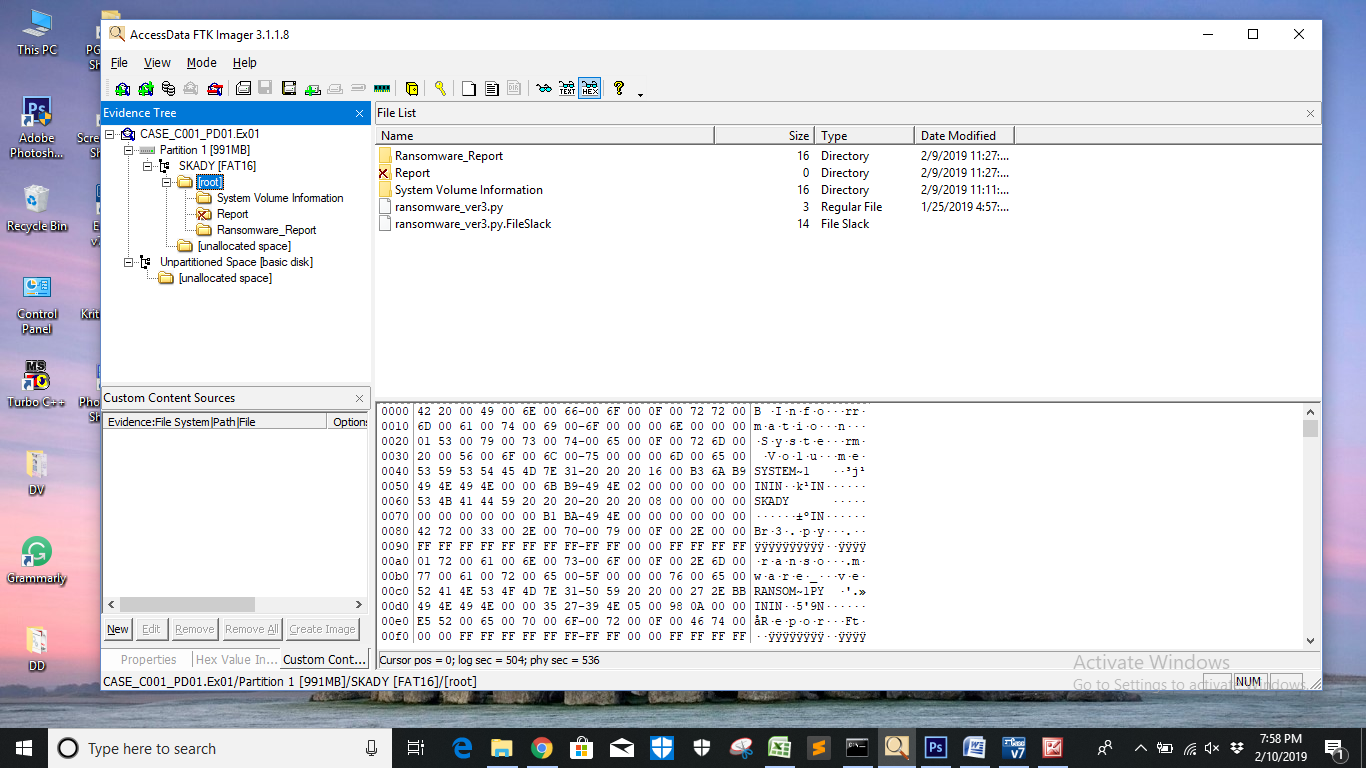
******

***Fig-18: Select EnCase Case file***

******

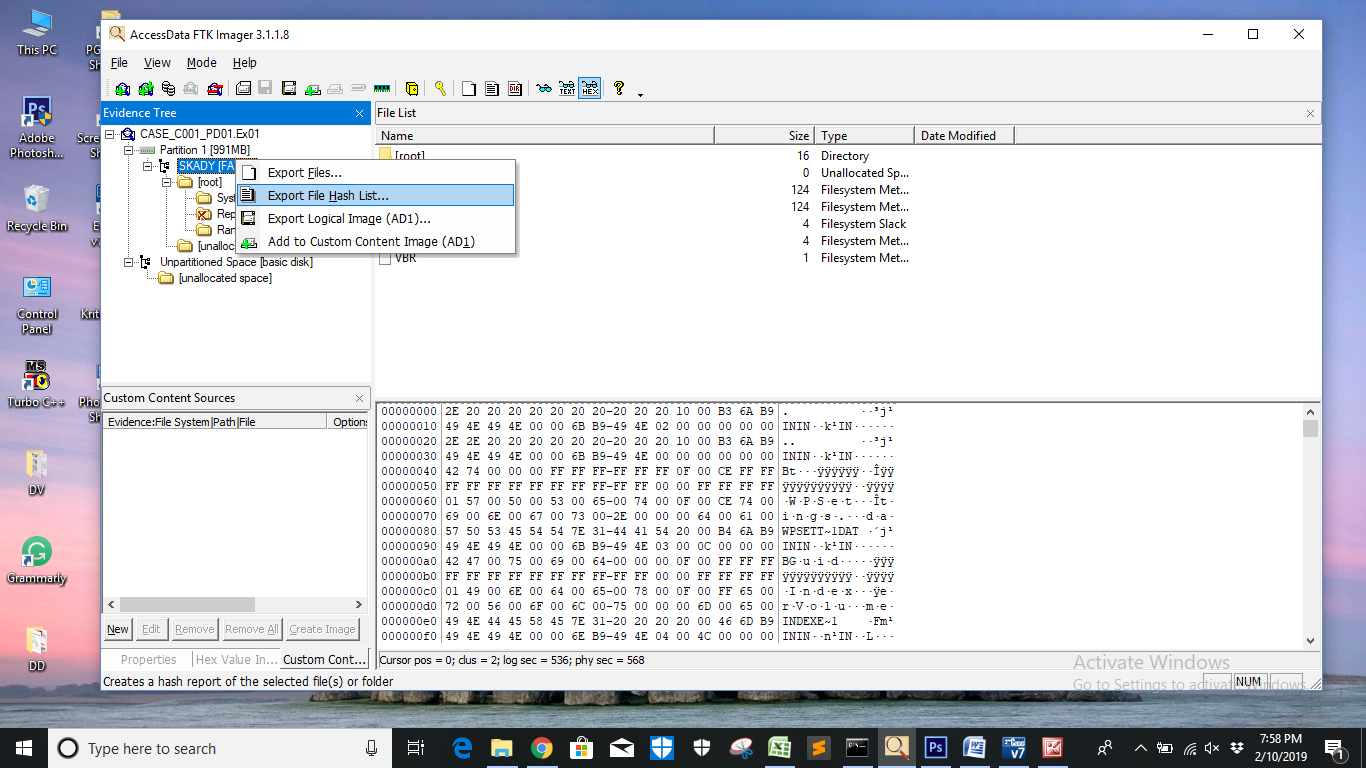
***Fig-19: Observe Path***

**Step 15**: Expand the evidence tree and observe directories and