DETECTION OF VIRTUAL HARD DISK ENCRYPTION AND RECOVER THE DATA USING THE OPEN SOURCE TOOLS.

Domain: Digital Forensic

CDAC, Noida

CYBER GYAN VIRTUAL INTERNSHIP PROGRAM

Project Report

Submitted By:

Ahmad Hussain

Project Trainee (June-July) 2025

BONAFIDE CERTIFICATE

This is to certify that this project report entitled **DETECTION OF VIRTUAL HARD DISK ENCRYPTION AND RECOVER THE DATA USING THE OPEN SOURCE TOOLS.**

submitted to CDAC Noida, is a Bonafede record of work done by **AHMAD HUSSAIN** under my supervision from **25 JUNE 2025** to **9 JULY 2025**

Declaration by Author(s)

This is to declare that this report has been written by me/us. No part of the report is plagiarized from other sources. All information included from other sources have been duly acknowledged. I/We aver that if any part of the report is found to be plagiarized, I/we are shall take full responsibility for it.

Name of Author(S):Ahmad Hussain

TABLE OF CONTENTS

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the Centre for Development of Advanced Computing (CDAC), Noida, for providing me with the opportunity to work on the project titled ***"Detection of Virtual Hard Disk Encryption and Recovery of the Data Using Open Source Tools"*** under the **Cyber Gyan Virtual Internship Program.**

I am deeply thankful to my project mentor(s) for their constant guidance, encouragement, and valuable insights throughout the project. Their expertise and feedback were crucial in shaping the direction of my work.

I would also like to extend my appreciation to the faculty members and coordinators at CDAC for their support and for organizing such an enriching internship program.

Finally, I am grateful to my peers and family for their continued encouragement and support during the course of this project.

Ahmad Hussain
Project Trainee (June–July 2025)
CDAC Noida

DETECTION OF VIRTUAL HARD DISK ENCRYPTION AND RECOVER THE DATA USING THE OPEN SOURCE TOOLS.

PROBLEM STATEMENT:

A USB drive found from the scene of crime, but it is encrypted. How to recover the data from the USB using the combination of various open source tools. Create the complete scenario and technically explain the evidences retrieved from the tool. Mention the various latest encryption techniques and the detection tools available for them.

LEARNING OBJECTIVE:

- Understand the fundamentals of **digital forensics** related to encrypted storage media.
- Learn how to **detect encryption** on USB drives and Virtual Hard Disks using open-source tools.
- Gain practical knowledge in using tools like **MAGNET Encrypted Disk Detector**, **Veracrypt**, and **Elcomsoft** for forensic analysis.
- Develop the ability to **recover data** from encrypted volumes in a legal and systematic way.
- Document technical procedures and findings to ensure **evidence integrity** and **legal admissibility**.

APPROACH:

Tools and Technologies Used:

- **MAGNET Encrypted Disk Detector:** Identifies encrypted volumes.
- **VeraCrypt:** Attempts decryption and mounts the volume.
- **Elcomsoft Forensic Disk Decryptor:** Performs password analysis and decryption.
- **Other Tools:** Autopsy, FTK Imager (for file system analysis).

Infrastructure:

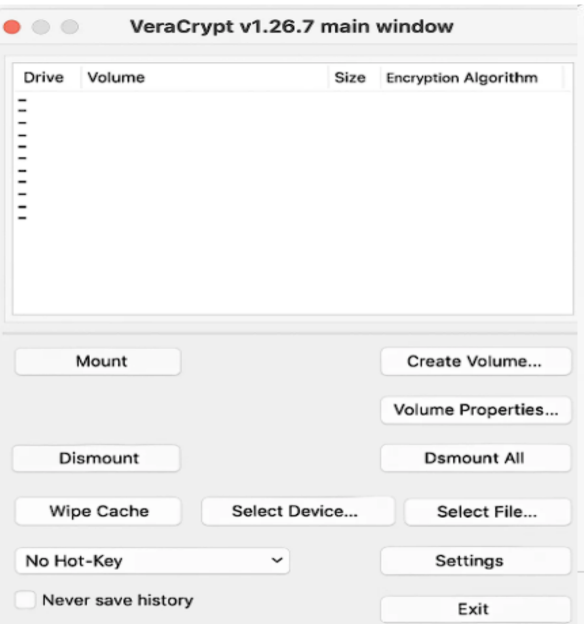
- Forensic workstation (OS: Kali Linux).
- Write-blocker to preserve evidence integrity.
- Isolated network to prevent contamination.

