Jean-Michel Batista

SSDs: Data Corrosion

Project unit: PJS480

Supervisor: Dr Li Fudong
Moderator: Dr Gareth Owenson

Table of Contents:

1. Introduction
    1.1. Overview
    1.2. Aims
    1.3. Objectives
    1.4. Constraints
    1.5. Document Structure

2. Project Management Approach
    2.1. Kanban
    2.2. Experiment management review

3. Literature Review
    3.1. Introduction
    3.2. Problem presented by Solid State Drives in Digital Forensics
    3.3. Wear-Levelling & Garbage Collection
    3.4. TRIM
    3.5. Can write-blockers prevent self-corrosion on SSDs?
    3.6. File Carving & File Systems
    3.7. Data Recovery on SSDs
    3.8 Automation in forensic data extraction applications
    3.9 Conclusion of Literature Review

4. Methodological Approach

5. Requirements
    5.1. Experiment requirements
    5.2. Interpretation and Discussion of Results requirements

6. Experimental Investigation
    6.1. Experiment 1: Can we recover data marked for deletion from unallocated space on a TRIM-enabled SSD?
    6.2. Experiment 2: How fast will the combination of TRIM functionality and garbage collection zero out data from unallocated space?

7. Interpretation and Discussion of Results

8. Recommendations and Guidance for Future Research
    8.1. The future of digital storage (2020)

9. Conclusion
    8.1. Personal Reflection

10. References

11. Appendices
    11.1. Appendix I: Experimental Environment
    11.1. Appendix II: Additional Screenshots & Information

Table of Tables:

Table 1 - Kanban Principles, Project Initialization through a Gantt chart.

Table 2 - Visualizing workflow

Table 3 - Recovered deleted files from the 120 GB Hitachi SATA SSD.

Table 4 - Division of unrecoverable data and time based on Experiment 1.

Table of Figures:

Figure 1 - Shipment of hard and solid-state drives.

Figure 2 - Example of how hard drives store data (a) vs how solid-state drives store data (b).

Figure 3 - Example of incorrect sequential recovery shown for a fragmented image.

Figure 4 - Example of automated file carving with Autopsy.

Figure 5 - Presence of test files metadata in unallocated space.

Figure 6 - Fully recoverable test files from unallocated space.

Figure 7 - Recovered data (11,100) vs Unrecoverable data (8900)

Figure 8 - Hint of evidence pointing to the deleted test files.

1. Introduction

1.1 Overview

Solid state drives are an important part of technology, they are exponentially growing to become the leading storage device across the industry and households. But they are more than just storage devices; they have been designed to ever-change for the sake of performance and optimization in order to extend their life with the help of wear levelling, garbage collection and trim features.

When data is deleted off a hard drive, it is practically possible to recover all data that has been marked for deletion. On the other hand, SSDs are capable of near-complete data deletion entirely on their own.

Tracking this automated process can give us a better understanding of SSDs. The information gathered can be useful to better determine the behaviour of wear levelling, garbage collection and TRIM combined and understand the rate at which a TRIM enabled SSD will naturally zero out data marked for deletion.

Extracting this information with the help of a data carving tool and presenting it in a visual manner will be the main support for our research.

1.2 Aims

The overall aim of this project is to recover data from unallocated space using file carving on TRIM-enabled SSDs. Based on the results we will discuss the possibility to create a graphical projection that will allow us to better understand how fast the combination of TRIM and garbage collection will permanently delete data.

The project will examine the following questions:

- Can we recover data marked for deletion from unallocated space on a TRIM-enabled SSD?
  - Knowing this information for certain will be crucial for the rest of the investigation.

- At which rate will TRIM-enabled SSDs zero out deleted data?
  - This is necessary as the process could be mathematically theorized.

- How could this investigation impact digital forensics?
  - The project is being conducted to analyse SSDs in the wild. It is an important part of the project to conclude whether the extracted data holds relevance within the field of the project.

- Based on our results, does using a TRIM enabled SSD over a non-trim enabled SSD or HDD increase the security of the consumer?

1.3 Objectives

The main objective is to create a proof of concept by extracting information with the help of a digital forensics' application.

Other objectives we will need to achieve are:

- Research past research made on similar projects.
- Research of existing forensic tools that will allow us to perform data carving.
- Investigate how to image an SSD.
- Automate the process of data carving with the help of forensic tools.
- Creation of proof of concept.
  - The results will need to be replicable.
  - The results will need to be able to show a range of data.
  - The results will need to be able to show a mathematical projection of unrecoverable data lost based on time.
- Evaluate findings and produce a final review of the project.

1.4 Constraints

Limited personal data storage. In order to test the proof of concept it will be necessary to store multiple images of the same drive. To mitigate this, it might be necessary to delete the images after we have analysed them.

Imaging and analysing the SSD images will require constant progression as it is a slow process. A project plan has been created with over-run time to avoid project failure. Extra time has also been accommodated for unforeseen delays

Limited research on the subject will prove to be challenging. All experiments found related to the subject will be used as a countermeasure. This project will be built based on past research projects on the subject.

1.5 Document Structure

The goal of the document structure will be to present the project in a coherent and logical manner. The intent on our first part was to discuss the aims, objectives and constraints during the development of the project. Our next part will be dedicated to how the project will be managed and will define the project management approach we will use. Next, we will include a literature review to increase our knowledge on the topic and support our research and then discuss the requirements needed to produce the proof of concept. Our primary research will be conducted to create our proof of concept. The results will be analysed, and conclusions will be drawn from the research.

2. Project Management Approach

In order to keep the project on track and keep the proof of concept in continuous development we will require to adopt a method of project management. An optimal project management approach will ensure us that the project develops efficiently over-time and will reduce the likelihood of failure.

To achieve our goal, we will follow the Kanban project management methodology. The Kanban approach will be used during the project development because it helps visualize our objectives and limit the work in progress. Awareness of what task is coming up next will make it easy to reprioritize, uncover process problems and prevent tasks from stalling. As we focus on one task at a time it will be possible to isolate individual aspects of the project and work towards creating the proof of concept.

2.1 Kanban

Kanban is built on a set of lean principles; the approach aims to manage work by balancing demands with available capacity and by improving the handling of possible bottlenecks. The Kanban principles will lead our work output to be flexible and light on process. The goal will be to manage the project under the Kanban framework and its core practices. These core practices will involve visualizing our workflow in order to have a rough idea where we are in the project, measuring lead time in order to re-prioritize different tasks of the project and manage overhead time that could be used to improve the project, and finally making process policies explicit while continually evaluating improvement opportunities. The principles, and how they apply to the project, can be seen at Table 1 & 2.

As we do not expect what the outcome of our proof of concept will be, it is necessary to have the possibility to accommodate changes. It will become a requirement to know what we will be working on, when we will be working on that process and how much time we are going to spend on that piece of the project. Kanban is commonly used in software development in combination with other methods, but it is possible to adapt it outside that spectrum. The workflow control will work similarly for every step. If we run into a problem, it will be possible to visualize where the problem is in the grand scheme of the project and re-planning can be done to spend more time solving the problem. Work management will be made possible by limiting work in progress across a timeline that team members can always see and track.

	Name	Category	Status	Owner	Start date	End date
	PID Submission & ECR	Progress reporting	In progress	Jean-michel Batista	9/10/2019	22/10/2019
2	Report Template & Introduction	Progress reporting	In progress	Jean-michel Batista	22/10/2019	25/5/2019
3	Research & Literature Review	Progress reporting	In progress	Jean-michel Batista	25/10/2019	25/11/2019
4	Report - Part 1: Methodology/Research Design	Progress reporting	In progress	Jean-michel Batista	25/11/2019	1/12/2019
5	Report - Part 2: Data Collection	Progress reporting	In progress	Jean-michel Batista	1/12/2019	16/1/2020
6	Report - Part 3: Data Analysis	Progress reporting	In progress	Jean-michel Batista	16/1/2020	14/2/2020
7	Report - Part 4: Discussion	Progress reporting	In progress	Jean-michel Batista	14/2/2020	1/3/2020
8	Report - Part 5: Conclusion	Progress reporting	In progress	Jean-michel Batista	1/3/2020	8/3/2020
9	Language & Referencing	Progress reporting	In progress	Jean-michel Batista	8/3/2020	15/3/2020
10	Style & Layout	Progress reporting	In progress	Jean-michel Batista	15/3/2020	22/3/2020
11	Project improvement & Optimization	Progress reporting	In progress	Jean-michel Batista	22/3/2020	30/4/2020

Table 1 - Kanban Principles, Project Initialization through a Gantt chart.

