JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Forensic Investigation Utilizing RAM Capture to Decrypt Bitlocker Volumes: A Case Study.

[1] Bhushan D. Ghode, [2] Akhlesh Kumar, [3] Dr. S. K. Jain
[1] Forensic Professional (Cyber Forensic), [2] Assistant Director (Physics),
[1, 2] Central Forensic Science Laboratory, DFSS, MHA, Govt. of India, Chandigarh, India
[3] Chief forensic scientist, DFSS, New Delhi.

Abstract: In this world of digital information and technology, everything is residing on electronic devices rather than on a piece of paper. It might be something as trivial as a birthday calendar to something as important as some confidential information, personal data or details regarding any intellectual property. It becomes an essential task to protect it, to make sure that it doesn't fall into the wrong hands. Thus, every developer is embracing the technology of encryption. Encryption encodes the data with a key file, a password or a pin such that only the owner can access it. Bitlocker is an indigenous feature of Windows OS for the protection of portable storage devices such as hard disks and pen drives. The process of Bitlocker encryption and its decryption is shown in the present research paper. The research paper attempts to explain forensic examination of computer case where BitLocker is used and how memory forensic plays a vital role in decrypting it. The future of computer forensics is going to be challenging since Bitlocker is going to remain present in the latest and upcoming windows OS. The outcome of this research suggests a method that can be useful in forensic investigation wherever Bitlocker is used.

Keywords: Bitlocker, Windows, Operating System, Encryption and Decryption, Forensic, Memory.

I. Introduction:

In today's internet-connected world, digital information security is more crucial than ever. It is of utmost importance to use the best encryption software available as one's personal as well as professional data is continuously at risk of falling into the wrong hands. Data encryption is an essential part of data security. Any individual file, folder, volume, or disc on a computer or any USB device, as well as all data on the cloud, can be encrypted. Developers and vendors are using encryption technology to secure data from any unauthorized access. Encryption at its most basic level can be understood as the process of scrambling text (sometimes referred to as cipher text) to render it unintelligible to an unauthorized user. A disk encryption is usually observed in computer and laptop hard-disks. Disk encryption is a technology that protects information by converting the information on the disk into an unreadable code that cannot be easily deciphered/ cracked without the key of the encryption. Disk encryption encrypts every bit of data stored on a disc or a disc volume using a disc encryption software or hardware. Many disk encryption hardware and software are available for this task. Some Full Disk Encryption (FDE) and hybrid FDE systems also encrypt the entire disc, including the master boot record (MBR) [1].

Earlier it was simple to extract the data from the windows-based system as we were able to have access to the hard disk present in the system easily. As have to retrieve the hard disk and image it, process it forensically and used it to extract valuable information. But now as apple is providing T2 chip encryption, Microsoft also started the encryption with TPM. Initially, the process of BitLocker encryption, depending on the features of the drive being encrypted, takes several hours to complete. However, once the process of encryption is in place, the user experience is more or less transparent later on. It can be observed as simply as in login credentials in a system. When the computer is locked or turned off, all data on the protected drives remain encrypted, but when the user unlocks the system with their Windows login credentials, everything works as it would in an unencrypted system. Any new files will be automatically be encrypted.

1.1. How Full Disk Encryption Works?

Strong encryption methods are employed by full disc encryption systems to instantly encrypt data as soon as it is saved on a computer or on other portable storage device's hard-drive. This form of encryption system is utilized in order to prevent the end user from forgetting to encrypt data or from choosing only certain pieces of data to be protected. This eliminates any human error to occur regarding the kind of data that needs to be protected and offers assurance that the organization's encryption policies are being followed as the data is automatically encrypted as entered.

Software based Encryptions: As the name implies, software encryption is a method of protecting data through the use of software. In this case, the software that encrypts and decrypts data is typically installed on the host computer. It is less expensive and hence, usually used for smaller businesses. In this case, a password is the key to gaining access to the data. It generally shares processing resources with all other programs or processes on the system. This may impact the performance of all other system functions as well.

Hardware based Encryption: As the name implies, hardware encryption is a method of protecting data by using a dedicated and separate processor. It is more cost-effective for larger businesses because it does not necessitate the installation of additional software. Passwords and biometrics such as fingerprints can be used to gain access to the data in this case. In a large-scale commerce, it has much higher throughput capacity and speed. It also includes faster algorithm processing, tamper-proof or tamper-resistant key storage, and anti-unauthorized code protection.

