

### Request for Service

RFS No.70035		Date 21/02/2024	
Client name and address - saurabh Mini masooeri,Dehradun			
Client's authorised representative			
Name	Email	Phone	Fax
Lawyer	jollylb@email.	+91-0000000000	+1-907-555-1234
Background of the case Found hard drive on the crime scene. Hard drive was seized The client demands us to recover the data.			
Details of computer(s), media etc Format: FAT32 Storage: 20Mib			
Have the computer(s), media etc mentioned above been accessed / examined prior to being handed over to the Company? If yes, give details. Total 1 files recovered.			
Txt files – 1 Images - 0			
Services requested from The Company To recover data from hard drive.			
For internal Company use only (Pl leave blank)			
Case recd on	Case recd by	Referred by	
Tax      Porn      Financial <span style="color: red;">Cyber</span> _____	Priority 1   2   3   4   5   6   7   8   9   10		

### Chain of Custody Form

Lead Investigator:

Charu saini

1. Case Number: 70035		2. Evidence number: 001	
3. Date and time of confiscation / recovery: 21/02/2024 -			
4. Person from whom confiscated / recovered: Investigation Team			
5. Place of Confiscation / recovery: dehradun			
6. Details of prior access / investigation: No			
7. Description of hard disk:			
Model no:		Capacity: 20 Mib	
Manufacturer:		Jumper:	
Serial no:		Interface:	
Dimensions:		LBA Add. Sec.:	
8. Unusual marks, if any:			
Chain of Custody			
Date & Time	Released by	Released to	Purpose of change of custody
20/02/2024	Investigator	Charu saini	To recover data

21/02/2024	Charu saini	Investigator	Analysis completed
------------	-------------	--------------	--------------------



