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.

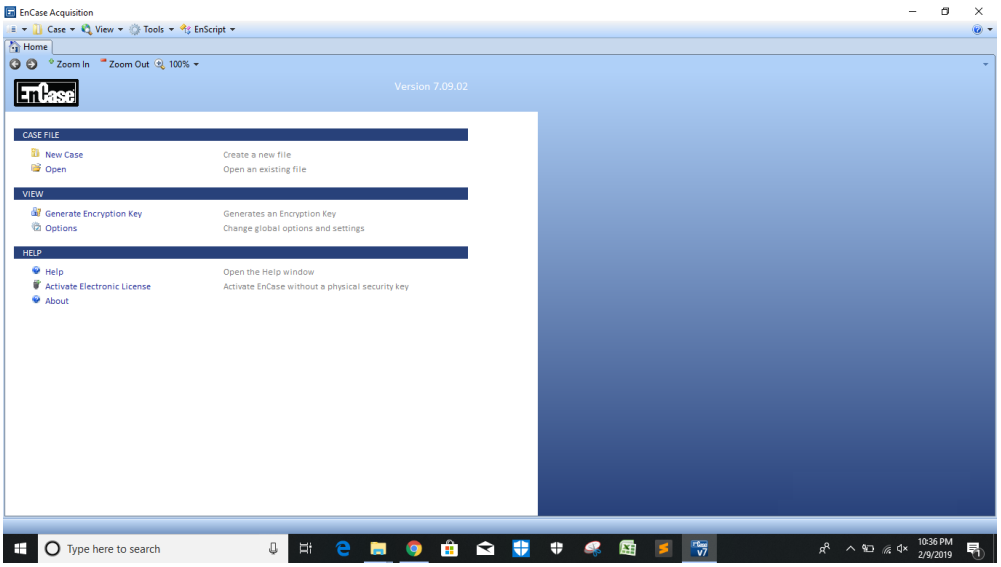


Fig-1: Launch EnCase Acquisition

Step 2: Create a new Case **Case_C003:**

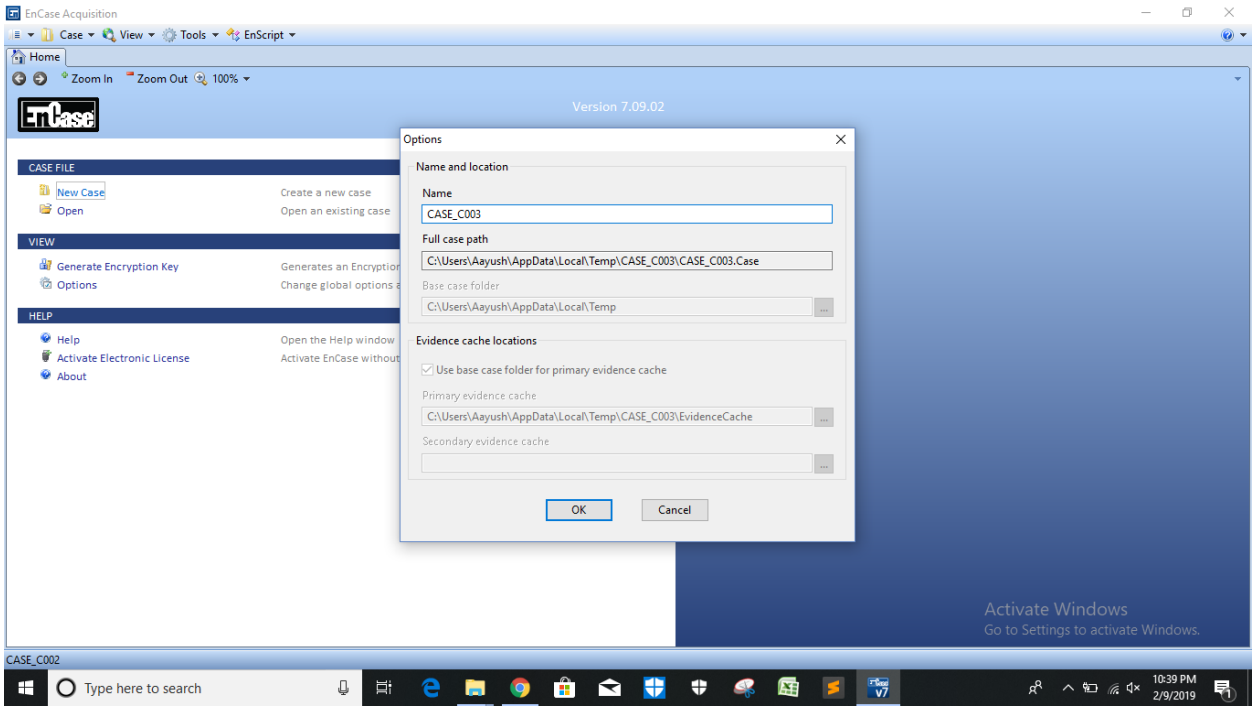


Fig-2: Create a new Case

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

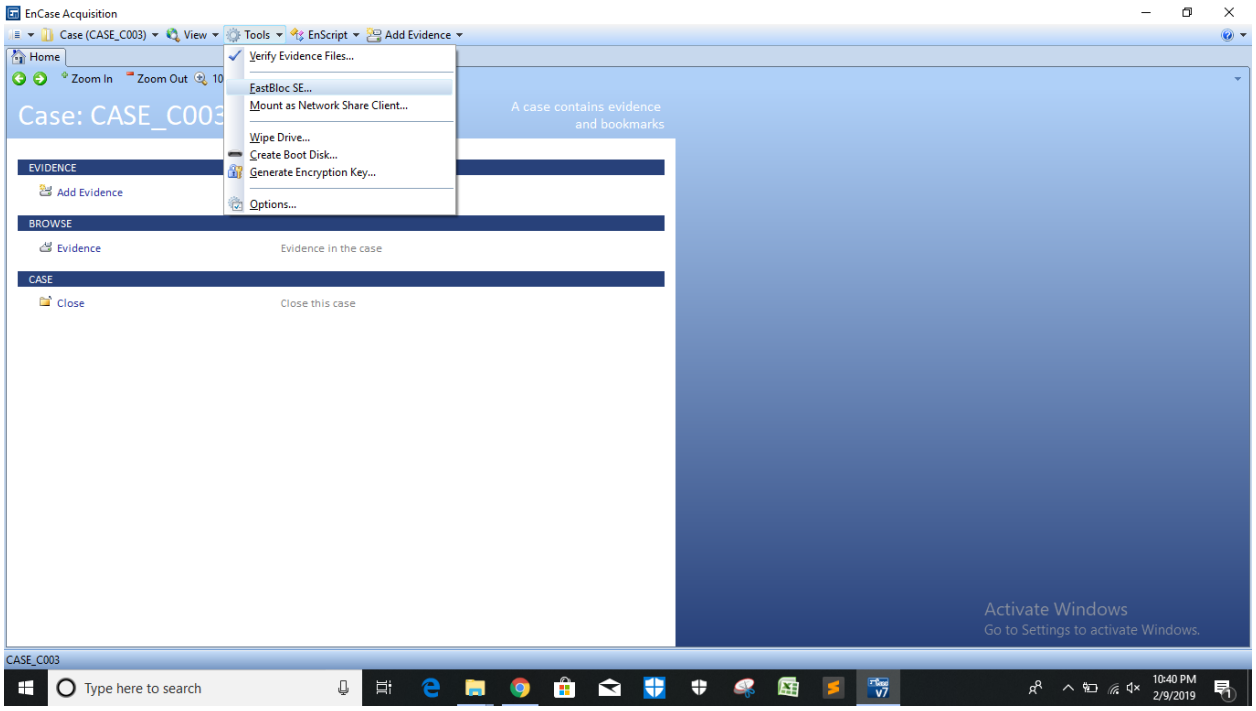


Fig-3: Enable Write Blocker

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