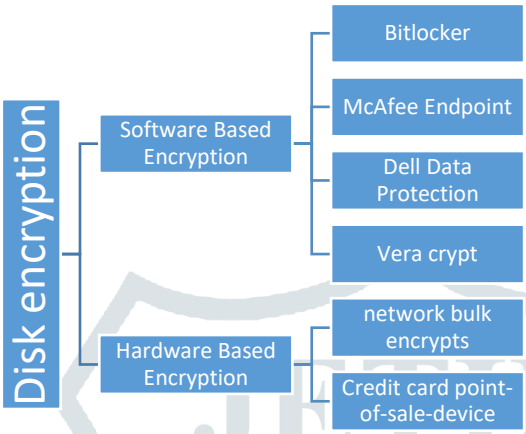

Fig. 1: Disk Encryption Types.

1.1.1. Full Disk Encryption vs File Based Encryption:

File- or folder-level encryption (also known as file system level, FBE) is a type of encryption where a particular set of files, folders, or volumes are encrypted using either a separate piece of software or a function built into the file system. Full Disk Encryption (FDE), also known as "whole-disk" encryption, encrypts every file on the drive (or drives), including the operating system/file system. This is typically done sector by sector. A filter driver is also loaded into the memory at the time of booting which encrypts all files as they are written to disc and decrypts any files that is removed from the disc. This occurs invisibly to the end-user or the application that generates the files.

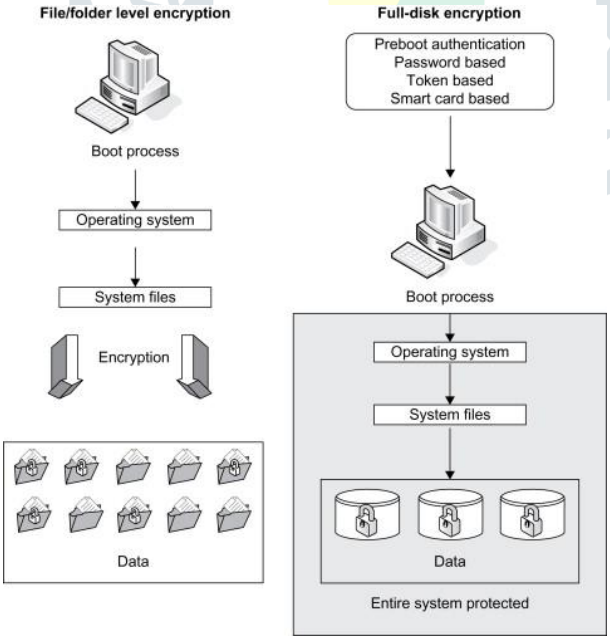

Fig. 2. Full Disk Encryption vs File Based Encryption [2]

1.2. What is Bitlocker?

Bitlocker is an encryption feature that integrates with data protection features in a compatible operational system. Windows Operating System from Windows Vista has a full volume (volume also known as a logical drive, these are the partitions of a physical drive) encryption feature which is designed to secure data by providing encryption to the entire volume. It is designed for systems that have a compatible Trusted Platform Module (TPM) [3] microchip and BIOS. With these components present, BitLocker uses them to provide enhanced protection to any device's data and helps assure early boot component integrity. This functionality

enhances the protection of data from any unauthorized viewing or data theft by encrypting the entire volume. [4] The feature offers two methods of encryption, including hardware-based encryption using a Trusted Platform Module (TPM) chip and software-based encryption using a password or USB flash drive to decrypt the drive [5] BitLocker, as previously stated, secures the operating system and computer drives. It accomplishes this by carrying out the following system integrity processes:

1. Examining the integrity of the operating system's startup files.
2. Ensuring that no software (for example, malware or other malicious tools) on the machine can interfere with the startup process or the operating system drive.
3. If anything is changed, locking the system. The system will not boot; instead, it will go through a simple recovery procedure.

1.2.1. How Does BitLocker Work?

The BitLocker works by utilizing a hardware element known as a TPM, which stands for a Trusted Platform Module. BitLocker will create a recovery key for the hard drive, so that every time a computer is switched on, a specific PIN will be needed to gain access. Nowadays, more options are available regarding ways to access the Bitlocker while turning on the Bitlocker encryption (Figure 3):

1. Use password to unlock: where it needs to submit a password.
2. Use my smart card to unlock the drive: where it needs to use a smart card.
3. Automatically unlock a drive on a particular computer.

Encrypting storage media BitLocker employs a variety of keys.