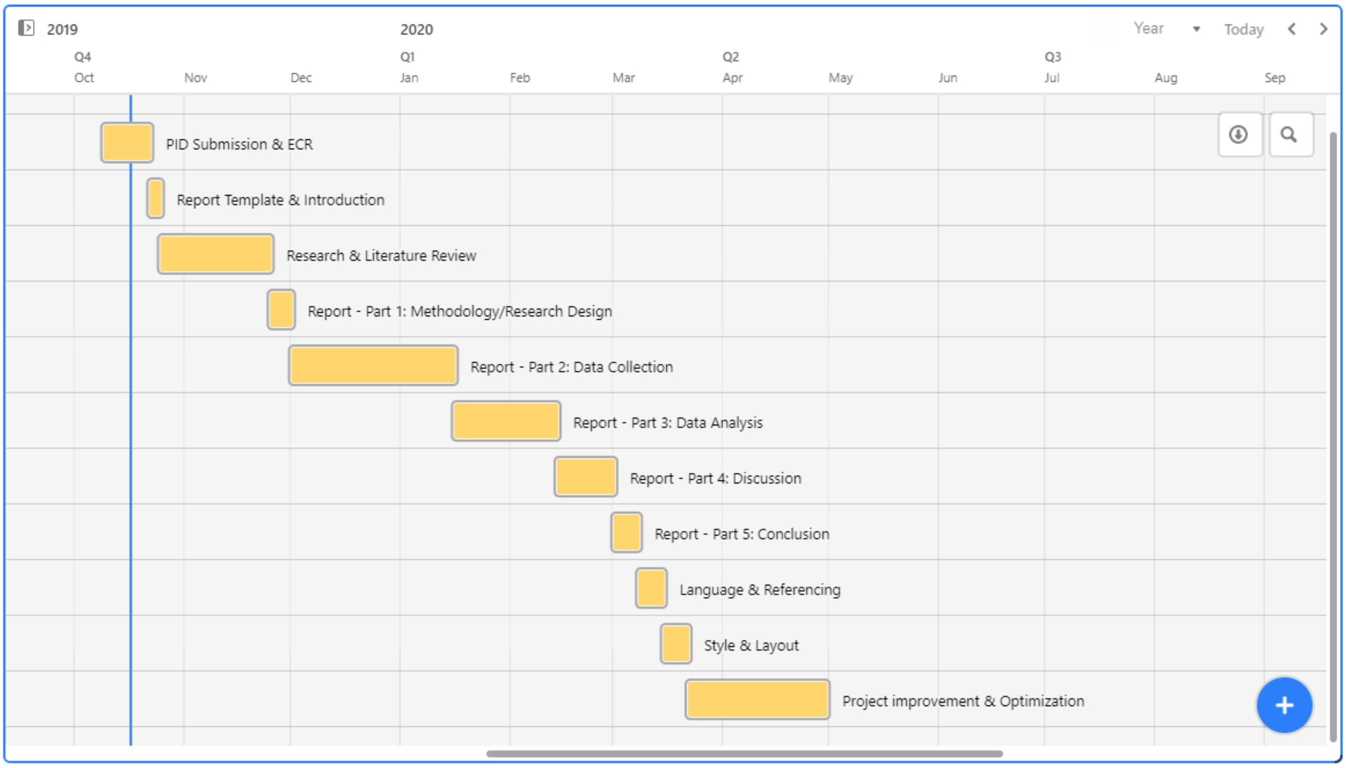

Table 2 – Visualizing workflow.

2.2 Experiment Management Review

The project itself will be supported and managed using Kanban. However, in order to create our proof of concept we will use a different methodology. The experimental method is a systematic and scientific approach to research in which the researcher manipulates one or more variables, and controls and measures any change in other variables in order to analyse cause and effect relationships. The method will best suit the goal of the research and will be dealt with using a deductive approach in order to test the asymmetrical relationship between TRIM enabled SSDs and deleted data.

We will aim to support our proof of concept through a controlled experiment where we will control conditions and where accurate measurements are possible. Controlled experiments attempt to be easy to replicate through a standardized procedure and allow for precise control of extraneous and independent variables. Results produced by this project obtained through experimental samples are to be compared against a control sample. In this project both experimental and control samples will practically be identical except for the one aspect whose effect is being tested. The aspect being tested on the SSD samples will be the TRIM functionality and the experimental phase will be carried out in the following order:

- Method of experiment
- Detail of experiment
- Expected result
- Actual result
- Interpretation and discussion of results

3. Literature Review

3.1 Introduction

A Solid-State Drive or also known by its abbreviation “SSD,” is a data storage technology that uses a simple memory chip called NAND flash memory. An SSD will emulate the functionality of a Hard Drive while having no moving parts and faster read/write speeds (Christensson, P., 2011) [1]. In 2010, Bell and Boddington [2] described SSDs as the beginning of the end for digital forensic recovery, reporting cases where significant corrosion of evidence was apparent when working with SSDs as they are capable of near-complete data deletion entirely on their own. With the SSD market soaring to £6.3 billion in 2013 (Shilov, 2014) [3] when SSDs were starting to appear in consumer’s households, there was no doubt the attraction and improvements over its brother, the HDD, would catapult the SSD game into a whole new chapter. In the past decade, consumer hardware has seen its fair share of evolution in terms of storage. From most systems only possessing an HDD, to both an HDD and an SSD mainly due to the Price/GB ratio for SSDs at the time and finally not needing an HDD with currently affordable consumer SSDs rocking up to 2TBs capacity.

According to the statistics of shipments of hard and solid-state drives worldwide from 2015 to 2021 (Holst, 2019) [4] SSDs are expected to surpass the number of HDDs by 30 million in 2021 with the number of shipped HDDs decreasing by an average of 20 million per year since 2016. Today, SSDs have become a prevalent part of our hardware and, at the same time, real pain for forensic investigators seizing digital evidence. One of the fundamental requirements of evidence in any civil or criminal case is its integrity. The evidence presented during a trial must be identical to the evidence seized. As stated in Nisbet and Jacob’s research study (2019) [5], there are three different forms of integrity alterations forensic investigators need to be aware of when working with SSDs, which are TRIM functionality, Wear Levelling and Garbage Collection. All three move or delete data from SSDs, forcing them to be at a different state and have a different checksum/hash value compared to the exact moment of acquisition even when using write blockers (Bell and Boddington, 2010) [2].