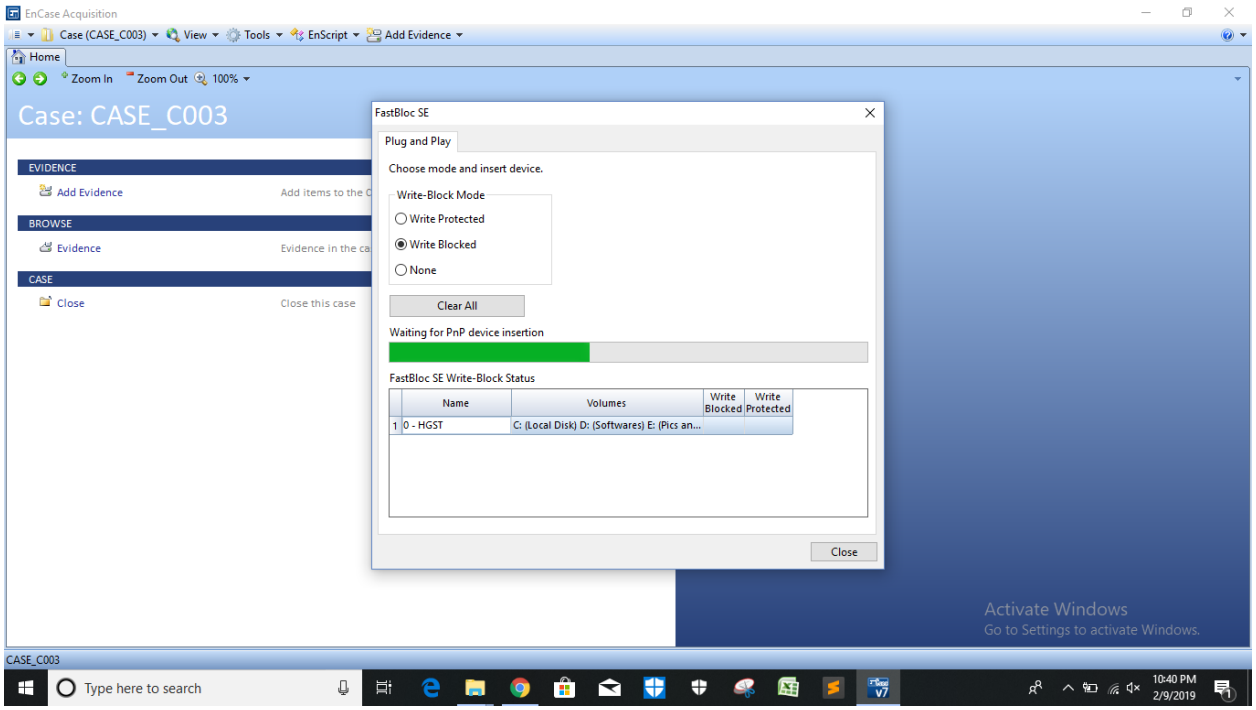


Fig-4: FastBlock SE window detected the Internal HDD

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

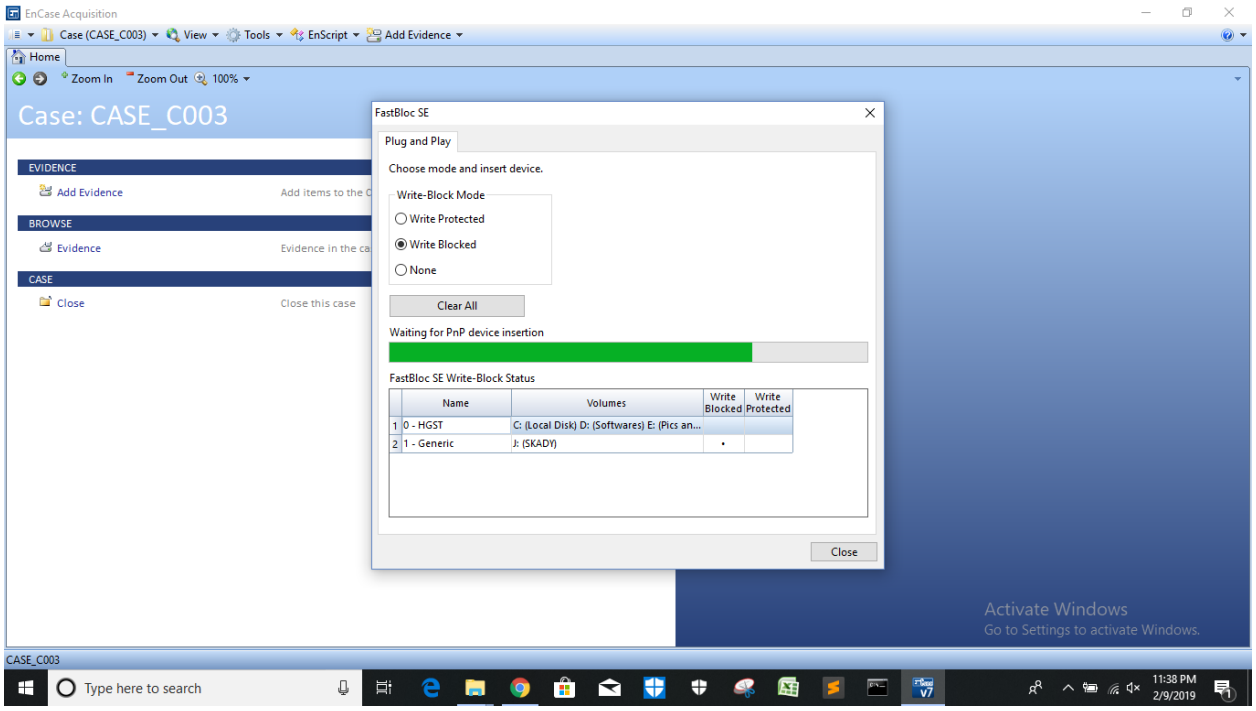


Fig-5: FastBlock window detected the USB HDD and enabled the write block.

Step 6: Add Evidence:

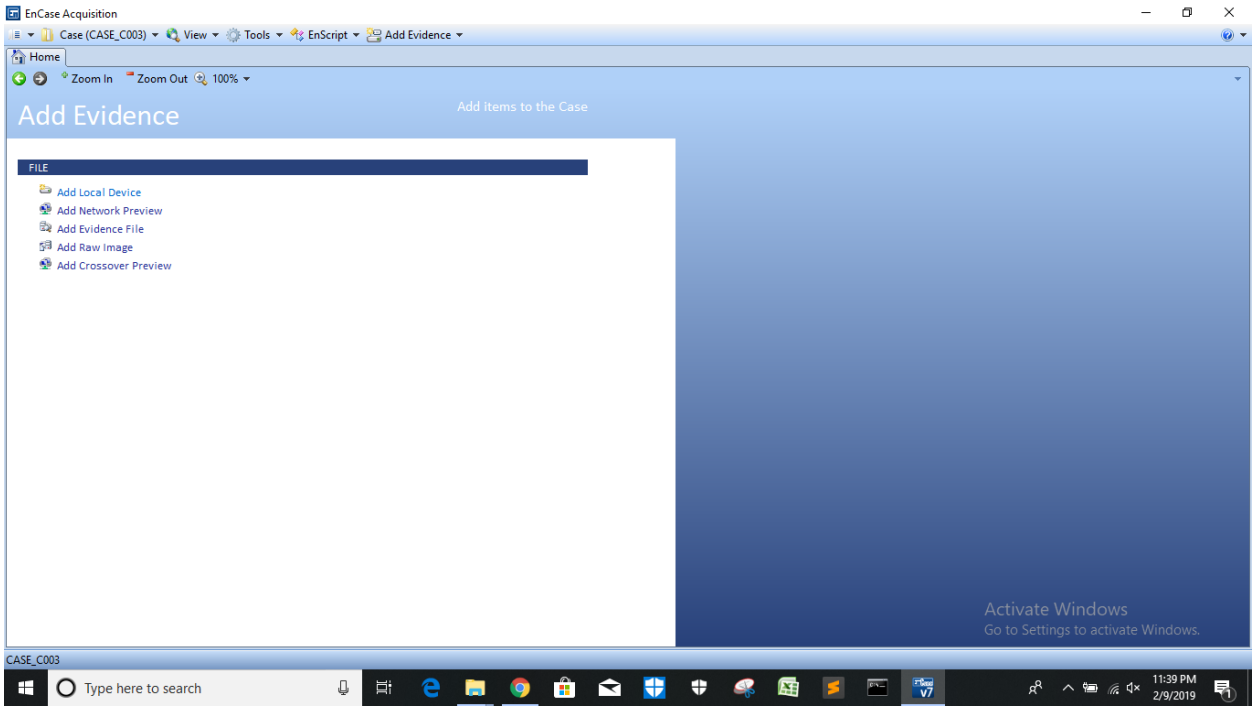


Fig-6: Add Evidence Section

Step 7: Add Local Device:

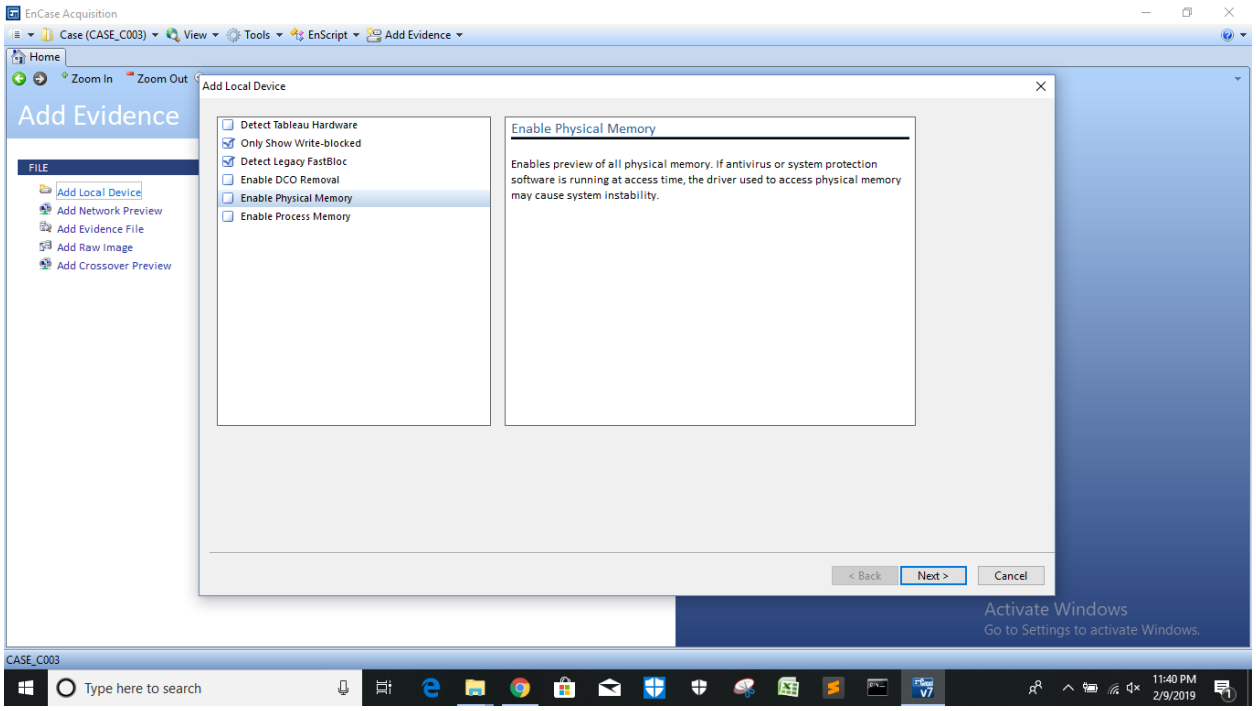


Fig-7: Add Local Device

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

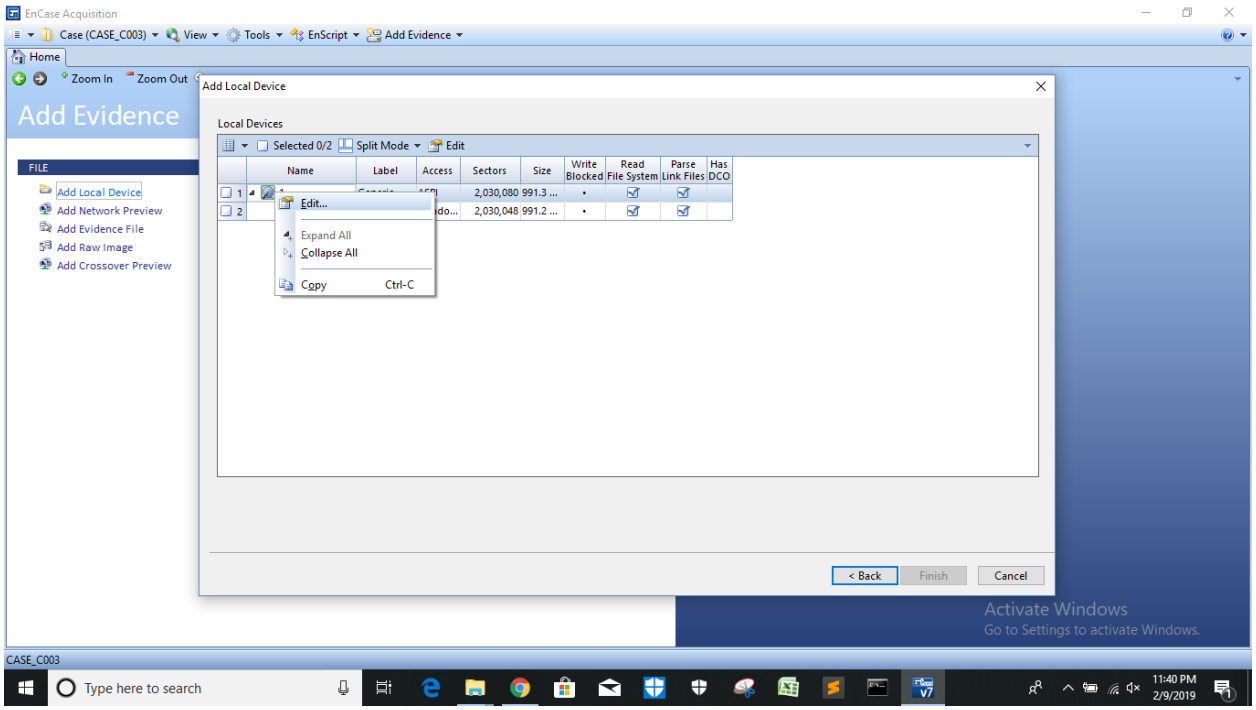


Fig-8: Name the Detected device

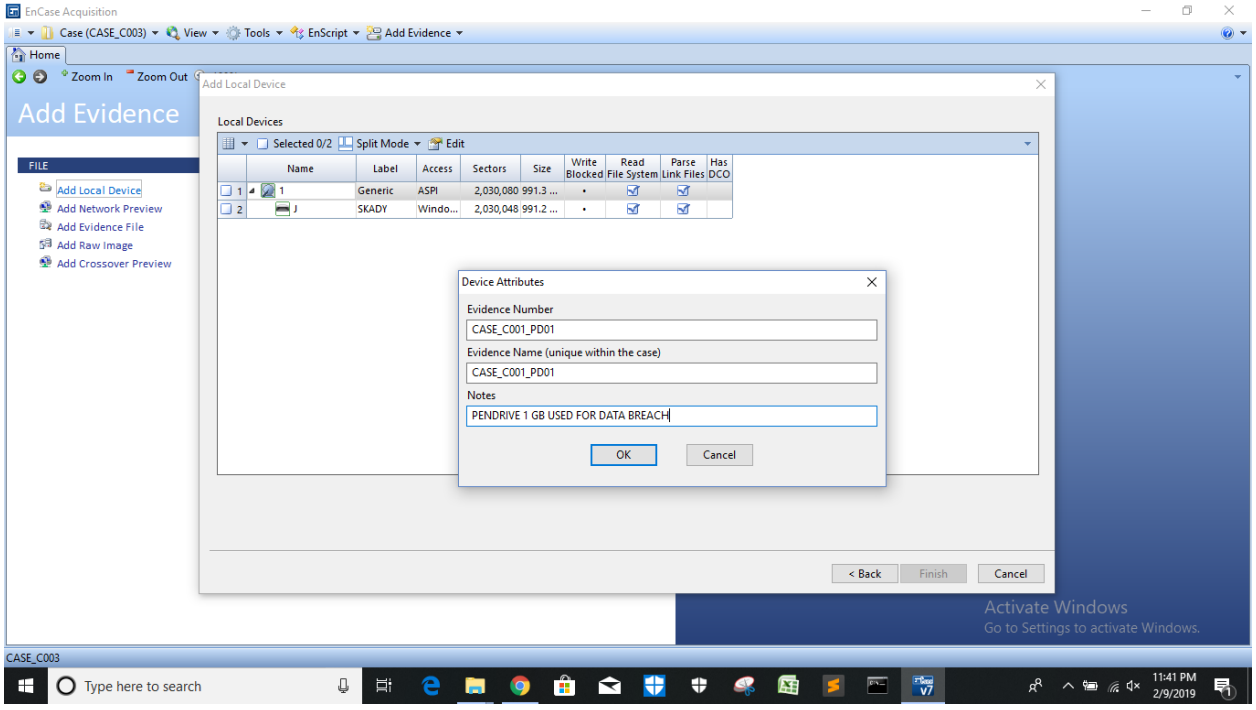


Fig-9: Set Device Attributes