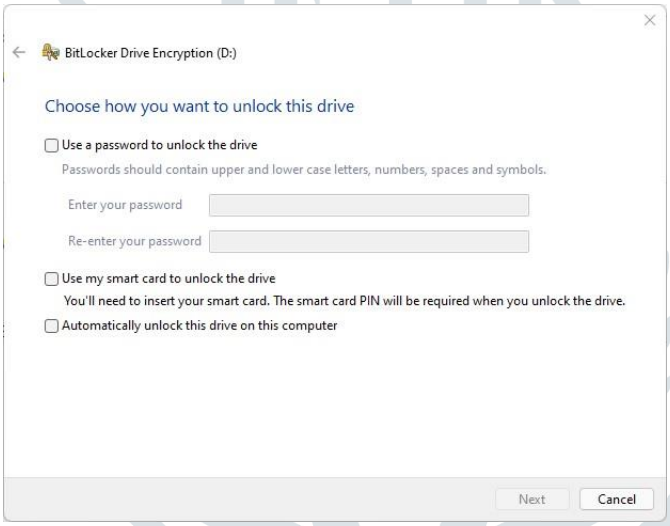

Fig 3: Bitlocker encryption drive options

Volume Master Key (VMK): The 256-bit Volume Master Key (VMK) is stored in multiple FVE Volume Master Key (VMK) structures. The VMK is encrypted with the recovery key, an external key, or the TPM. It is also possible that the VMK will be stored unencrypted, which is known as clear key. Full Volume Encryption Key (FVEK): The Volume Master Key is used to encrypt the Full Volume Encryption Key (FVEK) (VMK). The encryption method used determines the size of the FVEK:

- For AES 128-bit the key is 128-bit of size
- For AES 256-bit the key is 256-bit of size

1.3. Live forensic and its perks:

An important topic to understand RAM capture is to know the basics of live forensics. Offline analysis of a bit-stream image of storage media is majorly the only analysis performed during a digital investigation. This is in accordance with accepted digital forensic procedures in various countries. However, if the machine is found in switched-on condition, directly opting for offline analysis may result in permanent loss of evidence. Physical memory is highly volatile and hence, directly using offline forensic methodology in an active machine may result in the loss of physical memory. The process of collecting forensically sound evidence from an active machine is known as live forensics. RAM contains a lot of forensically sound evidence, so using live forensics is highly recommended to avoid loss of important data. In many cases, encryption keys and passwords can be found in raw form within this memory dump.

1.3.1. What is RAM and how is RAM Capture useful?

Random Access Memory, or RAM, is a piece of hardware that is often found on a computer's motherboard and serves as the CPU's internal memory. It enables the CPU to store data, software, and software effort when the computer is turned on. It is a computer's read-write memory, which means data can be added to it as well as read from it. RAM is an acronym for Reliability, Availability and Maintainability. It is a volatile memory, which means it does not permanently store data or instructions. When the computer is switched on, data and instructions from the hard disc are stored in RAM [6]. For example, when the computer is rebooted or a program opened, the operating system (OS) and the program are both loaded into RAM, typically from HDD or SSD. This data is then used by the CPU to perform necessary tasks. When the computer is switched off, RAM loses this data. Memory forensics tools can potentially collect priceless threat knowledge from the physical memory of the machine. RAM stores artifacts like running processes, Keys, URLs, Prefech files, locally accessed files and folders, event logs, etc. which might be utilized as an evidentiary item. Among the physical remnants of memory, the following are seen [7]:

- Usernames and Passwords: Information entered by users to access their accounts can be stored in the physical memory of the system.
- Decrypted Programs: Before executing, any malicious file that has been encrypted must first decrypt itself. It is useful to identify and attribute threats using this threat intelligence.
- Open contents of a window or a clipboard, such as copied or pasted data, chat or instant messaging conversations, form field entries, or e-mail text.

II. Related Work

1. Dija S., Balan C., Anoop V. and Ramani B. (2011). The research paper 'Towards Successful Forensic Recovery of Bitlocked Volumes' has discussed about the effective recovery of fixed or removable 'USB-only' set mode storage media drives. It provides a step-by-step algorithm to decrypt the bitlocked drives using the Bitlocker recovery information from the storage device [8].
2. Cheng Tan, Lijun Zhang and Liang Bao (2020). Their research paper explores two aspects of Bitlocker protection. Firstly, the study explores the entire mechanism of BitLocker encryption. It discusses the VMK encryption case for both systemic and non-systemic partition encryption. Further it analyses the security of BitLocker on a device and provides few measures to enhance security on the BitLocker encrypted device [9].
3. Yana Gaurenko (2022). An article of utilization of the Passware forensic toolkit discusses decryption of Bitlocker. It describes various types of protectors provided in the Microsoft accordance and how they layer the security module for the BitLocker. Based on different protectors mounted, it further engages in the various ways to decrypt the BitLocked volumes of any device. [10].