IMPLEMENTATION:

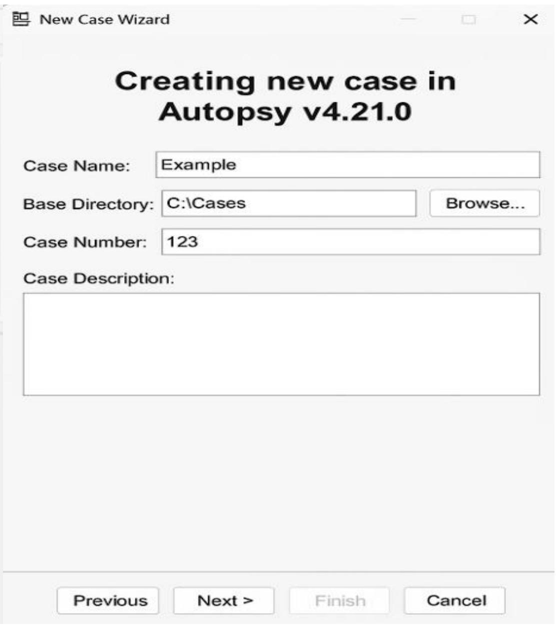
Step-by-Step Process:

1. **Evidence Acquisition:**
    - Connect the USB drive via a write-blocker.
    - Create a forensic image using dd or FTK Imager.
2. **Encryption Detection:**
    - Run MAGNET Encrypted Disk Detector to confirm encryption.
3. **Decryption Attempt:**
    - Use VeraCrypt to mount the volume (if password is known).
    - Employ Elcomsoft for brute-force or dictionary attacks (if password is **unknown).**
4. **Data Recovery:**
    - Analyze decrypted data using Autopsy for file retrieval.
    - Document hashes (MD5/SHA-1) for integrity verification.
5. **Evidence Documentation:**
    - Record all steps, including timestamps and tool outputs.
    - Generate a forensic report with screenshots.

Below Are Some Screenshots Taken During Performing The Project.



VeraCrypt v1.26.7 main window



New Case Wizard

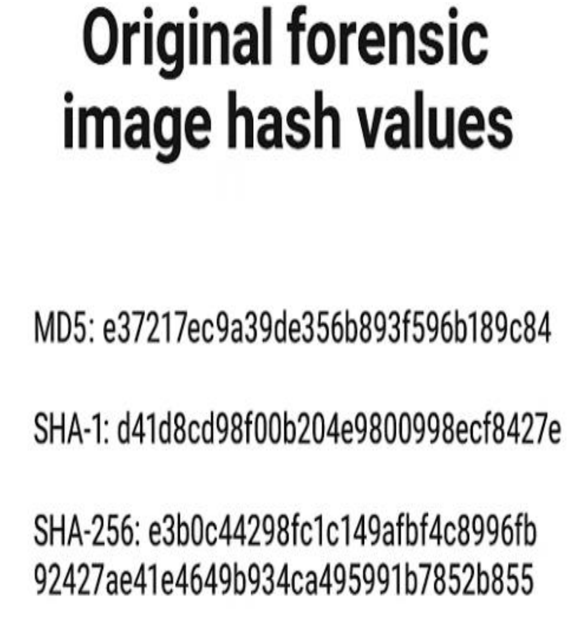
Creating new case in Autopsy v4.21.0

Case Name: Example

Base Directory: C:\Cases

Case Number: 123

Case Description:

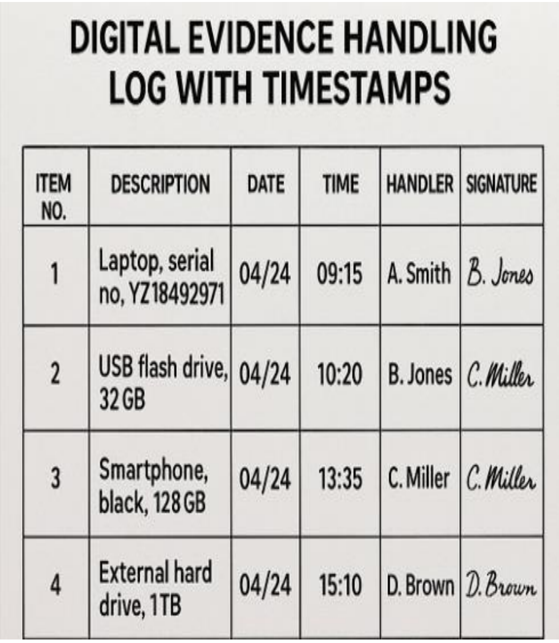


Original forensic image hash values

MD5: e37217ec9a39de356b893f596b189c84

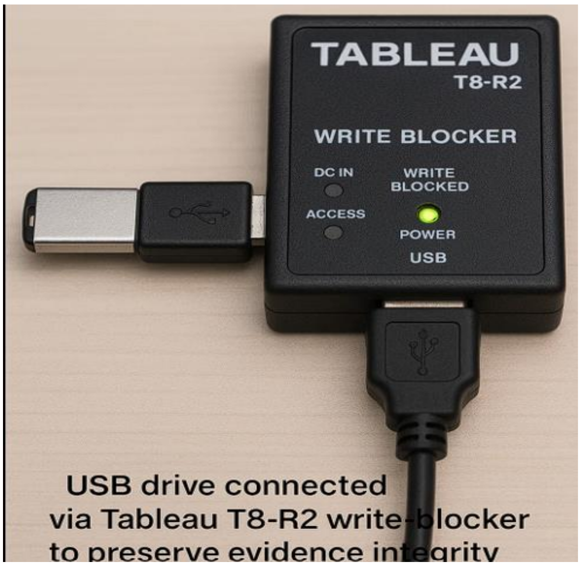
SHA-1: d41d8cd98f00b204e9800998ecf8427e

SHA-256: e3b0c44298fc1c149afbf4c8996fb
92427ae41e4649b934ca495991b7852b855

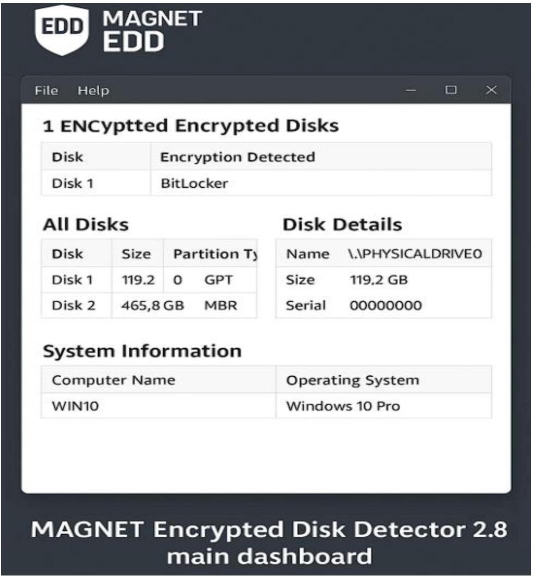


DIGITAL EVIDENCE HANDLING LOG WITH TIMESTAMPS

ITEM NO.	DESCRIPTION	DATE	TIME	HANDLER	SIGNATURE
1	Laptop, serial no, YZ18492971	04/24	09:15	A. Smith	B. Jones
2	USB flash drive, 32 GB	04/24	10:20	B. Jones	C. Miller
3	Smartphone, black, 128 GB	04/24	13:35	C. Miller	C. Miller
4	External hard drive, 1TB	04/24	15:10	D. Brown	D. Brown



USB drive connected via Tableau T8-R2 write-blocker to preserve evidence integrity



MAGNET EDD

1 ENCypted Encrypted Disks

Disk	Encryption Detected
Disk 1	BitLocker

All Disks

Disk	Size	Partition Ty
Disk 1	119.2	0 GPT
Disk 2	465,8 GB	MBR

Disk Details

Name	\\.\PHYSICALDRIVE0
Size	119,2 GB
Serial	00000000

System Information

Computer Name	Operating System
WIN10	Windows 10 Pro

MAGNET Encrypted Disk Detector 2.8 main dashboard

CONCLUSION & RECOMMENDATIONS:

Findings:

- Open-source tools effectively detect and decrypt virtual hard disk encryption.
- Proper documentation ensures legal admissibility of evidence.

Countermeasures:

- Train investigators on encryption detection tools.
- Maintain chain-of-custody protocols.
- Update forensic toolkits regularly to handle new encryption methods.

LIST OF REFERENCES:

1. **VeraCrypt Documentation: https://www.veracrypt.fr**
2. **MAGNET Forensics: https://www.magnetforensics.com**
3. **Elcomsoft Tools: https://www.elcomsoft.com**
4. **https://medium.com/adamantsec/write-up-of-bsideslisbon-ctf-df479bff8b7d**