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

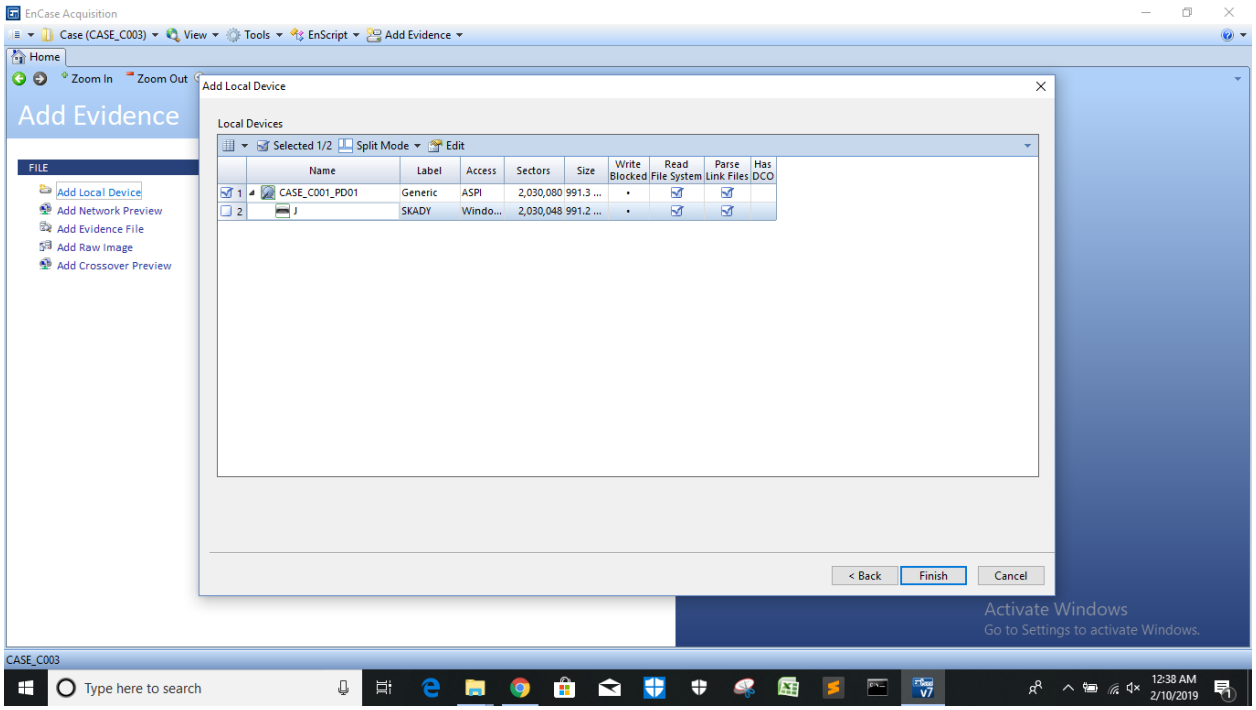


Fig-10: Finish attributes naming

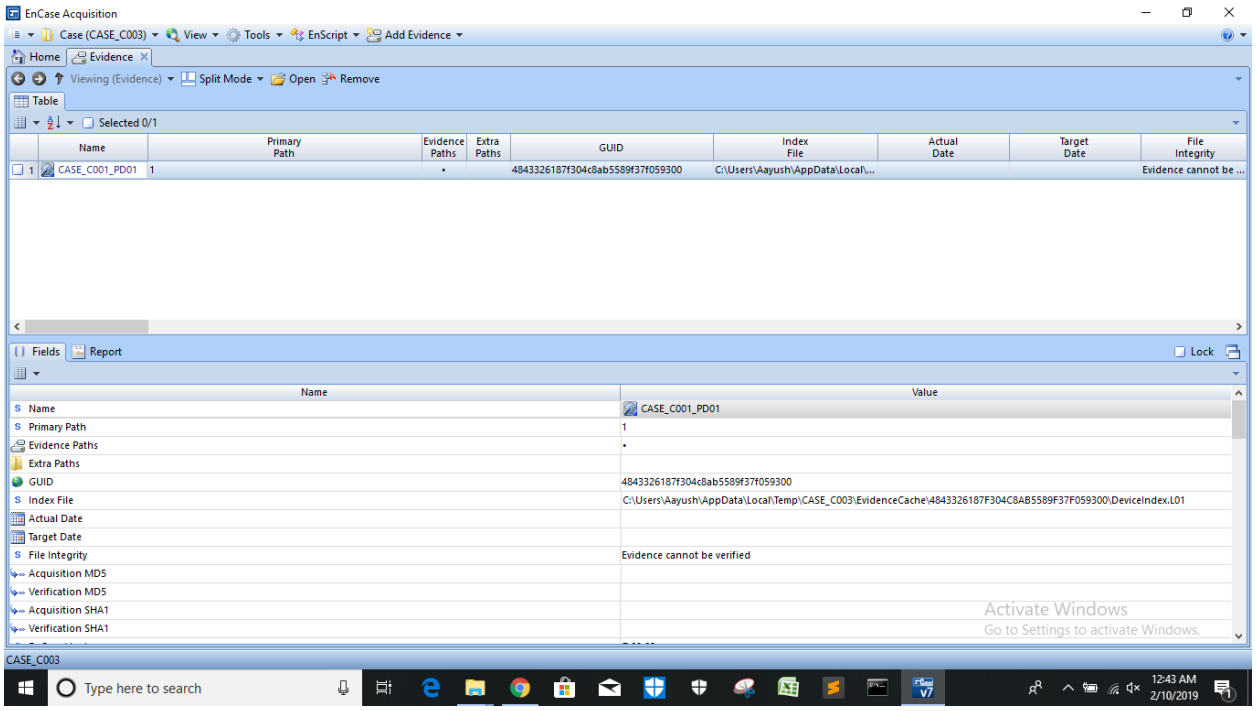


Fig-11: Case Details

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

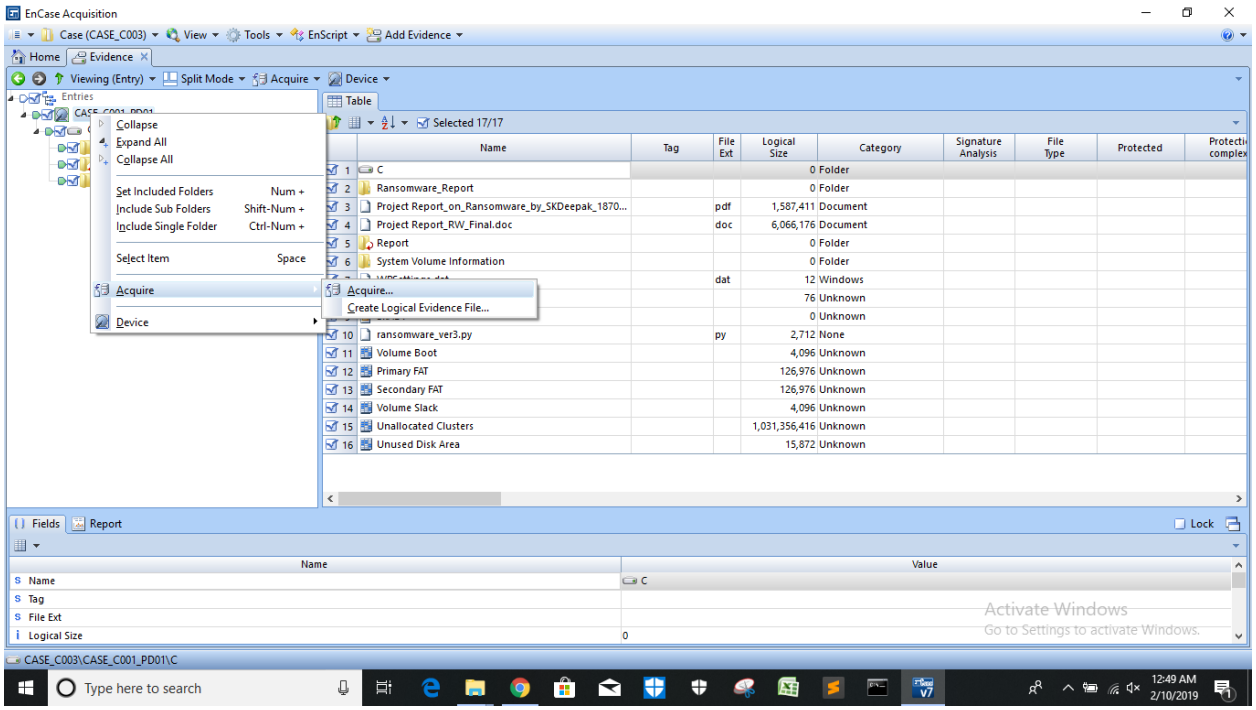


Fig-12: Acquire Data