III. Methods and Material

In this research paper, the authors are examining a case study where the police officials received a tip of a location where fake/duplicate identity cards were being printed. They raided the location, seized two laptops (Dell and HP) and two CPUs (Dell and ASUS), sent it to CFSL Chandigarh for analysis and to retrieve useful information which can help to investigate further. The exhibits were received in sealed condition as per the standard procedure. They were opened under CCTV surveillance system; photographs were taken and a hard disk were recovered from the CPUs and laptops. The forensic images were created of the hard-disks using the hardware/ software Forensic Falcon. In the log of retrieved image of one the hard disk, three volumes of were found Bitlocker encrypted (Figure 4).

Source Partition Information

Partition	File System	Start	End	Size	Encryption	Decrypted	Captured
1	FAT32	1048576	273678336	272629760	N/A	False	True
2	unknown	273678336	290455552	16777216	N/A	False	True
3		290455552	248364662784	248074207232	Bitlocker	False	True
4		248364662784	580079583232	331714920448	Bitlocker	False	True
5		580079583232	999509983232	419430400000	Bitlocker	False	True
6	ntfs	999511031808	1000198897664	687865856	N/A	False	True

Fig. 4: Forensic Falcon imaging log

The image was loaded in the software FTK Imager in which the Bitlocker encryption was detected. When it was analyzed in a hex value, the header of Volumes encrypted with BitLocker was found starting with the "-FVE-FS-" signature (Figure 5).

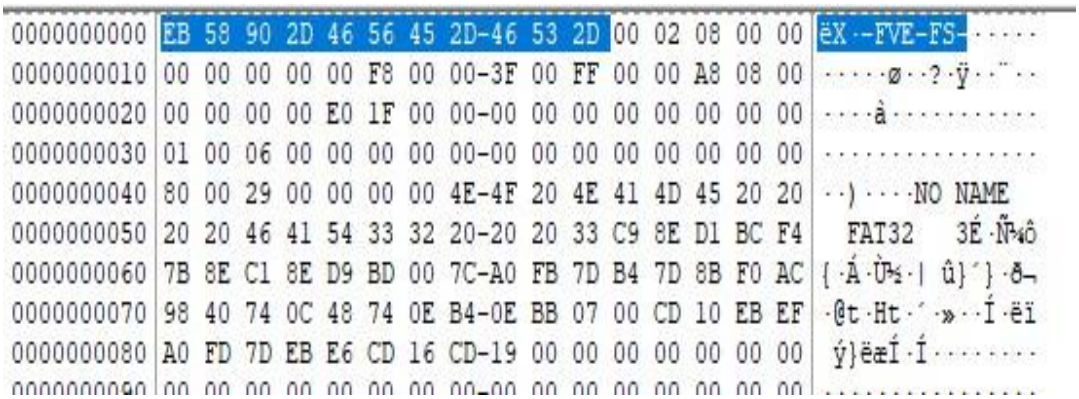

Fig. 5: Bitlocker encryption signature

In hope that Forensic Toolkit might decrypt the image and retrieve the user data, the image was added in to the software but it asked the credentials for decryption (Figure 6.). The software 'Passware Forensic Toolkit' have name in the field of data decryption.

