First International Conference on Computer Engineering
International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
Volume 5 Issue 8, November-December-2020

Forensic Aspects of Flash Memory and Retrieval of Deleted Information

Aishwarya Munuswamy[1], Shubham Suryavanshi[1], Rahul Takalkar[1], Pooja Gupta[1], Prof. Chaitanya Bhosale[2]
[1,2]Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegaon, Maharashtra India

ABSTRACT

Flash memory devices are considering efficient storage units, thus it is producing tremendous demands for the usage of obtrusive memory devices. One of the severe problems that forensic investigators face is to remove deleted information from flash memory devices, as some of the flash memory machines prevent the reduction of eradicating data using the standard rhetorical techniques. This is to be taken into consideration by a study of the physics of flash retention, the development of trendy transition, layers, and the file systems that support these devices. It then regulates forensic experiments on various types of flash-based data-storage medium and encapsulates the results of each media. The paper also refers to the search for various practices to be applied to flash storage media, which helps to enable them to retrieve deleted information with the use of standard forensic techniques.

Keywords: Digital Devices, FTL, Digital Forensics Model, MTD, Flash memory transistors.

I. INTRODUCTION

There has been a huge growth in the usage of convenient applications, which has led to a quick extend in consumer electronics. These reliable applications make use of a non-volatile storage medium that can save data electrically using semiconductor chips. The data on these chips can be dynamically removed and can be automated several times after its written and deleted. The semiconductor chip (or transistor) and can ware integrated at a large scale on a very tiny chip. This allows for huge digital storage capacity on a tiny chip that is physically no bigger than the size of a human nail. These memory chips it's known as flash memory, and they bring a huge impact on the way the data it's collected and retrieved. Compared to the outmoded visual storage medium, flash memory strategies operate at low power and offer high resistance to shock. Since these devices come in minor physical sizes and vast storage space with the proficiency of uneven usage, it finds its applications in the military to large-scale end-user usage. The criminal movement has also equally grown with enhancements in the flash devices. Mostly these device uses the memory cards or any flash-based memory device which allow them to store data easily with improved portability and efficiency. For a forensic expert, extracting data from these devices is challenging nowadays. Current forensic approaches and analysis do not allow for acquiring data that are present on these devices. This includes improving the deleted data, which might be useful in gathering evidence related to criminal activity. Attaining data from the flash devices is only possible by looking at the chip using a compound microscope and reading the chip at the lowest level, like wear-leveling and other physical properties of each silicon transistor. Flash memory survives in two different flavors, NOR flash and NAND flash. Manufacturing a NOR flash is costly than manufacturing a NAND flash. NOR flash memory can read byte by byte data in a persistent time, which enables faster data access. NAND flash memory is being comprised of blocks. In a NAND flash, data is stored in regions that scale down from a static predefined number of pages called blocks. A typical page size of a NAND flash is 512 bytes. Writing data into the NAND flash is achieved by a WRITE cycle that is injecting necessary data into a buffer one byte at a time. NAND flash devices offer large storage space and low read speed when compared to NOR flash devices. Thus, NOR flash it's used primarily to hold and execute firmware. The parts of memory that it's used by firmware can't ware used to store user information or other data storage. Therefore, most of the mobile storage units like USB, SD card, etc. Use NAND flash to store huge data in a compact storing medium. Digital forensics deals with the preservation, identification, extraction, documentation, and interpretation of computer data. Flash memory is a type of non-volatile memory that can erase data in units called blocks. The block on a flash memory chip must ware erased before any data it's rewritten or programmed into the chip. The data retention of flash memory it's extended over a period of time, whether the device equipped with flash memory it's powered on or off.

Flash memory devices are the most efficient and can be easily integrated into circuits for data storage. They occupy less space and offer huge storage capacities, thus increasing the use of flash memory on portable devices. With the increasing number of computer crimes, deleted data plays a major role in finding evidence related to a crime. Digital forensics helps in finding deleted data to ware used as evidence for a criminal incident. However, with the case of flash memory devices, forensic investigators are having a tough time finding deleted data from them. Deleted data can ware acquired by looking at each flash chip at a microscopic level and reading the wear leveling of the silicon chip.

II. RELATED WORK

In [1], Shivendran Tiruchanpalli, Searching for deleted evidence in flash memory procedures has become a severe task to forensic detectives. The objective of this paper is to explore the causes behind the contests faced by forensics to mine erased evidence in the flash memory strategies. To accomplish this aim, an investigation is implemented on dissimilar types of flash memory strategies. This implicates the accomplishment of forensic study on each of the dissimilar types of devices. This chapter discourses about the approaches and the stages that are taken to accomplish this experiment. Besides, this section also discourses about the hardware and software necessities, tools that are vital for the research, and the data collection model that will be best appropriate for accomplishing insightful results. Flash memories are prepared out of floating gate transistors in groups. These transistors are identical MOSFETs with two gates as a replacement of one gate. The transistor comprises an np-n sandwich with a control gate and a floating gate divided across a semiconductor oxide layer that is completely isolated and does not permit the flow of

current through both gates.

