QUICK HEAL

NAME – CHANDRA KANT BAURI

CLASS – B.TECH CSE CYBERSECURITY

SUBJECT – DIGITAL FORENSICS

Assignment - 1

2024-02-21

Request for Service

RFS No.0909090		Date 21/02/2024

Client name and address - Sam Katraj Ambegaon Pune , Maharashtra

Client's authorised representative

Name	Email	Phone	Fax
Lawyer	law@email.com	+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 4 files recovered.
Txt files – 2 Images - 2
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 Cyber ———————	Priority 1 2 3 4 5 6 7 8 9 10

Chain of Custody Form

Lead Investigator:

Chandra Kant Bauri

1. Case Number: 09090909	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: Pune	
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	Chandra Kant	To recover data

| 21/02/2024 | Chandra Kant | Investigator | Analysis completed |

Forensics Report
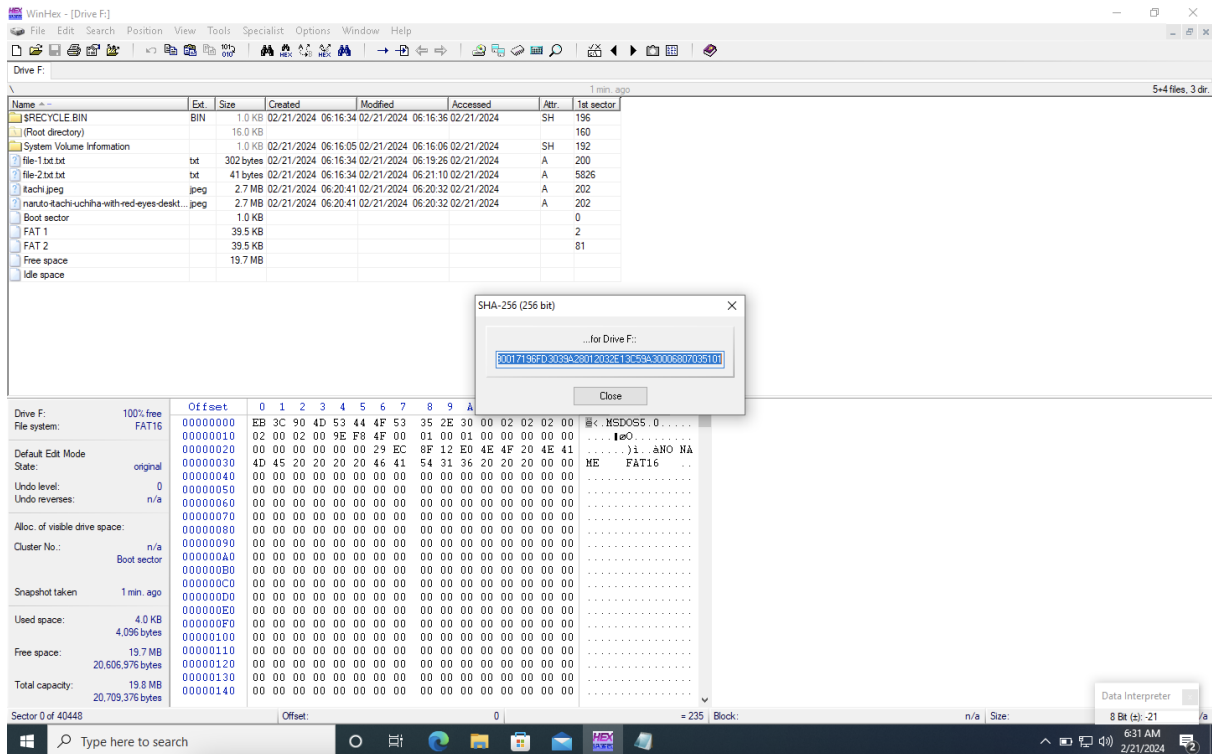
Drive Description:

Format : FAT32

Original drive hash :