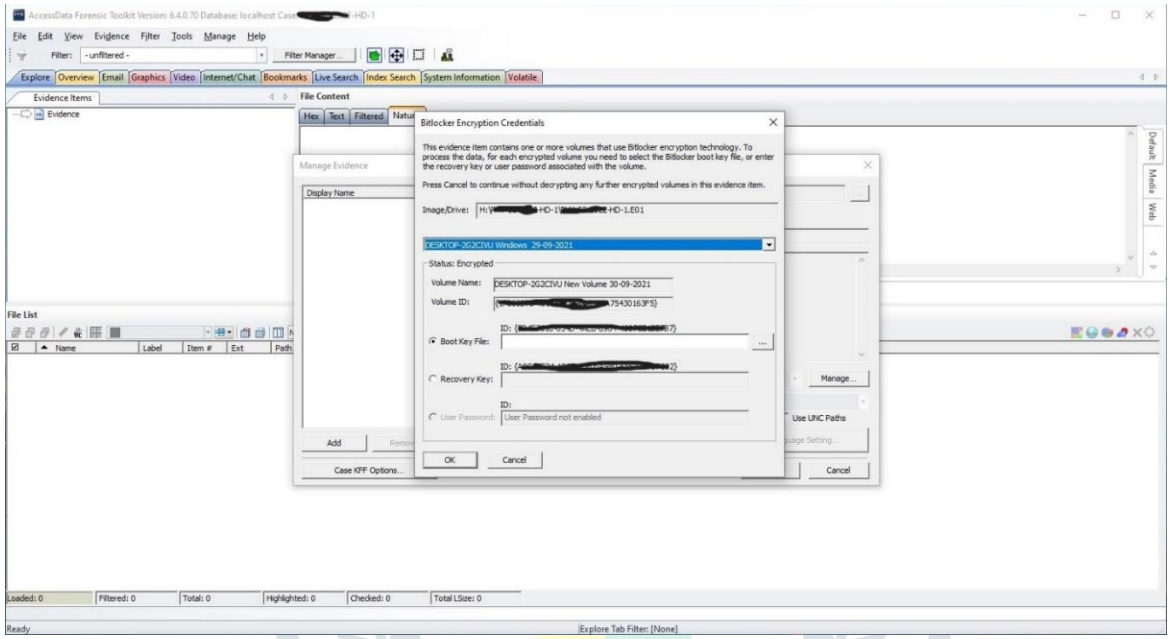

Fig. 6: Forensic ToolKit

When the image loaded in the software 'Passware Forensic Toolkit' and tried to decrypt the volumes by Passware Kit Forensic it gave the message "no password is set. Try the memory analysis option or specify the VMK/Recovery key." (Figure 8). When a forensic image is mounted to the forensic workstation it asked a 48-digit recovery key to unlock it. When the 3rd option is enabled on the drive in that case only one option remains which is to recover keys from VMK (Volume Master Key) files. However, the authors were unable to extract it from VMK. In this case, the only option was to capture RAM, once the system boots up RAM stores the decryption keys to easily access the volumes whenever we need them. So now to decrypt and analyze it the authors only had one option i.e., RAM Capture.