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

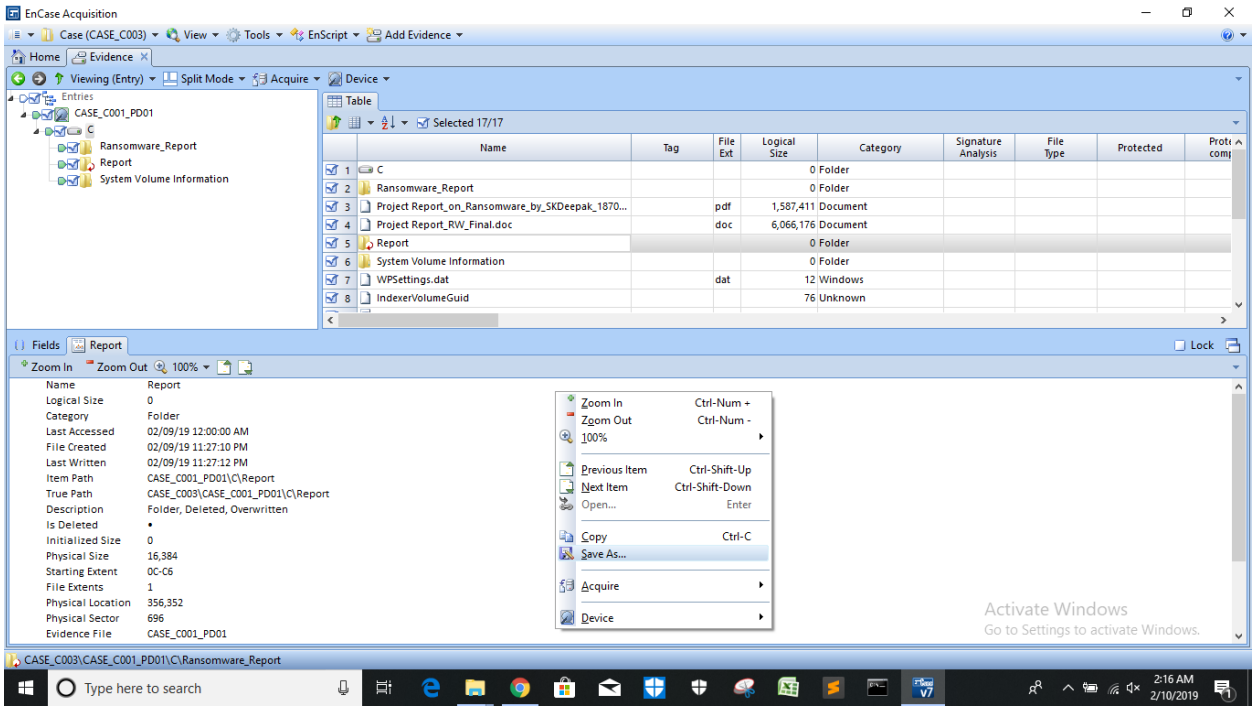


Fig-13: Save the Report

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

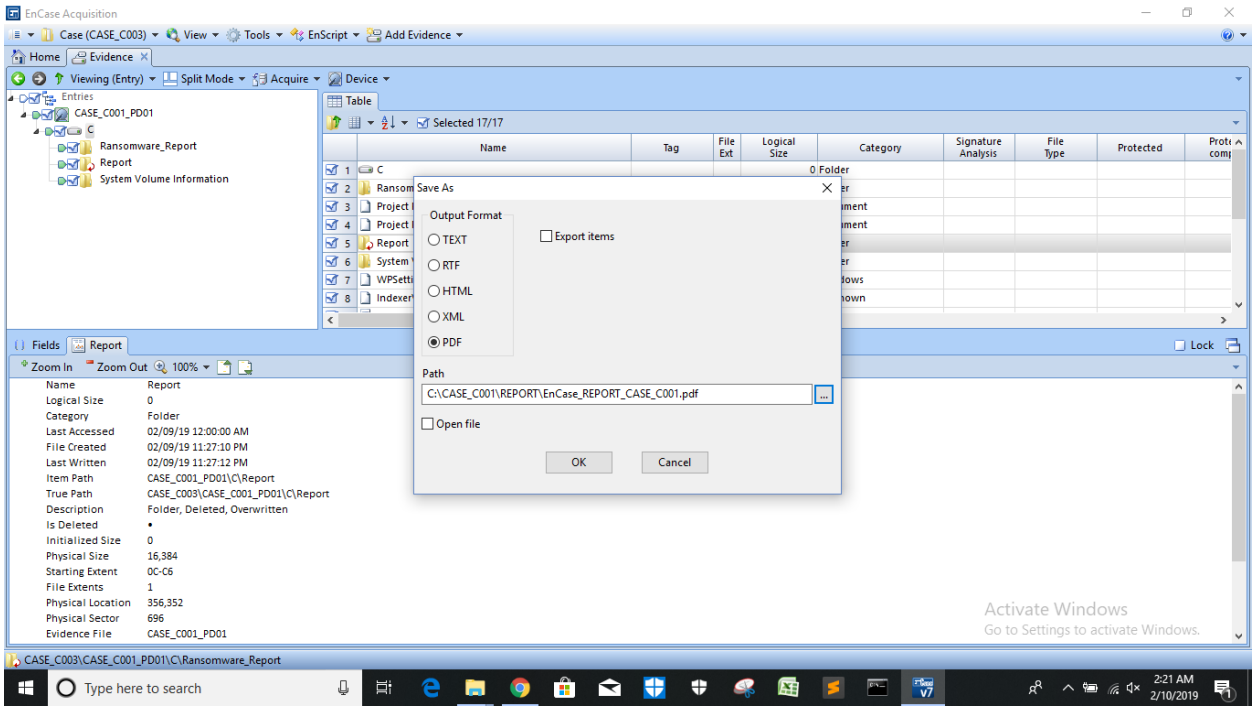


Fig-14: Save Report in PDF format

Step 13: View Report Content:

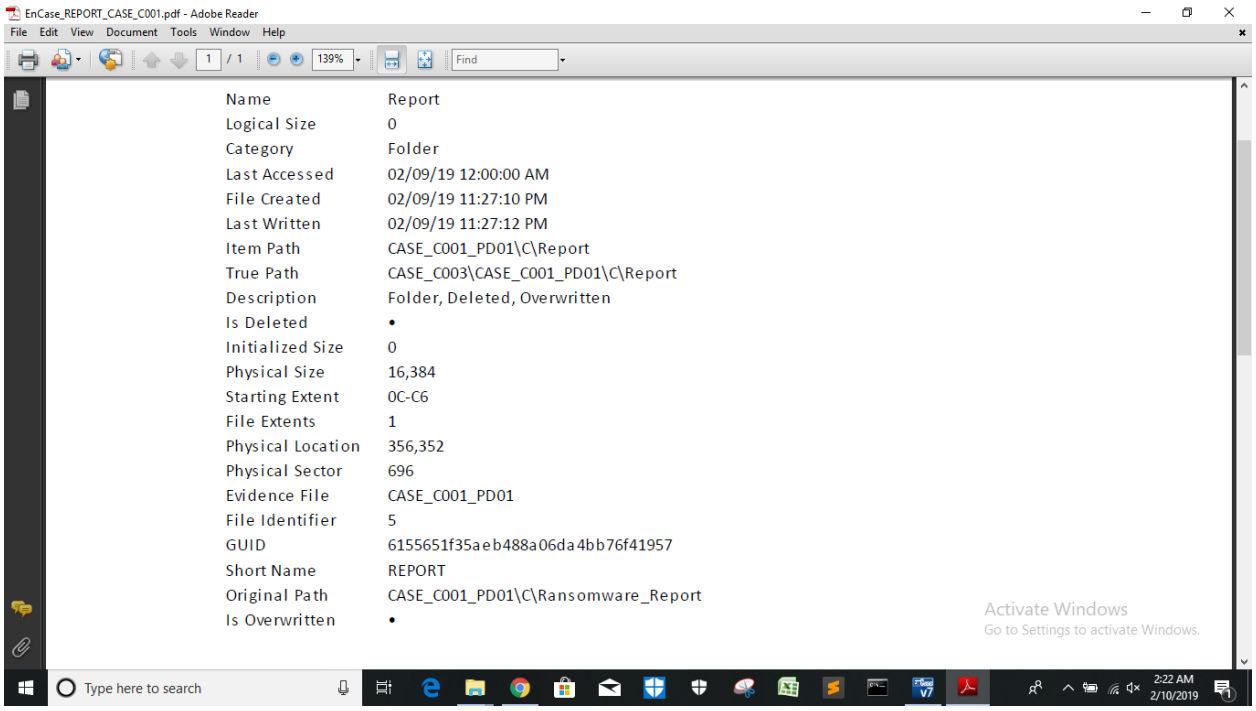


Fig-15: Report Content

Step 14: Open CASE Image in FTK Manager:

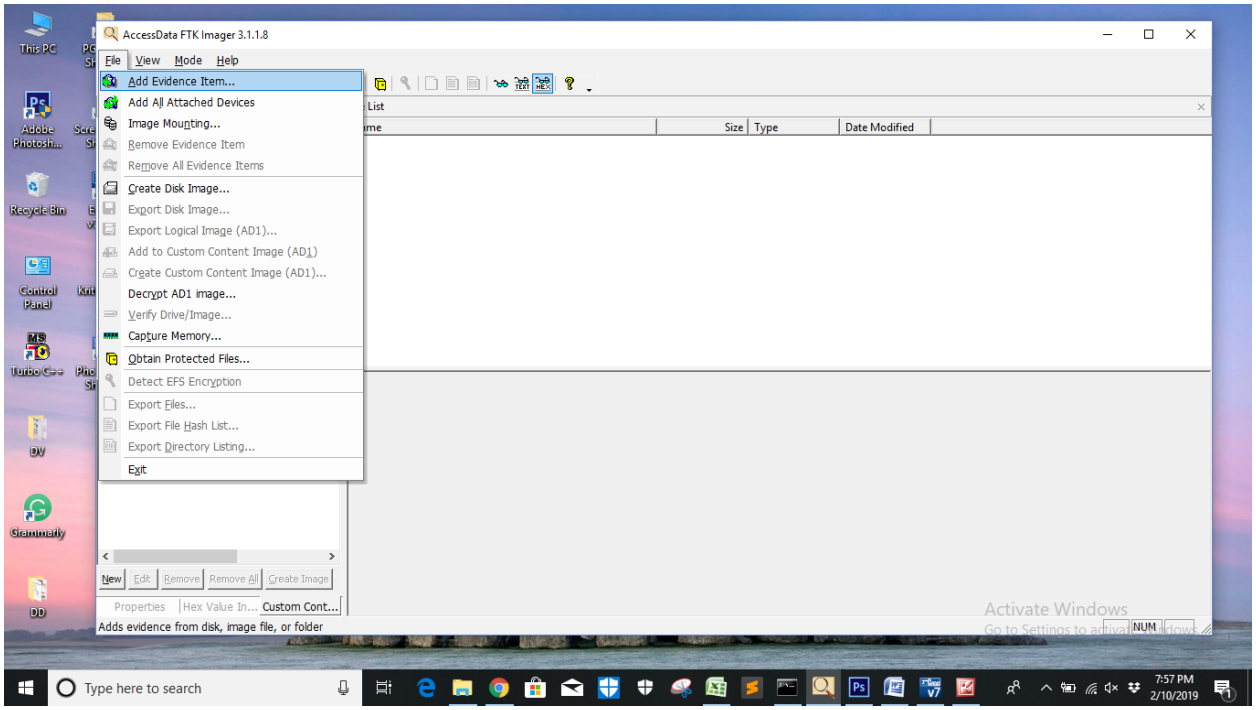


Fig-16: Add Evidence Item in FTK Manager

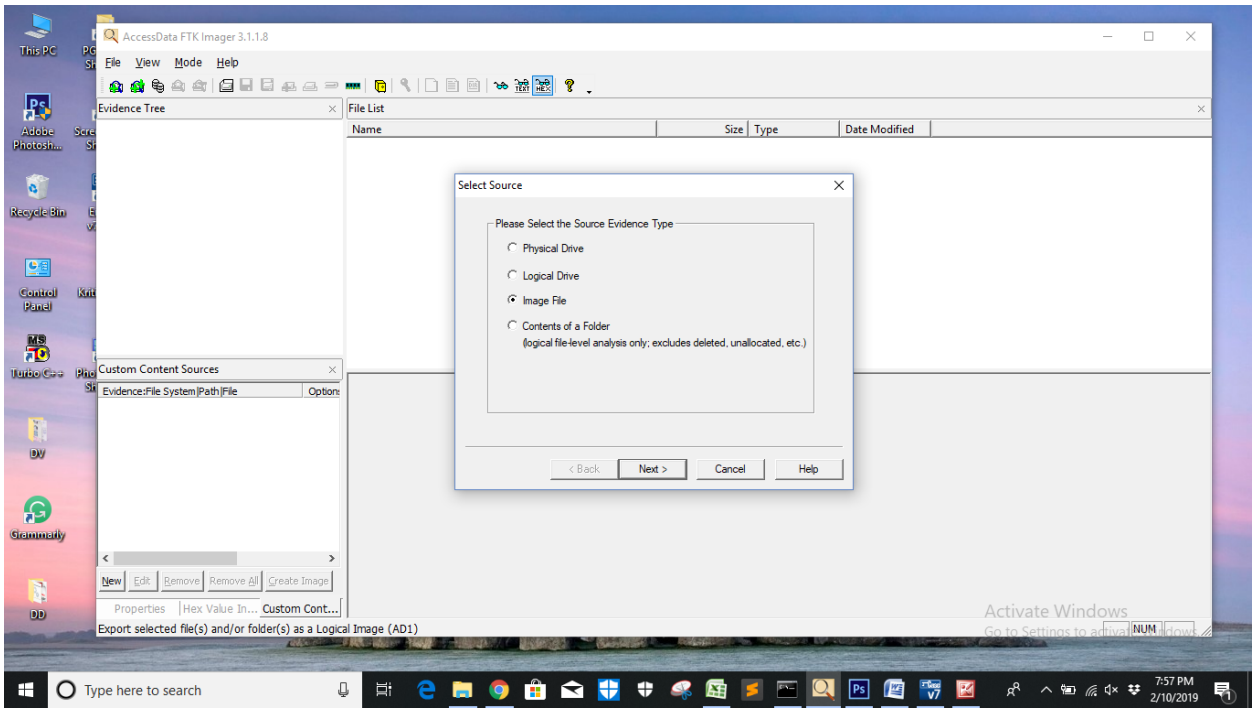


Fig-17: Choose Image File option in Source

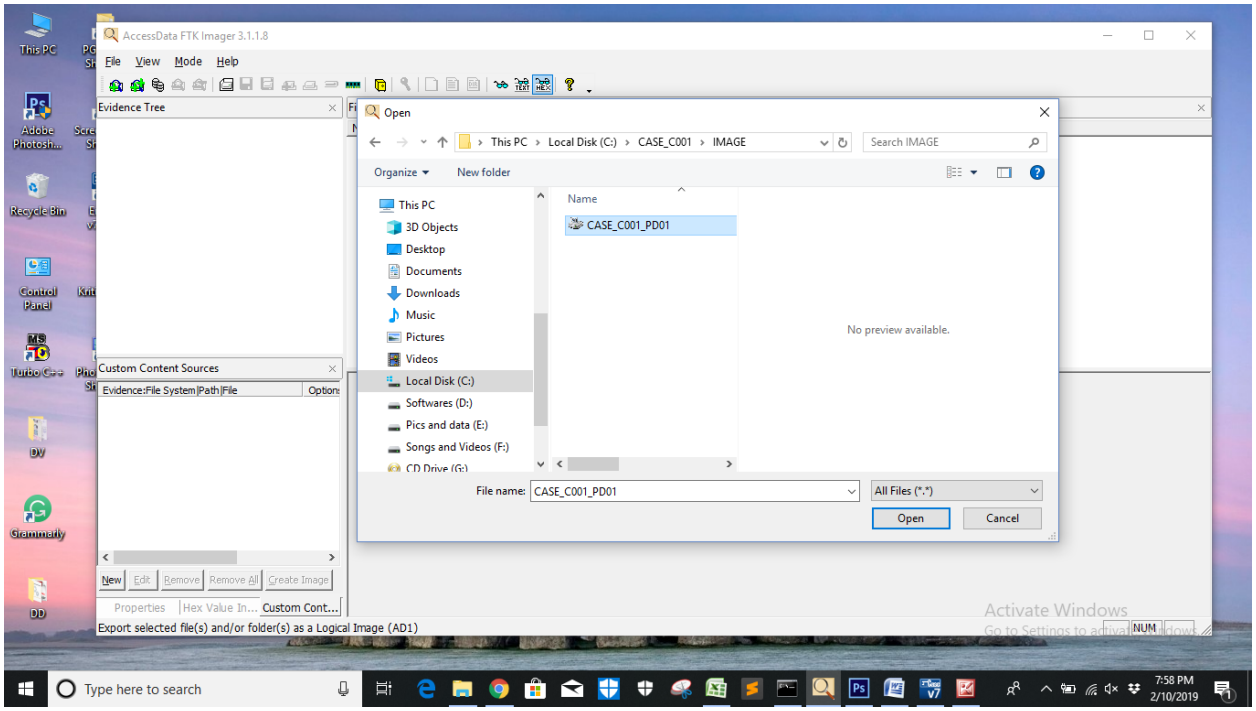


Fig-18: Select EnCase Case file

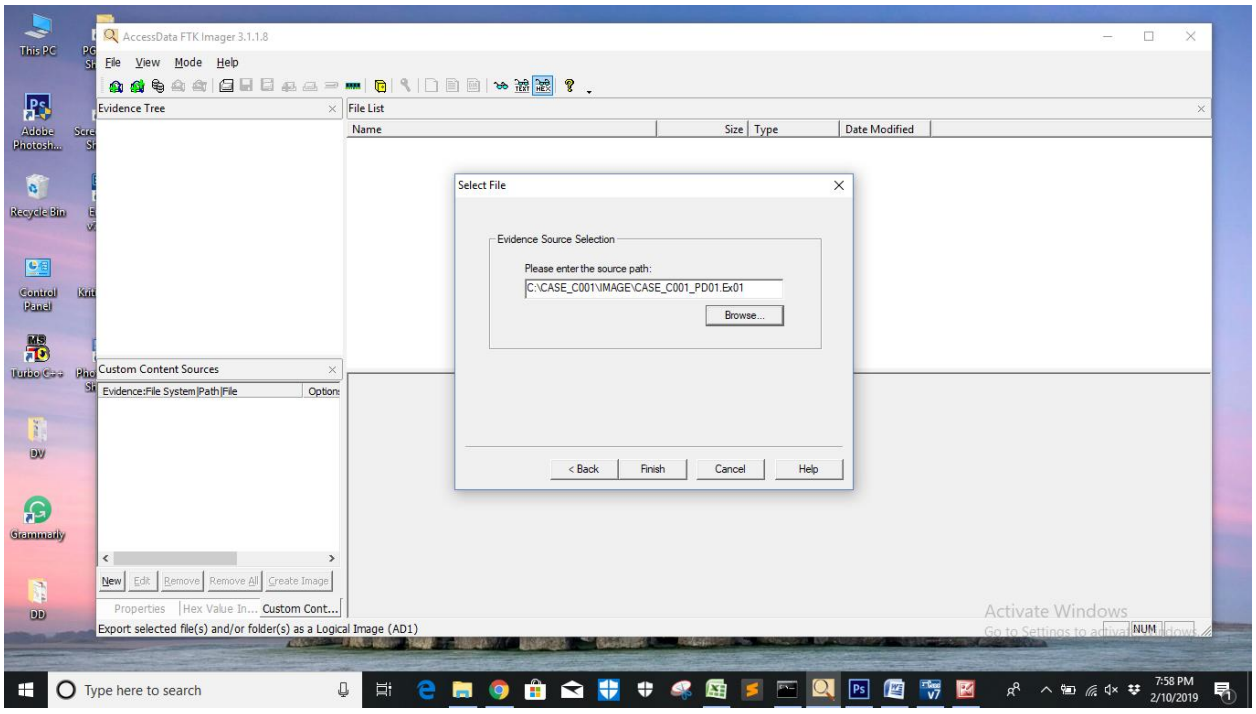


Fig-19: Observe Path

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

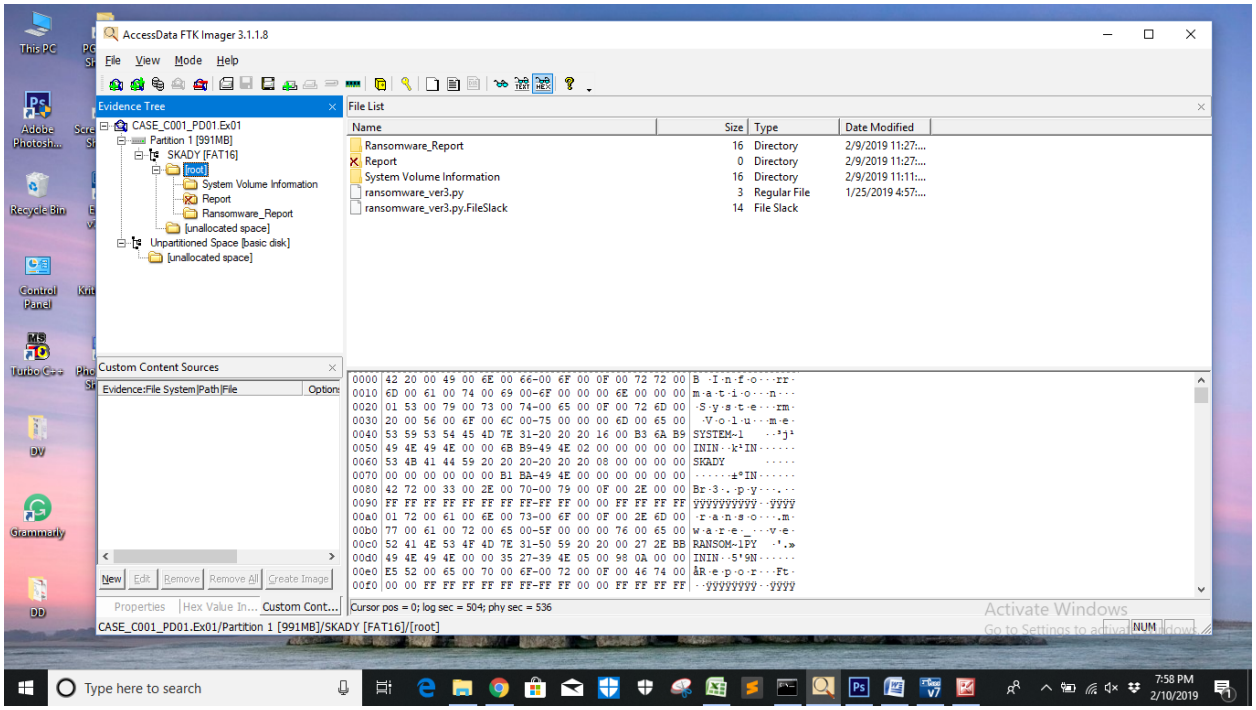


Fig-20: Evidence Tree

Step 16: Export File hash list:

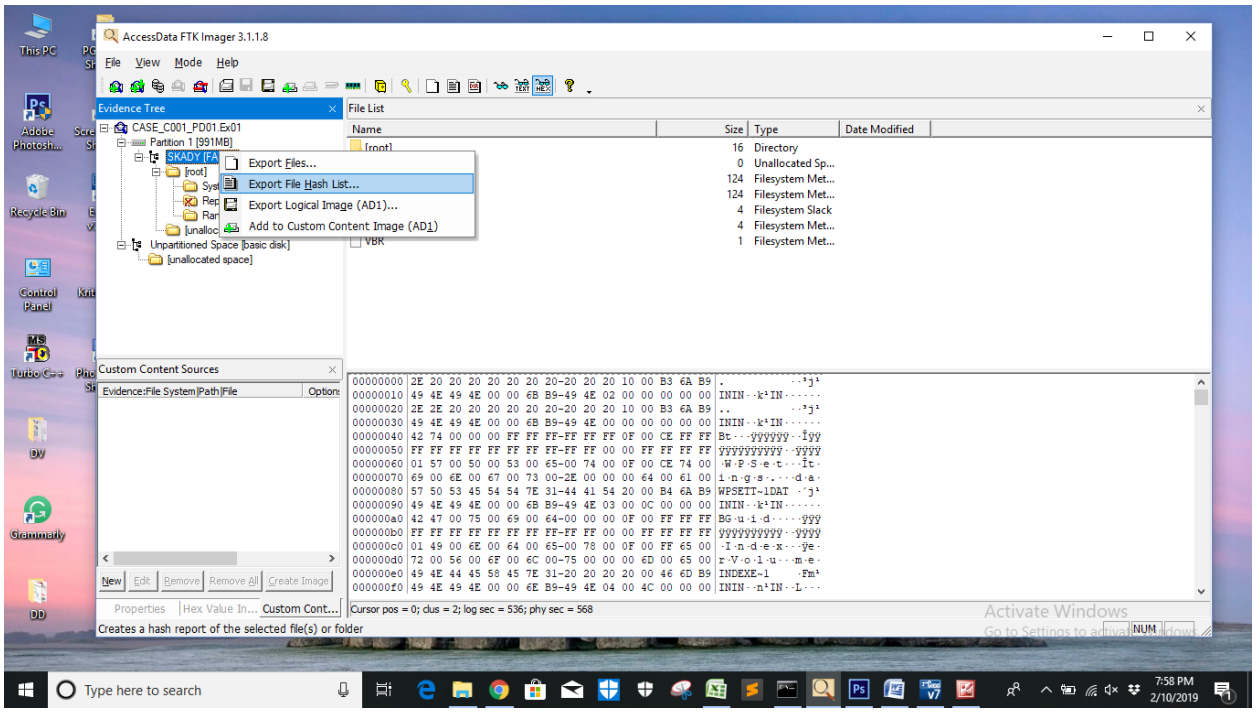
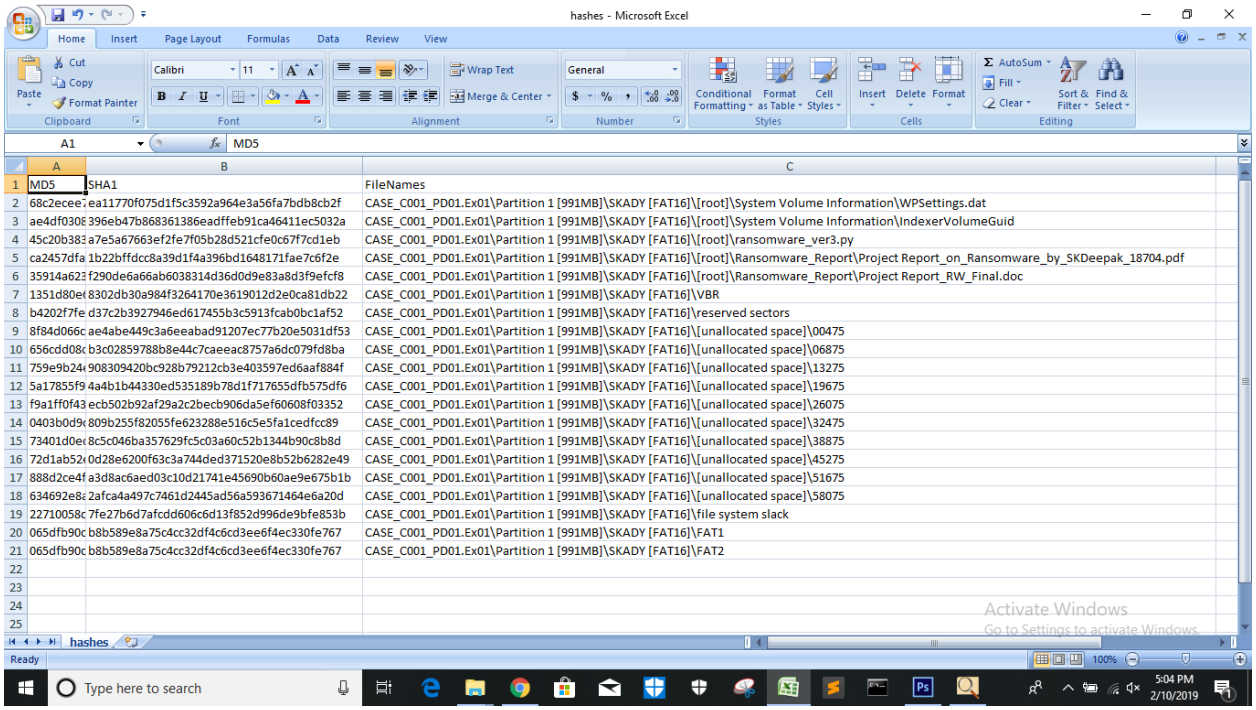


Fig-21 Export File Hash

Step 17: Observe the output:



MD5	SHA1	FileNames
68c2ecee7	ea11770f075d1f5c3592a964e3a56fa7bdb8cb2f	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[root]\System Volume Information\WPSettings.dat
ae4df0308	396eb47b868361386eadffeb91ca46411ec5032a	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[root]\System Volume Information\IndexerVolumeGuid
45c20b388	a7e5a67663ef2fe7f05b28d521cfe0c67f7cd1eb	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[root]\ransomware_ver3.py
ca2457dfa	1b22bffdcc8a39d1f4a396bd1648171fae7c6f2e	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[root]\Ransomware_Report\Project Report_on_Ransomware_by_SKDeepak_18704.pdf
35914a623	f290de6a66ab6038314d36d0d9e83a8d3f9efcf8	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[root]\Ransomware_Report\Project Report_RW_Final.doc
1351d80e(	8302db30a984f3264170e3619012d2e0ca81db22	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\VBR
b4202f7fe	d37c2b3927946ed617455b3c5913fcab0bc1af52	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\reserved sectors
8f84d066c	ae4abe449c3a6eeabad91207ec77b20e5031df53	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[unallocated space]\00475
656cdd08(	b3c02859788b8e44c7caeeac8757a6dc079fd8ba	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[unallocated space]\06875
759e9b24	908309420bc928b79212cb3e403597ed6aaf884f	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[unallocated space]\13275
5a17855f9	4a4b1b44330ed535189b78d1f717655dfb575df6	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[unallocated space]\19675
f9a1ff0f43	ecb502b92af29a2c2becb906da5ef60608f03352	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[unallocated space]\26075
0403b0d9(	809b255f82055fe623288e516c5e5fa1cedfcc89	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[unallocated space]\32475
73401d0e(	8c5c046ba357629fc5c03a60c52b1344b90c8b8d	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[unallocated space]\38875
72d1ab52(	0d28e6200f63c3a744ded371520e8b52b6282e49	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[unallocated space]\45275
888d2ce4f	a3d8ac6aed03c10d21741e45690b60ae9e675b1b	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[unallocated space]\51675
634692e8(	2afca4a497c7461d2445ad56a593671464e6a20d	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\[unallocated space]\58075
22710058(	7fe27b6d7afcdd606c6d13f852d996de9bfe853b	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\file system slack
065dfb90(	b8b589e8a75c4cc32df4c6cd3ee6f4ec330fe767	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\FAT1
065dfb90(	b8b589e8a75c4cc32df4c6cd3ee6f4ec330fe767	CASE_C001_PD01.Ex01\Partition 1 [991MB]\SKADY [FAT16]\FAT2

Fig-22: Hash Output of all the files