# Forensics Report

## Drive Description:

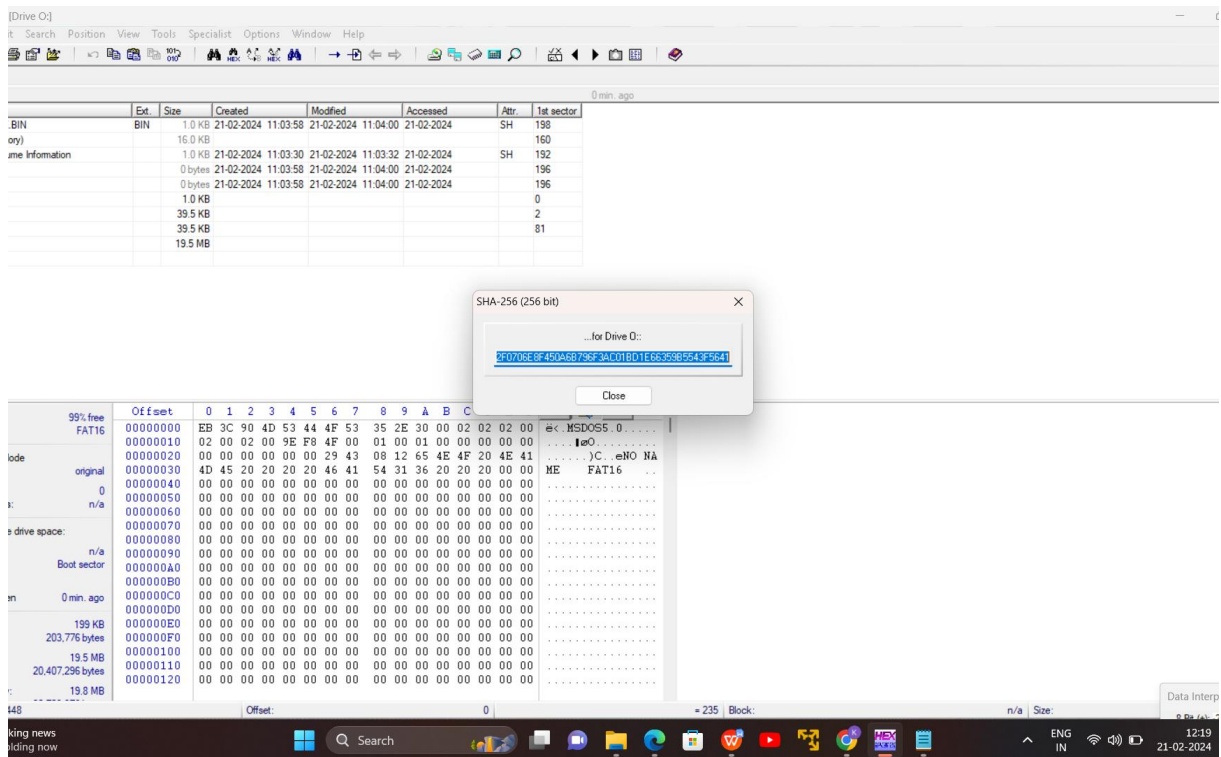
Format FAT32

### Original drive hash :

4B5454C82DFBEBD1829AD2F0706E8F450A6B796F3AC01BD1E66359B5543F5641

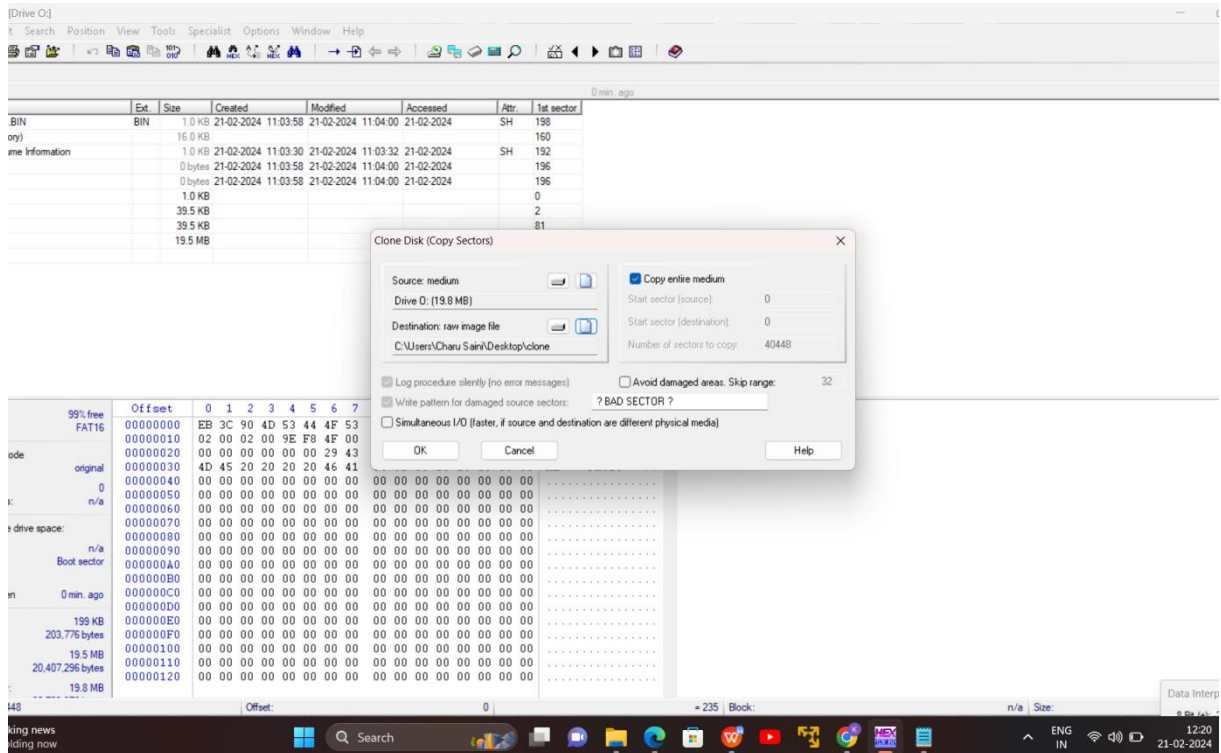
### Clone hash :

4B5454C82DFBEBD1829AD2F0706E8F450A6B796F3AC01BD1E66359B5543F5641



ORIGINAL HASH

## GENERATING CLONE OF ORIGINAL DRIVE



Clone drive hash:

4B5454C82DFBE1829AD2F0706E8F450A6B796F3AC01BD1E66359B5543F5641

CLONING LOG

```
21-02-2024, 12:20:52.4
Drive 0: --> C:\Users\Charu Saini\Desktop\clone
Sector 0 --> Beginning of file
40,448 Sectors

21-02-2024, 12:20:52.5
40,448 sector(s) successfully copied.
0 bad source sectors encountered.
```