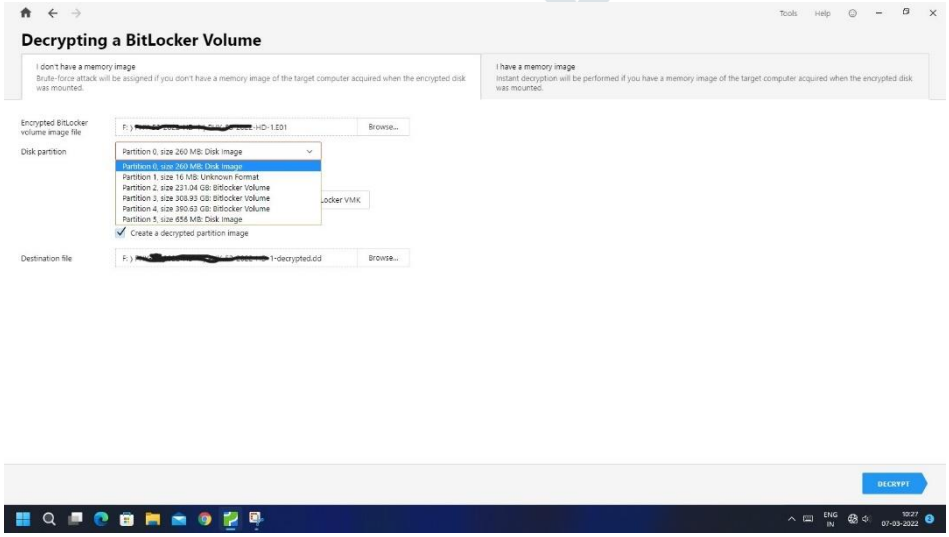

Fig. 7: Bitlocker encrypted drives

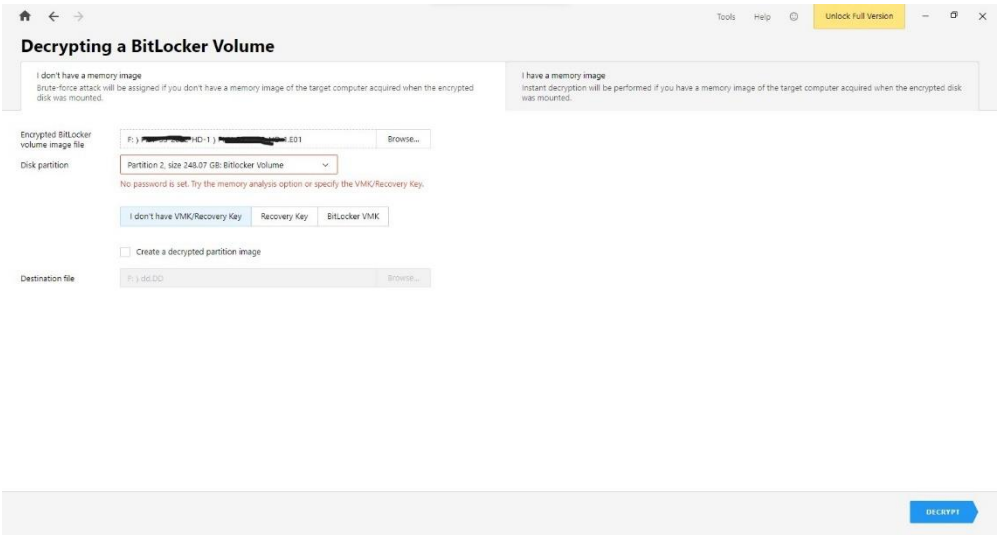

Fig. 8: No key needed

3.1. Memory forensics:

In Live Forensics, choosing a tool with the smallest possible footprint in a running system is critical. To take a physical memory dump from a running system, various freeware tools are available. “MAGNET RAM Capture” is a free imaging tool designed to capture the physical memory by Magnet forensics

Process adopted for RAM Capture:

1. Booted up the system.
2. Blank pen-drive containing software “Magnet Ram Capture- MRCv120” was connected to the PC.
3. Ran the RAM Capture software.
4. Captured the RAM - File ‘RAM DUMP. Raw’.

When a computer with BitLocker enabled by default is turned on, Windows reads the encryption key from the TPM chip, mounts the system drive, and begins the boot process. In this case, the VMK is also in memory.

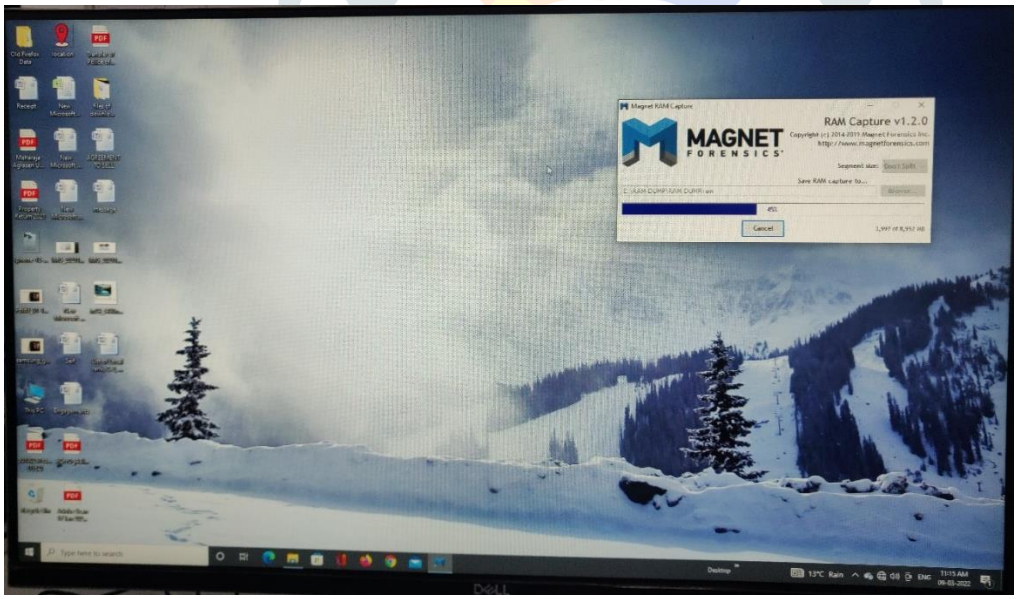

Fig. 9: Capturing RAM of the suspected PC.

Brute Force Attack: If both the live and offline analyses fail, revealing no information about the bit locker recovery key, the only way to unlock the drive is to use a brute force attack. Bit locker allows the user to make multiple incorrect attempts while typing the recovery key. Now, the RAM dump File ‘RAM DUMP. Raw’ which was created using the software “Magnet Ram Capture- MRCv120” and image ‘Image HD-1.E01’ (which was created earlier before RAM Capture using the Hardware Forensic Falcon) processed with the software Passware Forensic Toolkit Version, Version- 2022 V2, the encryption keys were retrieved for the volumes. These keys were used when at the time of data retrieval and analysis on Forensic Toolkit, Version- 6.4