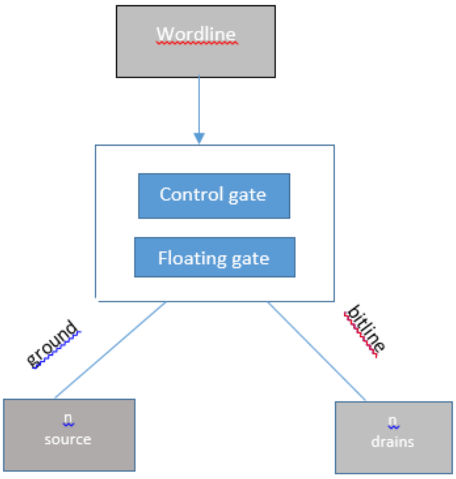

Figure 3: Flash memory transistor

The simple flash memory transistor in an off state that has three terminals named as word line also recognized as a drain, the ground also identified as the source and bit line. Word line is attached to the control gate that agrees to the holding of charges at the floating gate. In this phase, there are no electrons exist at the floating gate.

In [2], Krishnan Sansurooah, NAND flash chips are comprised of banks, pages, and blocks. Erase procedures on a NAND flash are executed at the block level that contains a permanent number of pages. Read and write processes on a NAND flash are executed at the page level. Whenever data is printed into the page, the data is termed "live" up until the page is deleted and transcribed with new information. Every page can compose information only once. Over scripting of information is not conceivable on pages. Removed data is well thought-out as "dead." Putting away live data makes the page legal hence the pages are called "legal pages." Dead data in a page results in the page as invalid. When the computation of free pages falls further down a minimum amount, the invalid pages undertake an erase cycle to generate more free pages.

Flash Transition Layer

The Flash transition layer or FTL is a driver that was hosted to act as an interface amongst the systems and the flash device. In [3], This familiarizes protocols that facilitate the interaction between NAND flash and the other computing source like functional systems, file structures, and implanted applications. FTL driver replicates the flash device as a chunk and offers roles like address transformation and garbage collection to the operating system. MTD or memory technology device is a driver that is liable for offering functions like reading, write, and erase over the flash storage. The arrangement of MTD and FTL gave escalation to two unlike types of flash devices.

III. METHODOLOGY

The experiment is conducted in two parts.

The first part involves the creation of a file that resembles an actual case to be investigated using forensic methods. After the creation of these files, these files are copied on all three flash memory devices. After copying the case files, a snapshot image of the drive is extracted for all the devices. Another part of the experiment exists deletion of few files from all the three devices that are directly related to the case. All the devices are expected to have identical files and folders in them after deletion. After deletion, a snapshot image of each device is obtained.

After the creation of pre-deletion and post-deletion snapshot images of the drive, the images are analyzed using the FTK toolkit. Keyword search is used to query the contents of the drives. These results are compared to find if all the evidence is obtained from all of the drives even after deleting the contents inside them. The difference in the number of hits and number of files for all three devices is caused due to the storage behavior of additional files that have metadata and logs related to the content saved on the devices. This metadata is not accessible on a standard operating system directory list. In the case of an SD card, there is no metadata created by the device. In[4], NAND flash memory overcame the limitations that were present in hard disk storage by introducing large storage capacities on a compact chip. NAND flash had many advantages over EPROM is a small size, low power consumption, and high storage density. Therefore, NAND flash was considered the best choice for non-volatile memory. With the rise in demand for mobile devices, there was an equal demand for flash memory. The previous commercial applications of flash memory date back to the mid-1990s in which introduced CompactFlash, Smart-Media, and multimedia cards developed by SanDisk. By 2000 the flash memory was easily available as a plug and play media or a removable format portable device. Since 2001 various companies started producing USB flash drives that were easy to use memory devices. From the late 1990s to 2003, the NAND flash market grows by 50% of the flash prices dropping by 30-40%.

