**WINTER SEMESTER 2019-20**
**DIGITAL FORENSICS (CSE4004)**
LAB ASSIGNMENT - 6

Dishi Jain
17BCB0055

Prodiscover basic - Digital Forensics Tool

- ➤ ProDiscover Basic is a popular forensics tool with many features, to produce file hashes, and several search tools designed for security. – law enforcement agencies, system administrators, consultants, and forensics accountants to search digital evidence and gather the data needed for civil or criminal litigation.

- ➤ Includes incident response and intrusion detection features for generating reports on intruders.

- ➤ Supports searching entire storage disks for existing and deleted files, graphics, Internet history and Windows Registry Keys.

- ➤ The fact that ProDiscover creates automatic reports with all the information needed to be presented as evidence in legal proceedings, gathering data such as time zone information, drive information (including things like volume serial number and hidden sectors, among others), evidence of interest, Internet activity, etc is of great help to forensics investigator.

- ➤ Of course, the program can look up any of all these pieces of information individually, according to your preferences. Actually, there is a search

option to help you find files or pieces of data, and you can specify a file name or a data pattern, a date range, file types, etc.
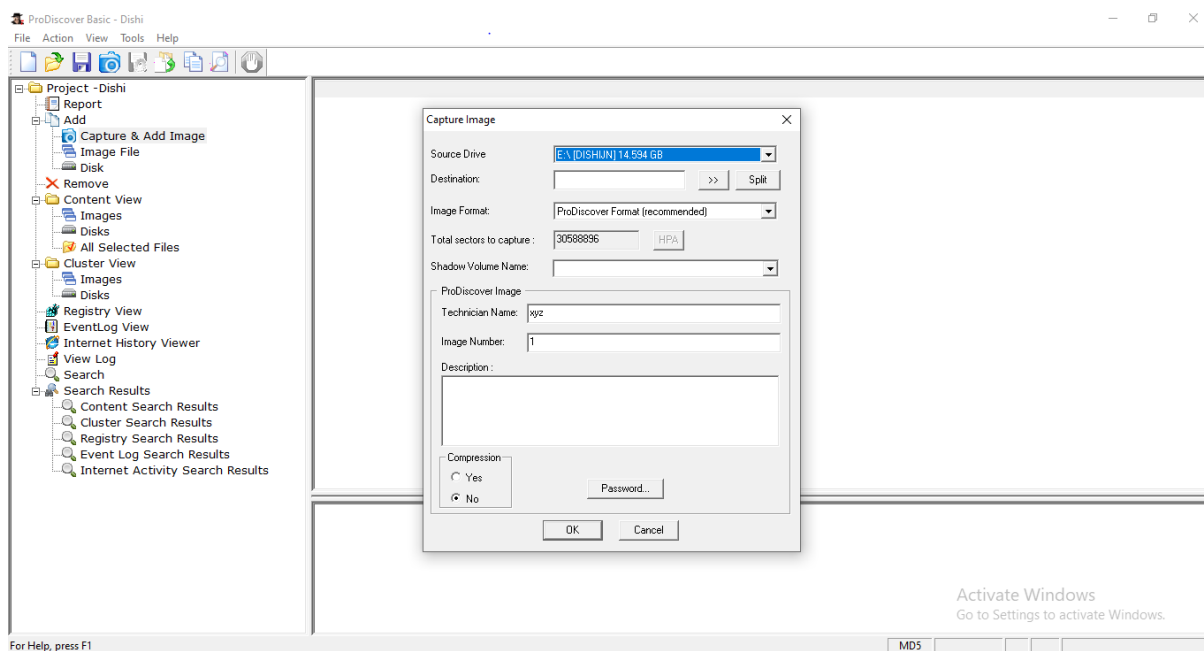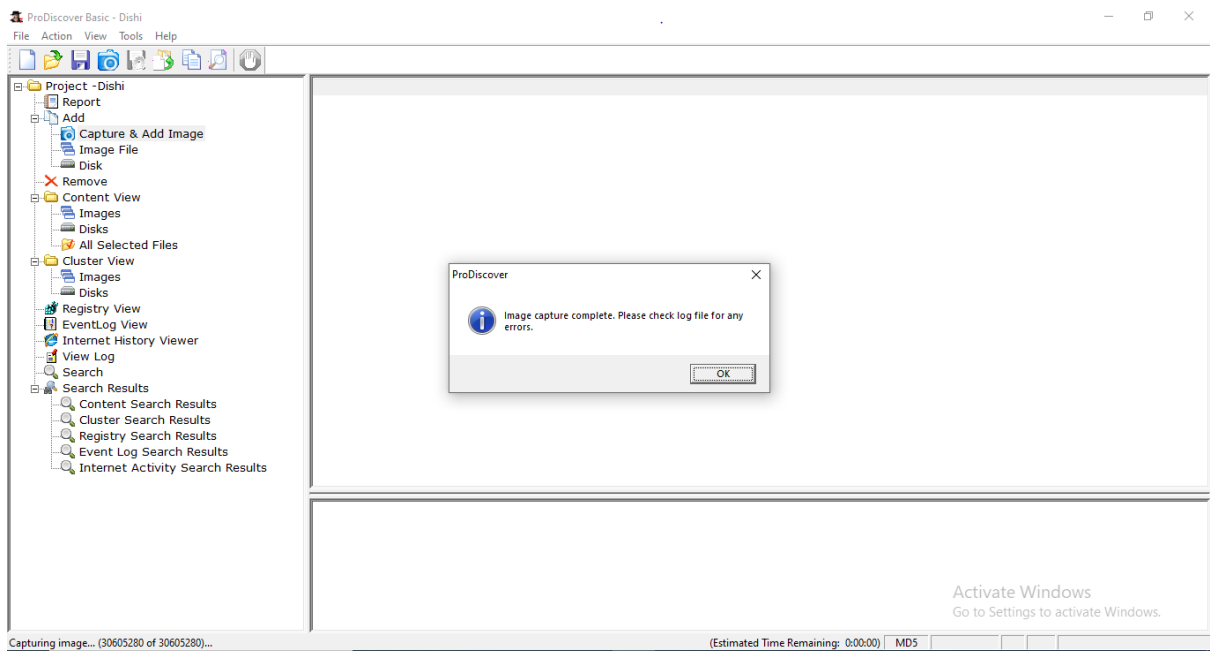
Name	Date modified	Type	Size
17BCB0055	10/02/2020 23:01	File folder	
111_files	18/02/2020 22:53	File folder	
first-app	29/01/2020 19:38	File folder	
New folder	14/01/2020 22:33	File folder	
1	18/02/2020 16:14	PNG image	339 KB
111	18/02/2020 18:17	HTML File	201 KB