files:



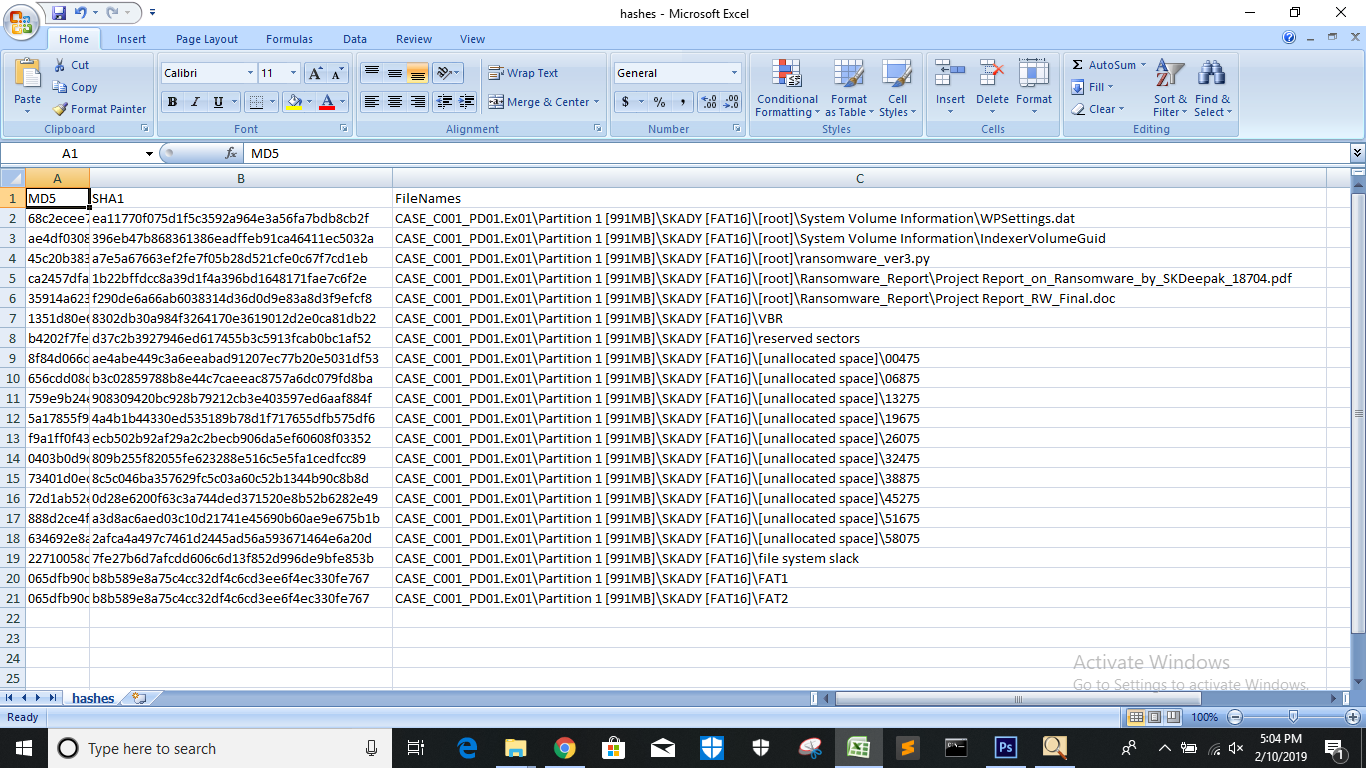
***Fig-20: Evidence Tree***

**Step 16**: Export File hash list:

******

***Fig-21 Export File Hash***

**Step 17**: Observe the output:



***Fig-22: Hash Output of all the files***