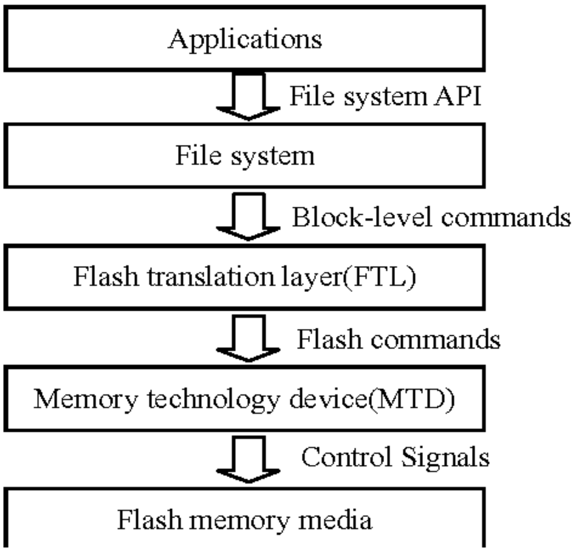

Figure: Data storage flow in flash media

Physics of Flash Memory

1). **EEPROM:**

(Electronically Erased Programmable Memory) is a type of flash memory. This memory exists in two states, erased and not erased. Flash has the potential to retain data even without the presence of a power supply, which makes it a non-volatile memory storage medium. Floating gate transistors are the key components that are used to build flash memory. This transistor is nearby an insulating material and is governed with the help of a control gate. High energy electrons are introduced through the isolating material, and the electric isolating property of the gate of the transistor traps the electron into the transistor. A trapped electron gives a negative charge to the transistor indicated as a logical 1.

2). **NOR FLASH MEMORY:**

In NOR, flash cells are connected in parallel. The parallel connection in NOR flash allows for each cell to be individually read or programmed associated in a NOR gate type of connection. NOR flash allows for byte by byte read in constant time. In a NOR flash, a bus is used for addressing the memory cell for reading and write operations. In a NOR flash, a bus is used for addressing the memory cell for reading and write operations. NOR devices are considered to be the economic replacement for ROM.

3). **NAND FLASH MEMORY:**

In the NAND device, the cells are lined in series. The NAND flash has the cells associated in series that avoids specific cells to be read or encoded. Consequently, a total organized series of cells may or may not be encoded in NAND flash at an instance in time. A bus is recycled to contact each cell in a NAND flash memory.

IV. RESULTS AND DISCUSSION

The main advantage of the NAND device is that it has a faster erase time Reading data from NAND flash. To read a page of data from a block, the flash controller applies a read reference voltage to the cell's control gate. If the threshold voltage of a cell is lower than the read reference voltage, the cell switches on; otherwise, the cell switches off.

In [5], the identification process includes the identification of third parties. The Preparation phase carries document work as a report, logging of events. Define methods to be used, specify what all tools are required, and describe a collection of information. Thorough documentation is done. Preservation restricts access to unauthorized users, read access is provided includes plans for data processing. The Collection involves the aggregation of data is done, formation, unification includes proper formatting of data, information, fusion includes integration of data. Examination transforms data includes altering data, normalization of data that is used to standardize information in a proper format. Analyzers verify the authenticity of data. Data presentation involves result implementation, generating reports [6].

However, no data was recovered after the shred delete command. We suspect that data may be recovered successfully by making customized embedded recovery setup and by using invasive microscopy-based techniques such as AFM/SCM/SEM etc. Flash USB when data is recovered on the same storage media.

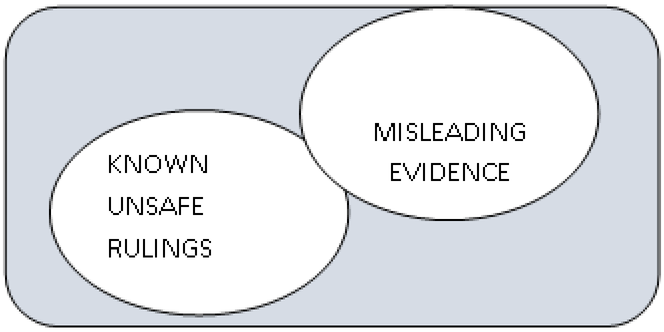

Figure: Criminal evidence in all rulings

In [7] Sonia Bui, There are some rules in criminal evidence which has to be known by the forensic departments. Accordingly, they follow the rules defined. Unsafe rulings are used to avoid the data into unsafe hands.