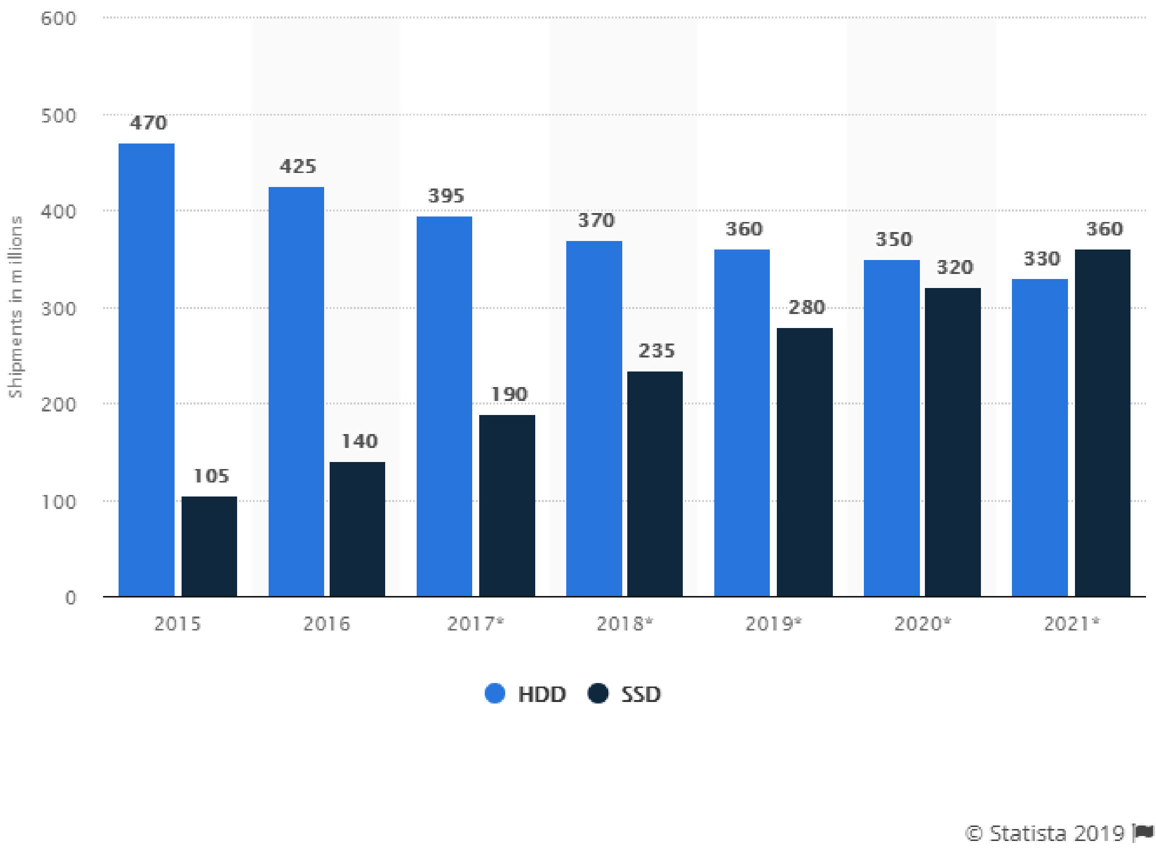

Figure 1 - Shipment of hard and solid-state drives (Holst, 2019)

3.2 Problem Presented by Solid State Drives in Digital Forensics

The problems presented by SSDs in Digital Forensics rely on three different pieces of technology SSDs support. These technologies are not implemented to make evidence retrieval from SSDs a nightmare but to increase their efficiency and prolong their microchip life, benefitting the user. However, these technologies pose a threat to forensic investigators when recovering data from unallocated space. When recovering data from HDDs, it is common that almost all the files are still up for recovery even if the user attempts to format the drive. In contrast, while experimenting with SSDs, Bell and Boddington (2010) [2] reported that only 0.03% of their data was recoverable in a 316,666 file sample size within a couple of minutes after a simple format command was issued.

We recognize SSDs are very vulnerable to data deletion, both from external sources and internal sources. All SSDs react to data deletion by the nature of their design. Hardware manufacturers implement wear levelling, garbage collection, and TRIM compatibility functionalities in SSDs only to mitigate their limitations. (Shemeretov, 2017) [6]. The solutions developed to work around the retrieval of data from unallocated space on NAND flash memories, up to this day, still trample the integrity of evidence when necessary. The practicality of hashing a storage and subsequently ensuring that all images match the original hash could no longer apply in some cases when working with NAND flash memory devices (Vieyra et al., 2018) [7]. According to the guidelines on Mobile Device Forensics from the National Institute of Science and Technology (2017), a change in evidence integrity sometimes can be necessary for the greater good of the recovery process.

3.3 Wear-Levelling & Garbage Collection

Solid state drives function by storing data in blocks, subsequently, the blocks are subdivided into pages. These blocks and pages are composed of large arrays of NAND transistors which hold a close similarity to NAND logic chips used to manufacture CPUs. The main difference is that the SSD's will own an extra gate known as a floating gate (Olson & Langlois, 2008) [8] to trap charge and use this as a supply of power.

Individual blocks within the SSD can only be written to a limited amount of times before they are at risk of failing. The number of writes to be expected before failure could be any amount of times between 10000 and 100000 times (Olson & Langlois, 2008) [8]. As a temporary solution to this inconvenience, Wear-Levelling was introduced to avoid continuously writing data to the same blocks in order to extend the service life of SSDs. Through this feature, SSDs will make use of a flash translation layer (FTL) to store each write to new or less-used locations (Bell and Boddington, 2010) [2]. However, the extensive use of a solid-state drive's storage capacity will require blocks to be erased electronically before they can be used again. Flash technology will only allow entire blocks to be erased, not pages. The problem led manufacturers to develop a strategy known as Garbage Collection (Bell and Boddington, 2010) [2], which will move all valid data to a page in another block so the invalid data (deleted data) can be erased after being identified by TRIM.

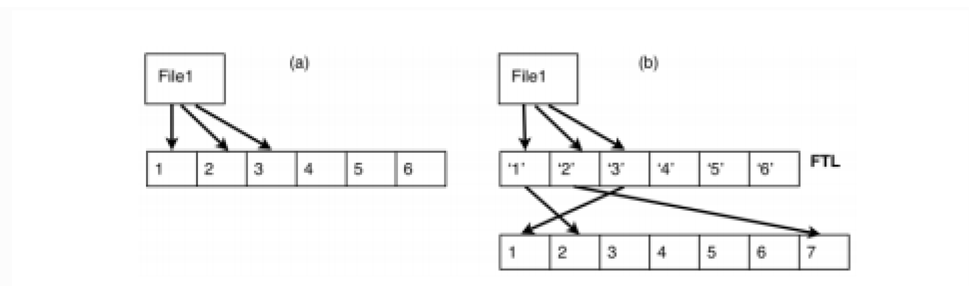

Figure 2 - Example of how hard drives store data (a) vs how solid-state drives store data (b). (Bell and Boddington, 2010) [2]

3.4 TRIM

On technical terms TRIM is a command designed for the ATA interface and it must be supported by both the operating system and the SSD in order to achieve its functionality. It is a functionality that can be enabled or disabled on the command line for a solid-state drive only if both the drive and operating system support it. With TRIM enabled, garbage collection will periodically take place permanently deleting unwanted data. The functionality will allow to skip the process of SSDs copying a block of data to the cache, delete the unwanted or invalid data while in the cache, clear the original block, and finally replace the block.

TRIM will achieve its goal by communicating to the SSD the areas where data is no longer in use so the next time a computer is idle, garbage collection will automatically delete the data (Crucial, 2020) [9]. Assuming TRIM is supported, every deletion on an SSD should be accompanied with the TRIM command to inform the drive about freed sectors, at some point the SSD should perform garbage collection of those freed sectors. The process of automatic routine garbage collection will always happen in the background and will not be obvious to the front-end user, but if active garbage collection took place before or during forensic extraction of the drive image there is a high chance evidence would be corroded (Bell and Boddington, 2010)[2].

3.5 Can write-blockers prevent self-corrosion on SSDs?

The experiment carried out by Bell and Boddington (2010) [2] demonstrated that when working with SSDs even with the usage of a write-blocking bridge, there can be a noticeable presence of self-corrosion. However, as their research proved the first case of a drive having substantial amounts of evidence purged from it despite the use of a conventional hardware write-blocker (Bell and Boddington, 2010) [2], no more than 18.74% or their data ended up being zeroed-out. While write-blockers seem to hold back garbage collection to some extent, it remains unclear whether using other types of SSD or write-blockers would provide any different result. Back when the research was done, results indicated there could be significant implications for legal matters involving digital evidence, more so in cases where digital data was alleged having been deleted intentionally or accidentally by a defendant (Bell and Boddington, 2010) [2]. Research predicted the mainstream use of SSDs would become a new grey area within the forensics industry. At that point in time SSDs were attributed to create the beginning of the end for known practice in digital forensics recovery as they were being introduced into the market and specifically at a commercial level. It was then realized the analysis of deleted data and deleted metadata had to adapt to the new changes brought by solid state drives when compared to hard drives. It is safe to say write-blockers will not guarantee the prevention of SSD self-corrosion, making the process of recovering data from an SSD a real challenge for forensic investigators.