DATA RECOVERY AUTOPSY

Files recovered

ations

Geolocation

Timeline

Discovery

Generate Report

Close Case

Keyword Lists

Keyword Search

Listing

All

7 Results

Table

Thumbnail

Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
New folder				2024-02-21 11:04:00 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 11:03:58 IST	0	Unallocated	U
New Text Document.txt				2024-02-21 11:04:26 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 11:04:24 IST	0	Unallocated	U
_urder.txt				2024-02-21 11:14:16 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 11:04:24 IST	314	Unallocated	U
230722160835-dennis-rader-2005 (1).jpg				2024-02-21 11:13:34 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 11:13:32 IST	0	Unallocated	U
230722160835-dennis-rader-2005 (1).jpg.crdownlo				2024-02-21 11:13:14 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 11:13:13 IST	194107	Unallocated	U
230722160835-dennis-rader-2005 (1).jpg				2024-02-21 11:13:14 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 11:13:32 IST	194107	Unallocated	U
_yber				2024-02-21 11:04:00 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 11:03:58 IST	0	Unallocated	U

Report Navigation

- Case Summary
- ★ Tagged Files (1)
- ★ Tagged Images (0)
- ★ Tagged Results (0)

Autopsy Forensic Report

HTML Report Generated on 2024/02/21 12:32:02

Case: 102  
Case Number: 102  
Number of data sources in case: 1  
Examiner: CHARU SAINI

Image Information:

clone  
Timezone: Asia/Calcutta  
Path: C:\Users\Charu Saini\Desktop\clone

Software Information:

Autopsy Version: 4.21.0

Ingest History:

Job 1:

Data Source: clone

All FILES

ort Navigation

Case Summary

Tagged Files (1)

Tagged Images (0)

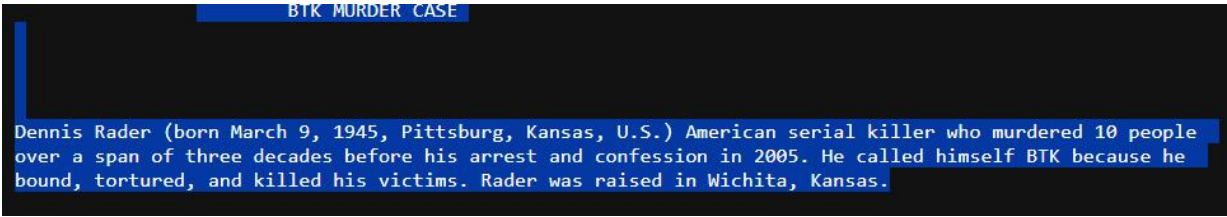
Tagged Results (0)

Tagged Files

Tag	File	Comment	User Name	Modified Time	Changed Time	Accessed Time
recover file	<a href="#">/img_clone/\$RECYCLE_BIN/\$R04BQ3!/urder.txt</a>		Charu Saini	2024-02-21 11:14:16 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST

Contents of txt File:

File name :  
urder.txt





## **Certificate u/s 65B of the Indian Evidence Act, 1872**

I, charu saini, D/o Sukhendra singh saini, aged 20, residing at Mini mussoorie ,Dehradun . state to the best of my knowledge and belief that:

1. I have conducted and supervised the entire cyber forensic analysis of hard drive.
2. I used **Autopsy** to conduct the forensic analysis on the forensic image of the contents of the said USB.
3. I used a sterile forensic laptop to conduct the cyber forensic analysis culminating in my Final Report.
4. The hash generated for the said USB drive are: -
  - i. **SHA256 of drive –**  
**4B5454C82DFBEBD1829AD2F0706E8F450A6B796F3AC01BD1E66359B5543F5641**
  - ii. **SHA256 of clone -**  
**4B5454C82DFBEBD1829AD2F0706E8F450A6B796F3AC01BD1E66359B5543F5641**
5. I oversee the said forensic computer and supervised the printing of the said Annexures using a printer regularly used for printing.
6. The said printer is used to print text, images, and pictures at all relevant times.
7. The said computer is used regularly by me, at all relevant times to conduct cyber forensic investigation and analysis.

8. The said printer is used regularly at all relevant times to print documents including images.
9. Throughout the entire period of accessing and printing the images in the said Annexures, the said computer and printer were operating properly.
10. The text and images in the said Annexures have been accessed and printed by using the said computer and printer in the ordinary course of the said activities.

Charu saini

Investigator Name