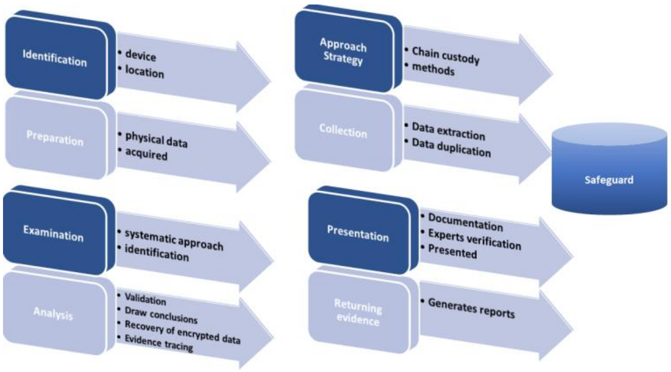

Figure: Digital forensic model

The identification process includes the identification of third parties. The preparation phase carries document work like the report, logging of events. In [8], Define methods to be used, specify what all tools are required, describes the collection of information, thorough documentation is done. Preservation restricts access to unauthorized users, read-access is provided, plans for data processing. The collection involves the aggregation of data is done, format unification that includes proper formatting of data, information fusion includes integration of data. In [9], Examination transforms data includes altering data, normalization of data that is used to standardize information in a proper format. Analyzers verify the authenticity of data. Data presentation involves result implementation, generating reports [10].

In SSD's [11], Data recovery statistics over the number of iterations for NAND. shred -n 1 -v /dev/sdb). Post-normal-delete command, the data was successfully recovered by using recovery software. However, no data was recovered after the shred delete command. We suspect that data may be recovered successfully by making customized embedded recovery setup and by using invasive microscopy-based techniques such as AFM/SCM/SEM etc. Flash USB when data is recovered on the same storage media [12].

V. CONCLUSION

From the results above is concluded that different types of flash memory devices respond differently when subjected to forensic investigation. The reasons behind the difference in behavior are elaborated in brief in this section. In the case of USB and SD cards, the deleted data is completely recoverable. This is because when data is deleted on a USB or SSD, the data is not actually deleted. It is marked as unimportant. Forensic tools try to explore the device's unused spaces to find out if there is any data that is marked unimportant and retrieves them. In the case of solid-state drives, the deleted data is not recoverable using traditional forensic analysis methods. This is because the solid-state devices work differently when compared to SD cards and USB drives. Before any data is written in an SSD flash cell, the flash cell must be emptied. New SSD's comes with empty cells.

VI. ACKNOWLEDGEMENT

Special thanks to Dr. Pankaj Agarkar, HOD and Prof. Chaitanya Bhosale, Department of Computer Engineering, D.Y Patil School of Engineering for guidance and resource provision which helped in development of this project. Thanks to all associated faculties for providing all necessary help.

VII. REFERENCES

[1]. Shivendran Divakar Tiruchanpalli, ”Forensic Aspects of Various Flash Memory Devices (Dec 2019)”, St. Cloud State University.

[2]. Krishnun Sansurooah, “A forensics overview and analysis of USB flash memory devices (Dec 2009)”, Edith Cowan University, Australia.

[3]. Jeong Uk Kang, Heeseung Jo, Jinn-Soo-Kim, Joonwon Lee, “A superblock-based flash translation layer for NAND flash memory (Oct 2006)”,Korea. https://dl.acm.org/doi/abs/10.1145/1176887.1176911

[4]. Abhilash Garg, Supriya Chakraborty “Investigation of Data Deletion Vulnerabilities in NAND Flash Memory Based Storage (Jan 2020)”, India.

[5]. Woodford, C. (2017, June 29). Flash memory. Retrieved from ExplainThatStuff: http://www.explainthatstuff.com/flashmemory.html

[6]. Aya Fukami, Saugata Ghose, Yixin Luo, Yu Cai, Onur Mutlu, “Digital Investigation (Jan 2017)”, Europe.

[7]. Sonia Bui, Michelle Enyeart, Jenghuei Luong,” Issues in Computers forensics (May 2003)”, COEN 150

[8]. Derek Bem and Ewa Huebner, “Analysis of USB Flash Drives in a Virtual Environment (June 2007)”, Small Scale Digital Device Forensics Journal, VOL. 1, NO.1.

[9]. Yatendra Kumar Gupta,”Systematic Digital Forensic Investigation Model”, (March 2016).

[10]. David A. Dampier 3 Arafat AL-Dhaqm1, Shukor Abd Razak 2 ,“ (IEEE) Categorization and Organization of Database Forensic Investigation Processes (June 2020)” Research Management Centre, Xiamen University Malaysia under the XMUM Research DOI:10.1109XXXXXXX.XXXX.3000747

[11]. Avinash Kumar, Ashar Neyaz & Narasimha Shashidhar, “A Survey On Solid-State Drive Forensic Analysis Techniques”, International

Journal of Computer Science and Security (IJCSS) 14 (2), 13-21 2020.USA

[12]. Nikunj Pansari and Dhruwal Kushwaha, "Forensic analysis and investigation using digital forensics- An overview" ISSN: 2454-132X, Uttar Pradesh.