3.6 File Carving & File Systems

In order to recover deleted files from unallocated space, file carving is the most efficient process up to date. Different forensic applications such as Autopsy, FTK and other commercial and open source forensic software possess their own different approaches and own versions of file carving. File carving is a forensic technique that will allow the recovery of files based on file structure, content, and without any matching file system metadata (Pal and Memon, 2009) [10]. In theory, if user modified files were to be deleted, file carving is expected to recover the totality of deleted files when working with an HDD or a TRIM-disabled SSD. First generation file carvers were known to use “magic numbers' ', byte sequences at prescribed offsets to identify and recover files. In the case of jpegs, starting clusters within the data blocks had to contain the hex sequence FFD8 and their footer in the cluster had to end in the hex sequence FFD9 for file carvers to identify them as jpegs in order to recover them (Pal and Memon, 2009)[10]. The file carvers that relied on structure alone attempted to merge and return unallocated clusters between the header and the footer. File carving technology has since then evolved with one of the most prominent examples up to date being the changes brought by the Foremost (Foremost, 2020)[11] software developed by the US Air Force in 2001, one of the first file carvers to implement sequential header to footer carving and also implement carving based on a header and size of file. However, none of them took into consideration whether the files being recovered were fragmented or not and, as a result, in cases where fragmentation was present file carving would recover contents out of unallocated space with “garbage” present in them. In current practice, the presence of fragmentation will require the file carving tool to attempt reassembly. Reassembly will involve finding the fragmentation point of each unrecovered file and then finding the next fragment’s starting point until a file is rebuilt or determined to be unrecoverable (Pal and Memon, 2009) [10].

Research has shown that the technicality of the process of “deletion” in computing will occur differently depending on the used file system (Pal and Memon, 2009) [10]. After performing a forensic file system analysis, Carrier (2005) [12] described file systems as a combination of structural and user data organized in such a way the computer system will know where to find them. The process of file allocation and file deletion will not be the same across the variety of file systems, a file allocation table (FAT)-32 file system will not allocate or delete files the same way as a new technology file system (NTFS) (Pal and Memon, 2009)[10]. As files move around within the file system whether they are added, modified or deleted most file systems will be exposed to fragmentation. According to Garfinkel’s experiment (2007) [13] where 350 disks containing FAT, NTFS and Unix file systems (UFS) were used to analyse fragmentation statistics, fragmentation could be attributed to different reasons. The reasons that could cause fragmentation were concluded to be low disk space, appending/editing files and wear-levelling algorithms. Fragmentation rates of forensically important file types were found to be 16% for jpegs, 17% for Microsoft Word Documents, 22% for audio video interleave (AVI) files and 58% for personal information store files (Garfinkel, 2007) [13]. As a result of wear-levelling, SSDs will be naturally fragmented, indicating that there are higher chances to recover contents off an SSD with “garbage” in them unless the process of reassembly has succeeded in rebuilding fragmented files.

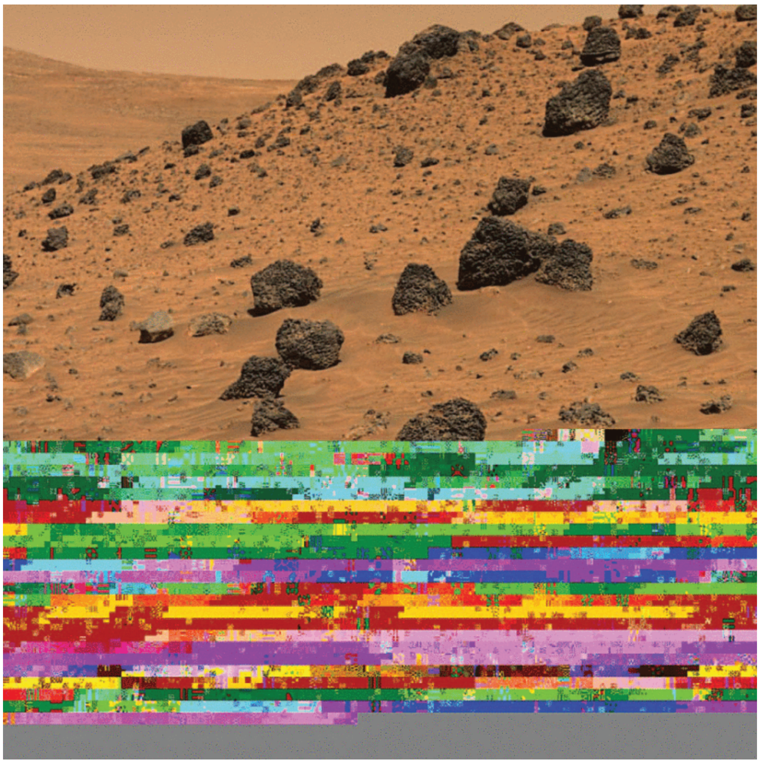

Figure 3 - Example of incorrect sequential recovery shown for a fragmented image. (DFRWS, 2006) [14]

3.6 Data Recovery on SSDs

Research and practice have proven that it is not impossible to recover data marked for deletion in SSDs. Research experiments carried out by King and Vidas (2011) [15] showed that all data is recoverable from SSDs without TRIM and only a total of 27% of the data was recoverable in TRIM enabled SSDs. Another research experiment concluded that when sending a simple format command to SSDs connected through either the USB interface or secondary SATA interface all data was recoverable, but when connected to the primary SATA interface, not a single byte of data could be recovered (Shah et al., 2014)[16]. Additionally, a research experiment on solid state drives with TRIM enabled file systems concluded it was only possible to recover 0.5% of the original data across NTFS and HFS+ file systems (Nisbet et al., 2013) [17]. The safest approach suggested when recovering data from SSDs is to isolate the drive from the system and connect it as an external disk drive, since TRIM is a command for the SATA interface it will not execute for external USB disk drives (Aldaej et al., 2017)[18]. Isolating the solid state drive from the system and connecting it through an USB interface is a good way to stop self-corrosion of the drive from TRIM, however, it will not be clear how much data the combination of TRIM and garbage collection will have already zeroed out from the drive from previous exposure. As a last resort option, white box acquisition was proposed to bypass the controller of the disk drive and read data directly from the NAND chips, but this method also holds the risk of data deletion (Bonetti et al,. 2013)[19].

3.7 Automation in forensic data extraction applications

Coding a file carver could be an entire project of its own. With the help of forensic applications, the file carving task can be automated to vastly increase the speed in which tasks can be performed as well as reduce the risk of mistakes to deliver accurate results. The use of forensic applications will result in increased efficiency and decreased cost as they will make an analyst's job easier (Breton & Bossé, 2003) [20]. There are different factors that will determine what makes a digital forensics platform feasible. Open source digital forensics platforms such as Autopsy can arguably compete with digital forensic platforms such as Encase or FTK as they will generally provide the same main features.