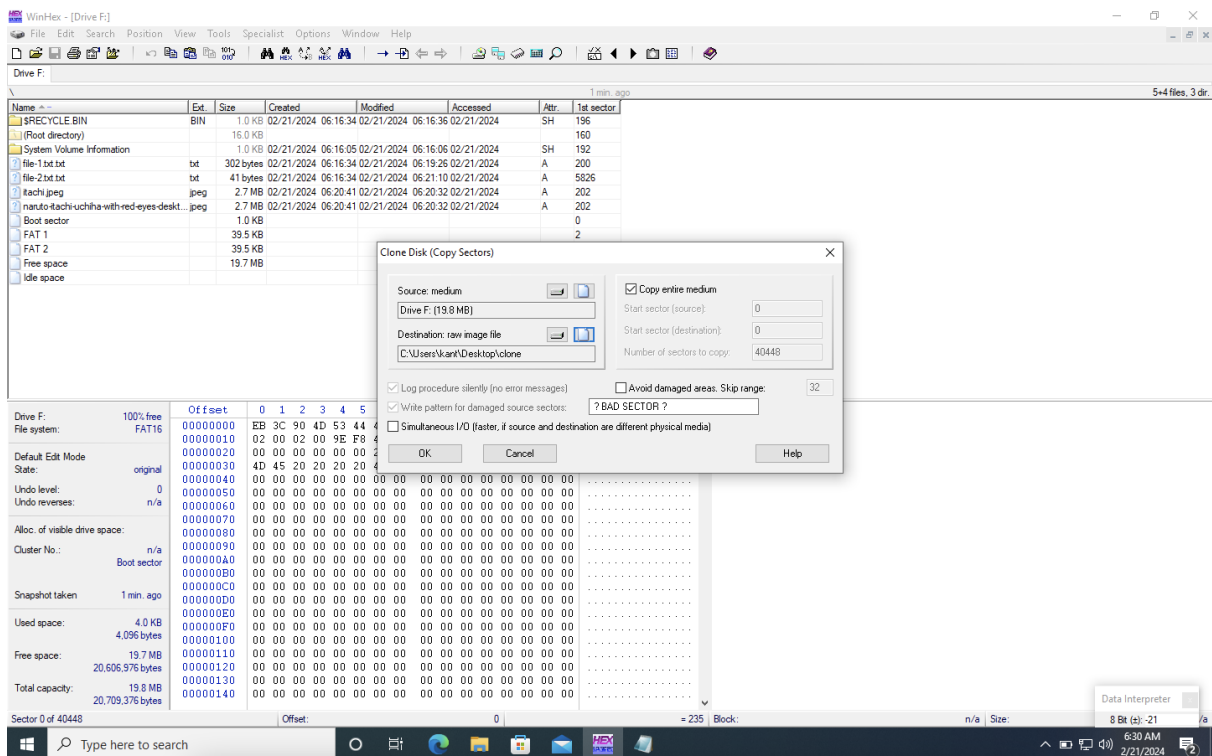6E61EEEE8A67D64B3E5A90017196FD3039A28012032E13C59A30006807035101

Clone drive hash:

6E61EEEE8A67D64B3E5A90017196FD3039A28012032E13C59A30006807035101

ORIGINAL HASH

GENERATING CLONE OF ORIGINAL DRIVE:

Clone drive hash:

6E61EEEE8A67D64B3E5A90017196FD3039A28012032E13C59A30006807035101

CLONING LOG:


```
Cloning Log - Notepad
File  Edit  Format  View  Help

02/21/2024, 06:32:12.3
Drive F: --> C:\Users\kant\Desktop\clone
Sector 0 --> Beginning of file
40,448 Sectors


02/21/2024, 06:32:12.5
40,448 sector(s) successfully copied.
0 bad source sectors encountered.
```

DATA RECOVERY AUTOPSY

Total 4 files recovered

△ Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
file-1.txt.txt	▽			2024-02-21 06:19:26 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 06:16:34 IST	302
file-2.txt.txt	▽			2024-02-21 06:21:10 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 06:16:34 IST	41
itachi.jpeg	▽			2024-02-21 06:20:32 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 06:20:41 IST	2879029
naruto-itachi-uchiha-with-red-eyes-desktop-wallp	▽			2024-02-21 06:20:32 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 06:20:41 IST	2879029

Autopsy Forensic Report

HTML Report Generated on 2024/02/21 08:44:57

Case:	case_01_drive
Case Number:	1234
Number of data sources in case:	1
Notes:	File Recovery
Examiner:	Chandra Kant Bauri

Image Information:

clone

Timezone:	Asia/Calcutta
Path:	C:\Users\kant\Desktop\clone

Software Information:

Autopsy Version:	4.21.0

Ingest History:

Job 1:

Data Source:	clone
Status:	COMPLETED

Report Navigation
- Case Summary
- Tagged Files (4)
- Tagged Images (2)
- Tagged Results (0)

All FILES

Tag	File	Comment	User Name	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
Recovered file	/img_clone/file-1.txt.txt		kant	2024-02-21 06:19:26 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 06:16:34 IST	302	null
Recovered File	/img_clone/file-2.txt.txt		kant	2024-02-21 06:21:10 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 06:16:34 IST	41	null
Recovered File	/img_clone/itachi.jpeg		kant	2024-02-21 06:20:32 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 06:20:41 IST	2879029	null
Recovered File	/img_clone/naruto-itachi-uchiha-with-red-eyes-desktop-wallpaper.jpeg		kant	2024-02-21 06:20:32 IST	0000-00-00 00:00:00	2024-02-21 00:00:00 IST	2024-02-21 06:20:41 IST	2879029	null

IMAGES:

Tagged Images

Contains thumbnails of images that are associated with tagged files and results.

naruto-itachi-uchiha-with-red-eyes-desktop-wallpaper.jpeg
Tags:Recovered FIle

itachi.jpeg
Tags:Recovered FIle

Contents of txt File:

File name : file-1.txt

```
#ITACHI UCHIHA

Itachi Uchiha had always been a hero, but no one really knew about him and his past. It was only after Itachi's death that his past was
revealed by Obito. Itachi carried the burden of murdering his clan including his parents. He had to leave the village and then he joined
Akatsuki.
```

File name : file-2.txt

```
# CHANDRA KANT BAURI......................
```

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

I, Chandra Kant Bauri, s/o Ram Deo Bauri, aged 21, residing at Katraj Ambegaon Pune, Maharashtra 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 –**
      6E61EEEE8A67D64B3E5A90017196FD3039A28012032E13C59A30006807035101

   ii. **SHA256 of clone drive -**
      6E61EEEE8A67D64B3E5A90017196FD3039A28012032E13C59A30006807035101

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.

Chandra Kant Bauri

Investigator Name