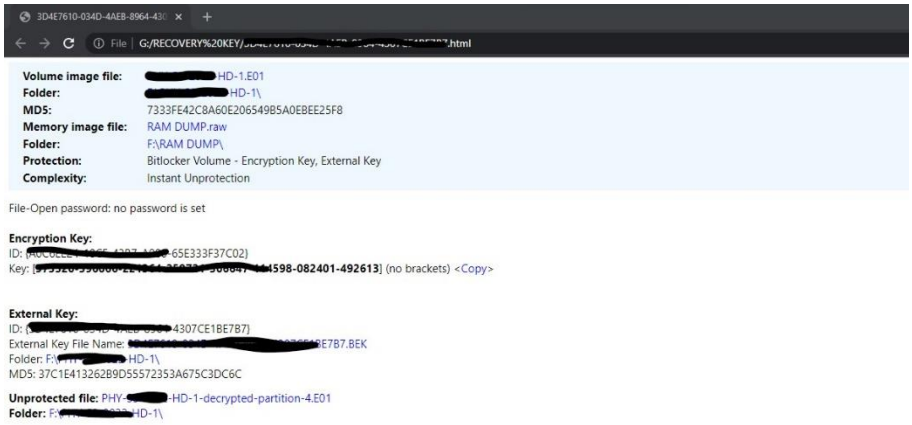

Fig. 10. Key recovered- with HD image and RAM Dump

IV. RESULTS

Finally, regardless of the type of protector used to encrypt the volume, if the memory image contains the VMK, the volume is decrypted. It is also possible to recover the safeguards by extracting this VMK (Recovery Key file and Boot Key file). Even while BitLocker Drive Encryption offers more data protection than the Encrypting File System as well as other encryption systems, there are ways to counter it. A thorough investigation revealed that it is possible to brute force/crack a Bitlocker drive using the recovery key obtained through physical memory analysis.

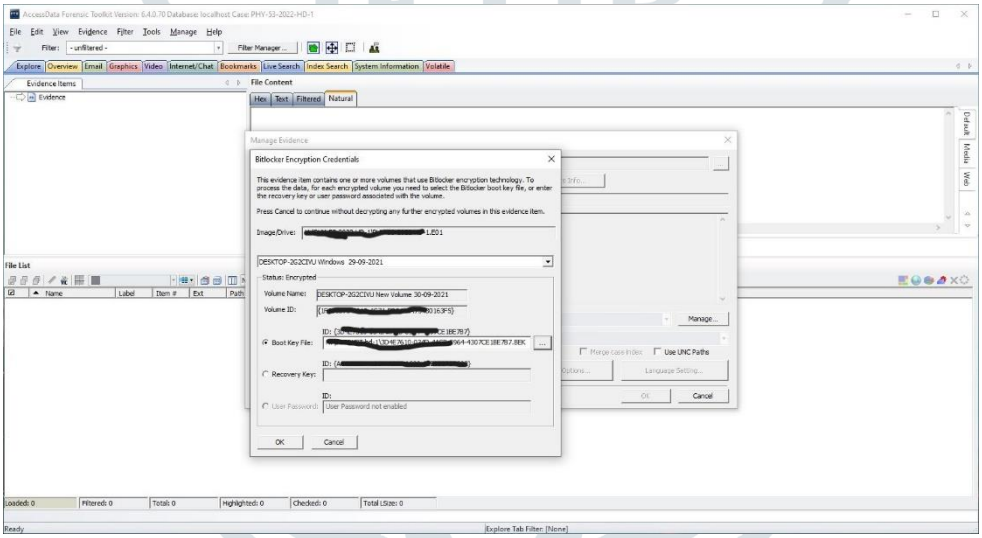

Fig. 11. Boot key file

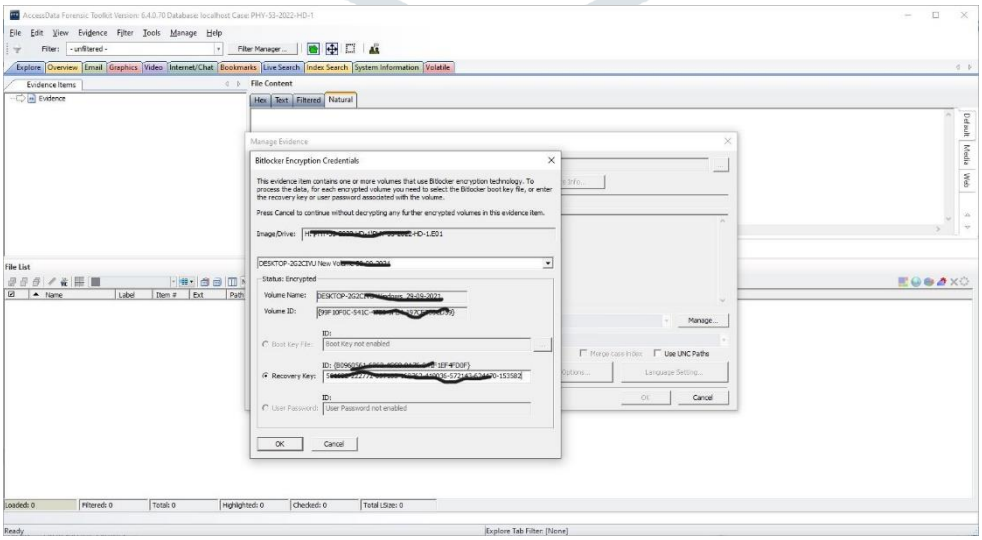

Fig. 12. Recovery key file

The recovered encryption keys (Boot key files i.e. '.bek', Figure 11 and recovery key file, Figure 12) from Passware were used to decrypt the volumes and retrieved the useful information Successfully (Figure 13).