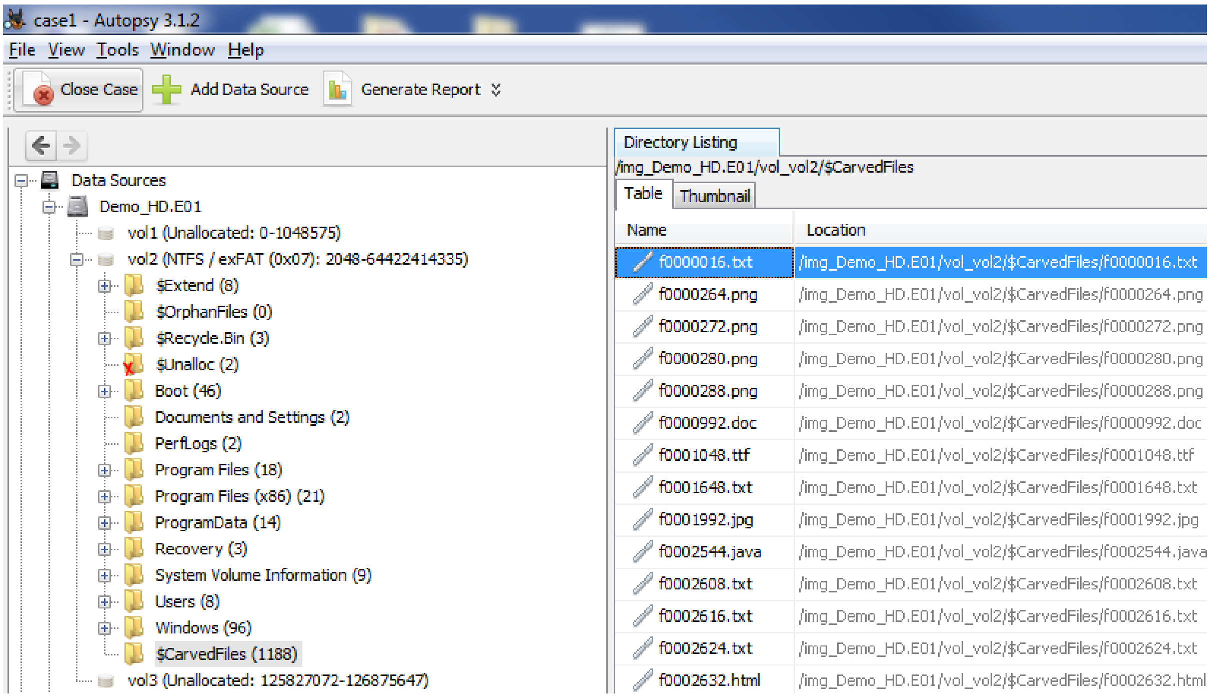

Figure 4 - Example of automated file carving with Autopsy. (Sleuthkit.org, 2020) [21]

3.8 Conclusion of Literature Review

There is not enough research done when it comes to recovering unallocated data from TRIM-enabled solid-state drives. More research will be necessary to decide the best way to mitigate the effects of SSD self-corrosion. In addition, more research will also be necessary to improve data recovery on TRIM-enabled SSDs.

There are experiments which have proved the amount of data recovered from TRIM-enabled SSDs after a format command was issued is minimal and experiments which have proved write-blockers can mitigate further self-corrosion to some extent as they will separate an SSD from the primary SATA channel. However, no experiment has been done that answers the question of how fast TRIM-enabled SSDs self-corrode after files have been deleted and more research needs to be done in order to explore this possibility.

4. Methodological Approach

The study carried out will take into consideration the range of research methodologies used on previously conducted experiments in the field. It is expected that all data used to support the research will be quantitative due to the nature of the project. In order to produce the quantitative data, requirements will be put into context in the next chapter by creating more in-depth analysis.

The research topic in place will examine the extermination of unallocated space data by the active combination of TRIM and garbage collection activities on TRIM-enabled SSDs and attempt to quantify the produced data based on results. One of the multiple achievements the research needs to accomplish will be to prove the possibility to recover data from unallocated space on TRIM-enabled SSDs and then attempt to establish a pattern based on behavioural response. Data was added to a TRIM-enabled SSD that is connected through the primary SATA channel of a TRIM-enabled system; this data was then marked for deletion to find out how fast TRIM and garbage collection act on the SSD through the process of imaging and file carving the drive. The weakness in this approach is that it is not friendly to forensics integrity, meaning that it will be necessary to let the hash value and state of the SSD to mutate naturally for our method to have higher chances of succeeding. Past research has indicated that the use of a write-blocker or connecting the SSD through any other means other than the primary SATA channel would most likely thwart TRIM functionality. The justification for using this technique of methodical research was to achieve full isolation of the data coming from file carvers and enforce our experimental results by discarding external factors that could have stopped or thwarted the combination of both TRIM functionality and garbage collection during the production of the proof of concept.

Procedures were planned thoughtfully in order to make the study project reproducible. Except for the file system, all data was wiped clean off the TRIM-enabled SSD. It was made sure that the SSD was connected through the primary SATA channel and that the system's TRIM functionality was turned on. Multiple disk images of the same TRIM-enabled SSD were created in the process of investigation to keep the data consistent and flowing from one source. The digital forensics platforms used were confirmed to support disk imaging and file carving to make the data reliable.

The aim was to confirm the possibility of data recovery from unallocated space on TRIM-enabled SSDs and produce quantitative data which could then be theorized and projected through a mathematical equation based on how much data was zeroed out from unallocated space and time taken for that same data to be zeroed out. Primary research was gathered using open source forensic platforms available to the public and the data which they presented upon going through the process of file carving. This data was then analysed, and conclusions were drawn from the experiments. The study relied upon the hypothesis that data is still recoverable after being marked for deletion on TRIM-enabled SSDs.

5. Requirements

In order to create our proof of concept it will be a requirement to have an SSDs which can be connected to the primary SATA channel. The SSD will also need to support TRIM functionality and have enough space for the tester to add data to the SSD. Another requirement will be a tool that can image the SSD, there are multiple ways to go about this, most digital forensic platforms can be used to create images of drives. The forensic platform used will also be required to extract data from unallocated space through file carving for the tester to be as efficient as possible.

The presented requirements were chosen by analysing the aims and objectives of the project. A considerable number of planned thoughts were implemented to accurately determine what the project needed to achieve. If the experiment phase of the project is successful in extracting desired results it will also be a necessity to further implement more requirements. For this reason, each section of extra requirements was broken down into subcategories.

5.1 Experiment requirements

It is required that the experimental investigation phase lays out the process of investigation by detailing each investigative step and the purpose of the experiment. Each one of these requirements will be necessary for a successful experimental investigation. The first one will be stating the purpose of the experiment will help clarify what the experiment is about and what it is expected to achieve. The second one will be stating the method of experiment, in which it will be required to briefly detail the exact process carried out in the experiment in order to achieve the results. The third requirement will be to provide an in-depth detail of the experiment where we discuss the files expected to be file carved, the hardware used, the commands used, and the digital forensics platform used including file carving settings. The third requirement within the experimental investigation will also need to discuss in detail the time intervals at which the TRIM-enabled SSD was imaged. The fourth requirement will be to discuss the expected result of the investigation and the fifth and final requirement for this section will be to provide and discuss the actual results of the experimental investigation.

5.2 Interpretation and Discussion of Results requirements

It is a requirement for the results created through the experiment phase to be presented in a clean and easy to understand manner for the results to be easily interpreted and understood even by someone with little understanding of the subject. It will also be a requirement for the results to be replicable with no changes made to the methodology for them to be reliable. As a final requirement, all data extracted must be the product of a trusted forensic platform, no external factors or external data that is not part of the experiment is to be mixed with the actual results. The project in place is responsible to allow the produced data to be both credible and reliable.

6. Experimental Investigation

6.1 Experiment 1: Can we recover data marked for deletion from unallocated space on a TRIM-enabled SSD?

Purpose of experiment: To determine through conventional dead analysis using forensic imaging the extent to which files that have been marked for deletion have been purged by a TRIM-enabled SSD and if any of those files are recoverable following a one hour period connected through the primary SATA channel without specific format commands or write instructions.

Method of experiment: The TRIM-supported SSD was filled with 20,000 pictures. The pictures were then deleted, and the drive was imaged to measure the extent to which the files inside the TRIM-enabled drive were affected by the combination of TRIM functionality and garbage collection.

Detail of experiment: The experiment was carried out as follows. We used the standard experimental machine and the configuration present in Appendix I. In order to produce test results for the experiment a 120GB Hitachi TRIM-supported SSD was tested. During each test of this experiment the drive was connected to the primary SATA channel on the motherboard and the machine powered on. After login we confirmed our Windows 10 operating system supported TRIM with the command *fsutil behavior query DisableDeleteNotify*, TRIM functionality is in place when the value returned equals to 0. A 138 KB template jpg file was selected containing the image of a frog. The file system partition was then filled with 20,000 copies of the template file and after the process of writing that data onto the drive was done the files were deleted. Upon deleting the test files the drive was then immediately imaged and file carved using Photorec within the Autopsy environment. From the time the files were deleted to the time of first top-level results given by Autopsy approximately 15 to 16 minutes had passed. The results given by Autopsy were then analysed and recorded in order to produce the data. Each run of experiment 1 was repeated 6 times in total in the span of 6 hours with approximately 15-minute intervals separating each image of the drive to determine whether the results occurred consistently and reproducibly.