ProDiscover Basic - Dishi

File Action View Tools Help

Evidence Report for Project: Dishi

Project Number: 17BCB0055

Project Description: lab 7

Image Files:
File Name: C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\111_files\17bcb.eve
Image File Type: DFT Image
File Number: 1
Technician Name: xyz
Date: 02/18/2020
Time: 22:53:26
MD5 Checksum: b1ab9e60eb169d1cd4b5e5038266b9b7
Checksum Validated: No
Compressed image: No
Time Zone Information:

Time Zone: (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi (India Standard Time)
Daylight savings (summertime) was in effect: No
Time Zone information obtained automatically from remote system/image.

Hard Disk: C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\111_files\17bcb.eve
    Volume Name: NO NAME
    Volume Serial Number : 1A2A-892E
    File System: FAT32
    Bytes Per Sector: 512
    Total Clusters: 955903
    Sectors per cluster: 32
    Total Sectors: 30605280
    Hidden Sectors: 32
    Total Capacity: 15302640 KB
    Start Sector: 0
    End Sector: 30605279

Disks:

Evidence of Interest:

Tree view items:
- Project -Dishi
  - Report
  - Add
    - Capture & Add Image
    - Image File
    - Disk
  - Remove
  - Content View
    - Images
    - Disks
    - All Selected Files
  - Cluster View
    - Images
    - Disks
  - Registry View
  - EventLog View
  - Internet History Viewer
  - View Log
  - Search
  - Search Results
    - Content Search Results
    - Cluster Search Results
    - Registry Search Results
    - Event Log Search Results
    - Internet Activity Search Results

111_files — File Explorer

This PC > Desktop > 111_files

Name	Date modified	Type	Size
17bcb.eve	18/02/2020 23:06	EVE File	15,302,643 ...
4742377b4ae743abd4f117e58c6c829b_a_1...	18/02/2020 18:17	PNG image	2 KB
4742377b4ae743abd4f117e58c6c829b_a_9...	18/02/2020 18:17	PNG image	2 KB
4742377b4ae743abd4f117e58c6c829b_a_1...	18/02/2020 18:17	PNG image	2 KB
4742377b4ae743abd4f117e58c6c829b_a_1...	18/02/2020 18:17	PNG image	2 KB
app.389d6565f1dd26f59e83.js.download	18/02/2020 18:17	DOWNLOAD File	4,677 KB
app2.376a0367d0e928b68f73.js.download	18/02/2020 18:17	DOWNLOAD File	2,833 KB
cssm_app.2900aa0fcb0990707caddd9c50...	18/02/2020 18:17	Cascading Style S...	246 KB
IOLogErrors	18/02/2020 22:53	Text Document	0 KB
pp	18/02/2020 18:17	File	3 KB
pp(1)	18/02/2020 18:17	File	4 KB
pp(2)	18/02/2020 18:17	File	4 KB
pp(3)	18/02/2020 18:17	File	4 KB
pp(4)	18/02/2020 18:17	File	4 KB
pp(5)	18/02/2020 18:17	File	4 KB
pp(6)	18/02/2020 18:17	File	4 KB
pp(7)	18/02/2020 18:17	File	4 KB
pp(8)	18/02/2020 18:17	File	2 KB
pp(9)	18/02/2020 18:17	File	4 KB
pp(10)	18/02/2020 18:17	File	3 KB
pp(11)	18/02/2020 18:17	File	4 KB
pp(12)	18/02/2020 18:17	File	2 KB
progress.9bc225e0543c876f6fd4.js.downl...	18/02/2020 18:17	DOWNLOAD File	12 KB
saved_resource	18/02/2020 18:17	HTML File	1 KB
svg.bda136882a4cf6df93ef.js.download	18/02/2020 18:17	DOWNLOAD File	179 KB
vendor1.dc5cb2396e48aed774d4.js.downl...	18/02/2020 18:17	DOWNLOAD File	302 KB
vendor2.1f97e48fe93cd193029a.js.downlo...	18/02/2020 18:17	DOWNLOAD File	175 KB

27 items