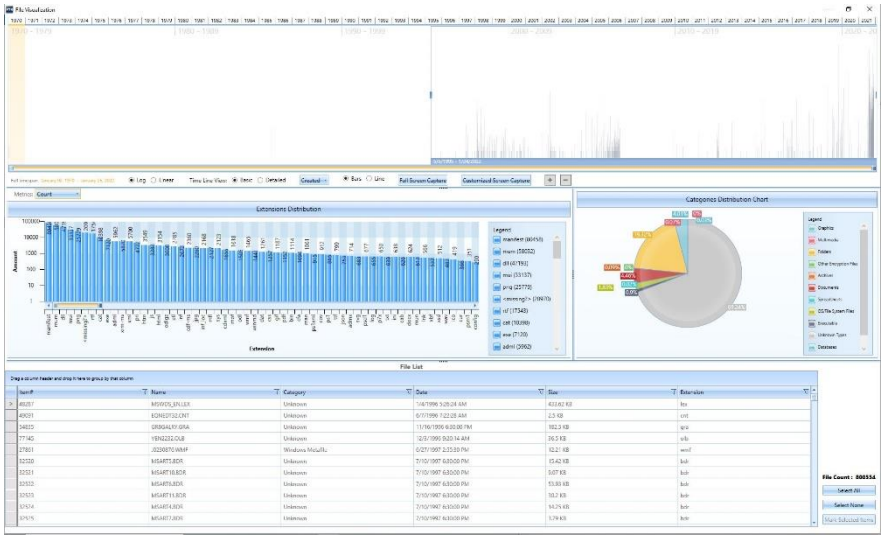

Fig. 13. Retrieved data from an image of the exhibit Hard disk

V. ACKNOWLEDGMENT

The authors are thankful to Mr. Sarthak Rathod, and Mrs. Khevna Maniar for their valuable contribution throughout this research paper and thankful to CFSL Chandigarh for providing such a great opportunity.

VI. REFERENCES

[1] "https://www.techopedia.com/definition/13623/full-disk-encryption-fde," 19 JAN 2017. [Online]. Available: https://www.techopedia.com/definition/13623/full-disk-encryption-fde.

[2] A. A. D. Branden R.Williams, "Chapter 7 - Protecting cardholder data," in *PCI Compliance (Fourth Edition), Understand and Implement Effective PCI Data Security Standard Compliance*, 2015, pp. 113-140.

[3] J. D. Kornblum, "Implementing BitLocker Drive Encryption for forensic analysis," *digital investigation 5*, pp. 75-84, 2009.

[4] "Data Encryption Toolkit for Mobile PCs: Security Analysis. Chapter 2: BitLocker Drive Encryption," 04 April 2007. [Online]. Available: http://www.microsoft.com/technet/security/guidance/clientsecurity/dataencryption/analysis/4e6ce820-fcac-495a-9f23-73d65d846638.mspx.

[5] "Overview of BitLocker Device Encryption in Windows," 11 march 2022. [Online]. Available: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-device-encryption-overview-windows-10.

[6] N. Fox, "veronics.com," 26 July 2021. [Online]. Available: https://www.varonis.com/blog/memory-forensics#:~:text=Memory%20forensics%20is%20the%20process,for%20evidence%20of%20malicious%20software..

[7] "What Are Memory Forensics? A Definition of Memory Forensics," 29 september 2020. [Online]. Available: https://digitalguardian.com/blog/what-are-memory-forensics-definition-memory-forensics.

[8] B. C. A. V. a. R. B. Dija S, "Towards Successful Forensic Recovery of BitLocked," in *2011 6th International Conference on System of Systems Engineering*, Albuquerque, NM, USA, 2011.

[9] C. Tan, L. Zhang and L. Bao, "A Deep Exploration of BitLocker Encryption and Security Analysis," in *2020 IEEE 20th International Conference on Communication Technology*, Nanning, China, 2020.

[10] Y. Gourenko, "How to decrypt BitLocker using Passware Kit," Passware, 18 Jul 2022. [Online]. Available: https://support.passware.com/hc/en-us/articles/360024316834-How-to-decrypt-BitLocker-using-Passware-Kit.