Expected result: We expected to see self-corrosion behaviour to some extent on the TRIM-enabled SSD but we expected that the self-corrosion event would still allow a portion of the unallocated data to be recovered and that in time, little to no presence would eventually be found of the jpg files that had been deleted. Based on past research experiments, it was originally expected that the combination of TRIM functionality and garbage collection would erase unallocated file contents within the SSD to the point of no recovery and that eventually there would be no trace or any artefacts left that would hint that any file had been deleted at all.

Actual result: The results of the experiment are shown in Figure 7 and 8. It was amazing to see how consistent and fast garbage collection took place when combined with TRIM. On average, at the 15 minutes mark routine imaging, we could only find partial metadata of 11,100 of the test files. Out of the average of 11,100 test files, it was rarely possible to reconstruct a maximum of 1 or 2 test files whole, but most images indicated nothing could be reconstructed out of metadata alone (Provided in Appendix II). The Photorec file carver used through Autopsy also indicated zero trace of any of the test files in all the instances of the experiment which was both surprising and disappointing at the same time. These results really stood out, with TRIM in place garbage collection will act very aggressively, this means that files deleted that are exposed the combination of these two functionalities will generally be unavailable for forensic recovery in a matter of minutes. Following the results of experiment 1 we knew it would be a real challenge to further analyse the speed at which the TRIM and garbage collection combination erased these files completely.

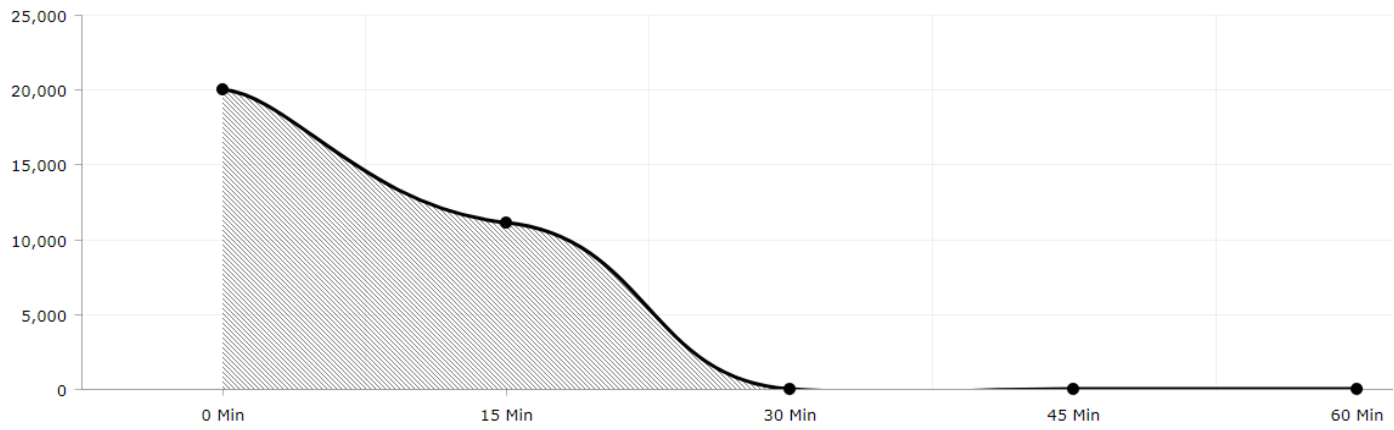

Figure 5 - Presence of test files metadata in unallocated space. The X axis shows time in minutes and the Y axis shows the approximate amount of test files found in unallocated space. In all six runs of the experiment the solid-state drive self-corrosion was very apparent in the first image of the drive roughly 15 minutes after the test files were deleted. In the second image of the drive even all pre-existing metadata left had been entirely wiped.

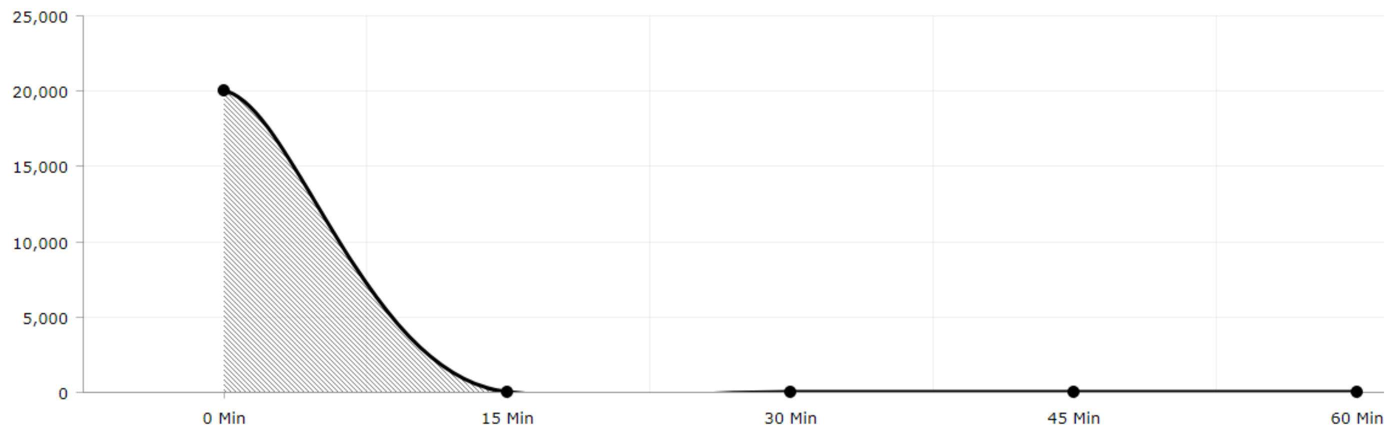

Figure 6 - Fully recoverable test files from unallocated space. The X axis shows the time and the Y axis shows the average amount of recoverable test files that could be reconstituted as an original jpg image. After 6 runs of the experiment, only an average of one image test file per experiment could be reconstituted. There were runs of the experiment in which zero image test files could be reconstituted.

Device 120GB Hitachi SATA SSD	Average of files recovered	Description of recovered files
11,100 deleted test jpg images were recovered from the drive.	**11,099** **---------------------------------** **1**	**File name and temporal metadata recovered but not readable. These files could not be reconstituted as an original jpg image.** **---------------------------------** **File name and temporal metadata recovered. The file could be reconstituted as an original jpg image.**

Table 3 - Recovered deleted files from the 120 GB Hitachi SATA SSD.

Following the results of experiment 1 we knew it would be a real challenge to further analyse the speed at which the TRIM and garbage collection combination erased these files completely. At this point, the speed at which the TRIM-enabled SSD was completely erasing the test files paired with hardware limitations proved to be a real problem, there was no way for us to reduce the imaging time.

6.2 Experiment 2: How fast will the combination of TRIM functionality and garbage collection zero out data from unallocated space?

The possible data drawn from experiment 1 proved to be very limited. However, it is possible to draw conclusions from the experiment in order to theorize the speed at which both TRIM and garbage collection will erase data tied to deleted files. Out of the 20,000 test files, an average of 11,100 of the test files file name and temporal metadata were still being recovered from unallocated space in the first 15 minutes. As shown in figure 9, The test files recovered represented roughly 55% of the total amount of test files while the completely erased files mounted up to roughly 45% of the total amount of test files. By dividing the total number of test files completely lost and time that had passed we could get an approximate of how fast the data was being completely deleted.

Figure 7 - Recovered data (11,100) vs Unrecoverable data (8900)

Unrecoverable data:	Time (In Minutes):	Result: (Unrecoverable data/Time)
8900	15	593.33

Table 4 - Division of unrecoverable data and time based on Experiment 1.

Based on the results found in experiment 1 we may judge that the test files used for the experiment were being deleted at a speed of roughly 593 test files per minute. This could further be translated to 4.29 MB of data per minute. In order to test this theory, we had to carry out a second experiment where we increased the number of test files and see if this could impact our results in any way.

Purpose of experiment: To identify whether the proposed theory can be proven through conventional dead analysis using forensic imaging. The experiment will try to test the theorized speed at which the combination of TRIM and garbage collection will completely purge deleted test files following a 15-minute period connected through the primary SATA channel without specific format commands or write instructions.

Method of experiment: The TRIM-supported SSD was filled with 40,000 pictures. The pictures were then deleted, and the drive was imaged to measure the speed at which the files inside the TRIM-enabled drive were purged by the combination of TRIM functionality and garbage collection.

Detail of experiment: The experiment was carried out as follows. We used the standard experimental machine and the configuration present in Appendix I. In order to produce test results for the experiment a 120GB Hitachi TRIM-supported SSD was tested. During each test of this experiment the drive was connected to the primary SATA channel on the motherboard and the machine powered on. After login we confirmed our Windows 10 operating system supported TRIM with the command *fsutil behavior query DisableDeleteNotify*, TRIM functionality is in place when the value returned equals to 0. Two template image jpg files were selected, one containing the image of a frog with a size of 138 KB and one containing the image of a cat with a size of 35.9 KB. The file system partition was then filled with 20,000 copies of the first template file and 20,000 copies of the second template file. After the process of writing that data onto the drive was done the files were deleted. Upon deleting the test files the drive was then immediately imaged and file carved using Photorec within the Autopsy environment. From the time the files were deleted to the time of first top-level results given by Autopsy approximately 15 to 16 minutes were expected to pass just like in experiment 1. We would then use the results given by Autopsy and analyse them in order to record and produce the data. The results of the images of the drive made are meant to represent an approximate 15-minute exposure to TRIM and garbage collection. Experiment 2 was repeated a total of 5 times to determine whether the results occurred consistently and reproducibly.

Expected result: We expect to see very either very promising or very volatile results. The experiment could either confirm or debunk our theory. If our theory is correct, we can expect an average total of 18,000 test files completely erased from the SSD (45%). If our theory is incorrect then we can expect the average of completely erased test files to be higher, lower or random.

Actual result: The experiment itself resulted in a failure and we could not confirm the proposed theory. It was not possible for us to replicate the imaging time achieved in Experiment 1 across multiple attempts. The operating system became extremely unresponsive each time we deleted 40,000 files at once. From the time we deleted the test files to the time to the time of first top-level results given by Autopsy approximately 38-45 minutes passed. We could, however, often find some vague metadata evidence in the totality of 200,000 .jpg files deleted across different runs of the experiment but as seen in figure 10, nothing pointed to their original file name and their content had been zeroed out.

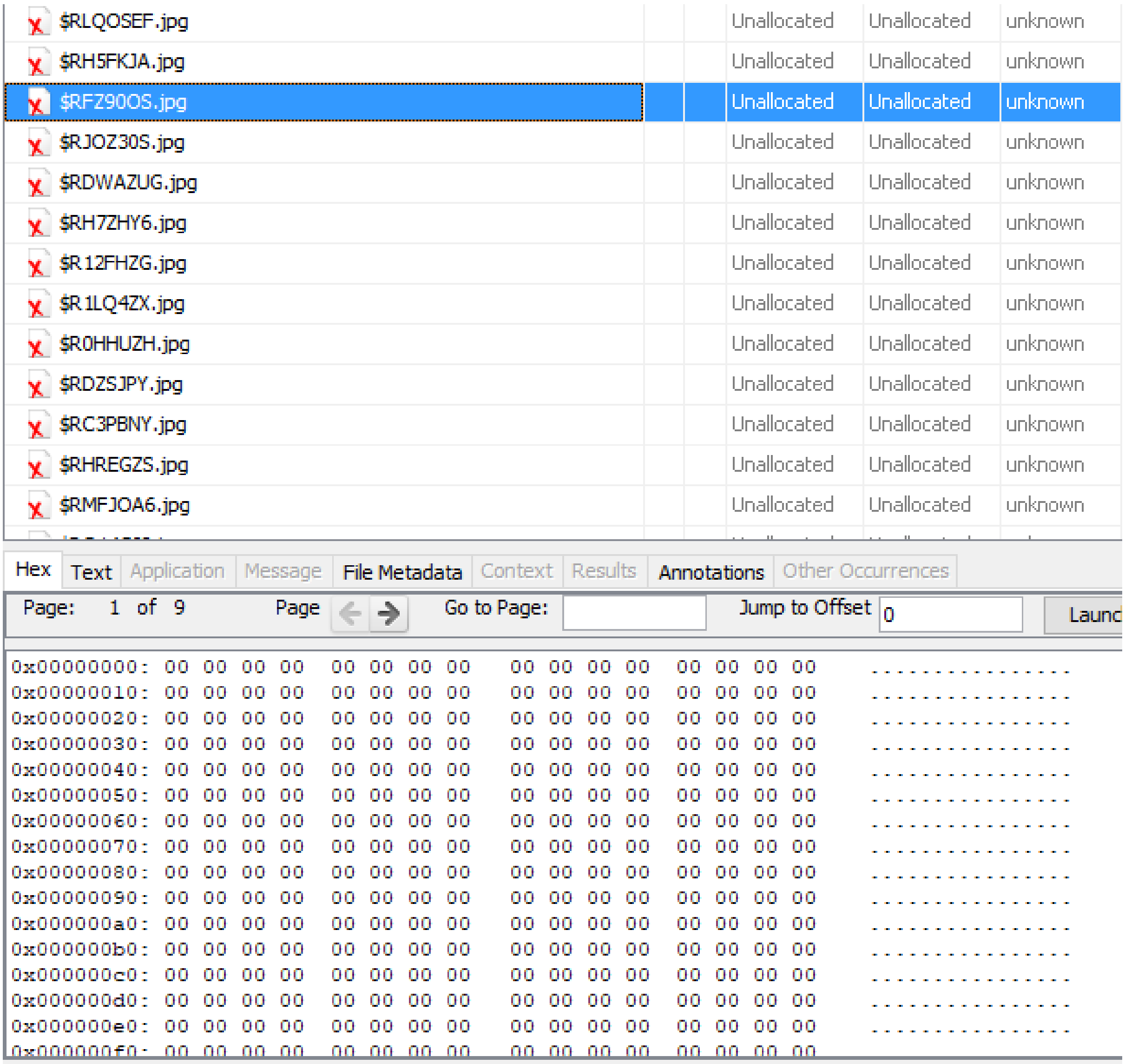

Figure 8 - Hint of evidence pointing to the deleted test files.

We can know for sure these are the files we deleted only thanks to the controlled environment. In a real case scenario, it would be impossible for a forensic investigator to relate these files to anything that could be relevant to an investigation. The only conclusion drawn from this could only be that .jpg files were deleted.

7. Interpretation and Discussion of Results

The results from the experiments were generally quite extraordinary but also somewhat expected. Based on the experiments carried out in this project and experiments carried out in past research TRIM-enabled SSD will not behave the same way as SSDs that do not support TRIM. The process of garbage collection will be sped up quite drastically when it is being supported by TRIM. SSDs by themselves will be quite capable of near-complete corrosion of evidence but the speed at which the event of self-corrosion happens will be much faster when adding TRIM to the equation.

The fastest we could imagine the drive on average was 15 minutes. Based on our results within the first 15 minutes the entirety of the files were damaged and almost all were purged entirely. On average, only a single file out of 20,000 files was 100% recoverable. It was originally thought that the combination of TRIM and garbage collection would be slow enough for files to be recovered out of unallocated space in an experiment timeline consisting of multiple hours between each image instance of the SSD. Another interesting concern is that we could not achieve lower imaging times since data deletion on our second experiment and thus could not confirm our proposed theory. It would be safe to assume that more powerful hardware could achieve faster and better response times along with faster imaging of the drive.

Results between runs of the experiments were expected to be more volatile and less consistent. This proves there is a dangerous potential for digital evidence to be corroded faster as technology progresses. The clear problem for forensic analysts is that TRIM by itself could subsequently lead to an ineffective or misleading digital forensics analysis. We could imagine many scenarios in which the recovery of deleted data is essential. But if the drive alone has deleted that data to the point of no recovery, who is to be held accountable? Sure, a forensic investigator could suspect the existence of a logic bomb put in place to prevent data from being used as evidence as Bell and Bodington suggested back in 2010, however, modern SSDs with active TRIM will logic bomb themselves in order to efficiently manage their lifespan with the only user interference being simply deleting the files. We end up finding ourselves at a period where forensic practice has not yet fully caught up to new technologies.

The evolution of technology affecting data deletion should be expected to hinder forensic investigators, police operations management and court arguments until the field of digital forensics evolves to a point it is able to reliably counter-measure self-corrosion of a drive, this grey area within the field can only hold a grim future.

Consumers who own or are looking to buy SSDs that support TRIM should do so if they are concerned about their security and are not interested in the possibility of recovering any data after it was deleted. The retail price of SSDs is currently at a stage of never seen before affordability, eventually there will be no real benefit to use HDD over an SSD. Data projections hint that HDDs will become extinct soon and the possibility of a world run by SSDs as the champion storage device becomes more and more likely.

8. Recommendations and Guidance for Future Research

There are a lot of valid ideas that could be carried out as research that further analyses the relationship between TRIM and SSDs. More controlled experiments could be based on experiments presented in this project or past experiments presented in past research projects. Any hypothesis that could be used as a starting point for further investigation is welcome as the evidence of proof of concept remains very limited.

Nevertheless, we propose the following:

1. More TRIM-supported SSDs are tested on a larger scale. This would determine whether the combination of TRIM and garbage collection acts differently or the same across different manufacturers.

2. With more computing power available than the used system for this project, there's a good chance faster imaging times could decrease substantially, allowing the possibility for a better hindsight on the speed at which TRIM-enabled SSDs will completely erase data. Perhaps the theory proposed in experiment 2 could then be tested.

3. Developing a novel method to reliably recover more deleted data off TRIM-enabled SSDs or a method to slow down the aggressive garbage collection that takes place due to TRIM.

8.1 The future of digital storage (2020)

Up to this day, SSDs in general have remained a concern for digital forensics investigators. With the widespread standard of TRIM support on both operating systems (Windows 7+, Linux, Mac OS) and SSDs this concern has nothing but worsened over time. Presently, newer SSD technologies like M.2 SSDs can also support TRIM and nothing indicates the proliferation of self-corrosion capable manufactured drives will slow down anytime soon. As SSDs become faster improving read and write speeds, future technological breakthroughs and global implementation of TRIM across different devices could leave integral digital forensic acquisition in the dust. However, overcoming such challenges should remain a priority for digital forensic. New ways to analyse self-corroding drives might surface to light in the upcoming years and that's a possibility that should not be ignored.

9. Conclusion

The project research and study in place were able to answer three out of four questions:

- Can we recover data marked for deletion from unallocated space on a TRIM-enabled SSD?
- How could this investigation impact digital forensics?
- Based on our results, does using a TRIM enabled SSD over a non-trim enabled SSD or HDD increase the security of the user but harm digital forensic investigations?

From an extensive literature review in chapter 3, through the creation of concept proof through experimental investigation and primary research data in chapter 6, to interpreting and analysing the results in chapter 7, conclusions for the project's objective are described below:

- Can we recover data marked for deletion from unallocated space on a TRIM-enabled SSD?

Although minimal, data was recoverable from unallocated space on a TRIM-enabled SSD. Some instances of experiment 1 allowed the data recovery of 0.009% of the original data sample to be reconstituted as an original file.

- How could this investigation impact digital forensics?

The undeniable truth is that digital forensics is lagging and hasn't yet fully caught up to newer technologies in the sense that the possibility to recover unallocated data becomes less and less likely with no real countermeasure for an answer. The way we see things, self-corrosion behaviour on a drive might just become more aggressive, hindering the potential for a forensic investigator to hold full control of integrity in an analysis and thus becoming exposed to the possibility of misjudging presented evidence.

- Based on our results, does using a TRIM enabled SSD over a non-trim enabled SSD or HDD increase the security of the consumer?

Apart from faster read and write speeds, a side bonus is that TRIM will remain as a safe and reliable option if an SSD consumer wants their deleted data to truly be deleted without relying on third party software. The use of a TRIM-enabled SSD will indeed increase the security of the consumer by purging away deleted data, making it near impossible for forensic investigators, police or court investigations to rely on potential deleted data to create evidence.

The Kanban methodology principles applied in this project turned out to be effective. Each task of the project was adapted to meet the final deadline with overhead time for improvements. The tasks were worked on one at a time and the deadline for these tasks were extended depending on whether more time was needed to finish the task without detrimentally affecting other tasks.

9.1 Personal Reflection

The original scope of the project was to find out the speed at which TRIM-enabled SSDs purged files from unallocated space. Even though the experimental phase could not confirm the theory intended for the original scope of the project itself, other interesting data was produced. The information found by following the workflow of the project throughout proved to be quite interesting. A lot was learnt about the relationship between TRIM and SSDs and the practical use of multiple forensic platforms, it was also truly fascinating to experience the implications TRIM-enabled SSDs have brought to digital forensics.

10. References

[1] Christensson, P. (2011, January 13). *SSD Definition*. Retrieved 2019, Nov 23, from https://techterms.com

[2] B. Bell and R. Boddington, Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? Perth: 2010

[3] Shilov, A. (2014). Samsung remains the world's largest maker of SSDs - Gartner. Retrieved from: https://www.kitguru.net/

[4] A. Holst, (2019). Shipments of hard and solid-state disk (HDD/SSD) drives worldwide from 2015 to 2019 (in millions). Retrieved from: https://www.statista.com/

[5] A. Nisbet, R. Jacob, (2019). 18th IEEE Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data And Engineering (p. 1-8). IEEE Computer Society.

[6] S. Sheremetov, (2017) Chip–Off Digital Forensics - Data Recovery After Deletion in Flash Memory, Myrtle Beach: Techno Security and Digital Forensics Conference.

[7] J. Vieyra, M. Scanlon, N. Le-Khac, (2018). Solid State Drives: Where Do We Stand? Forensics and Security Research Group, University College Dublin, Ireland. Conference Paper.

[8] Olson, A. R., & Langlois, D. J. (2008) Solid State Drives (SSD) Data Reliability and Lifetime. National Media Lab White Paper April 2008. http://www.imation.com/PageFiles/1189/SSD_Gov_DataReliability_WP.pdf

[9] Crucial, (2020). What is TRIM? Retrieved from: https://uk.crucial.com/articles/about-ssd/what-is-trim

[10] Pal, A. Memon, (2009). "The evolution of file carving".

B. Carrier, File System Forensic Analysis, MA, Boston:Pearson Education, Addison-Wesley Professional, 2005.

[11] Foremost, (2020). "Introduction to foremost". Retrieved from. http://foremost.sourceforge.net/

[12] B. Carrier, File System Forensic Analysis, MA, Boston:Pearson Education, Addison-Wesley Professional, 2005.

[13] S. Garfinkel, "Carving contiguous and fragmented files with fast object validation", *Proc. 2007 Digital Forensics Research Workshop (DFRWS)*, pp. 4S:2-12, 2007-Aug.

[14]B. Carrier, V. Wietse, C. Eoghan, *File Carving Challenge 2006*, [online] Available: http://www.dfrws.org/2006/challenge.

[15] C. King, T. Vidas, "Empirical analysis of solid-state disk data retention when used with contemporary operating systems", *digital investigation*, vol. 8, pp. S111-S117, 2011.

[16] Z. Shah, A. N. Mahmood, J. Slay, "Forensic potentials of solid-state drives", *International Conference on Security and Privacy in Communication Systems*, pp. 113-126, 2014.

[17] A. Nisbet, S. Lawrence, M. Ruff, "A forensic analysis and comparison of solid-state drive data retention with trim enabled file systems", 2013.

[18] A. Aldaej, M. G. Ahamad, M. Y. Uddin, (2017). "Solid state drive data recovery in open source environment".

[19] G. Bonetti, M. Viglione, A. Frossi, F. Maggi, S. Zanero, "A comprehensive black-box methodology for testing the forensic characteristics of solid-state drives", *Proceedings of the 29th Annual Computer Security Applications Conference. ACM*, pp. 269-278, 2013.

[20] Breton, R., & Bossé, É. (2003). The cognitive costs and benefits of automation. Defence Research and Development Canadaval Cartier (Quebec).: DTIC Document.

[21] Sleuthkit, (2020). Photorec file carving module documentation. Retrieved from: https://sleuthkit.org/autopsy/docs/user-docs/3.1/photorec_carver_page.html