Initial Project Plan

Title – Solid State Forensics:

Investigating the Effects of Garbage Collection on Potentially Volatile Data During the Process of Forensic Extraction of SSDs

Module number: CM3203

One Semester Individual Project – 40 credits

Author: Michael Lawson

Supervisor: Michael Daley

Moderator: Kirill Sidorov

2018

Cardiff University

School of

Computer Science and Informatics

Contents

Project Description

This project aims to investigate how the garbage collection and trimming functions impact the effectiveness of forensic investigation of Solid State Drives (SSDs). At present, it is unclear what triggers the garbage collection, so there is potential for the loss of evidence at unknown points in the forensic process (Bell and Boddington, 2010).

Historically, Hard Drive Discs (HDDs) were the best way to store data and were widely used for forensic investigation and are still common place in the field. They use magnetic storage to retrieve digital information and store it for future use. However, within the last decade, SSDs have become far more accessible, reliable and process faster than HDDs (McKemmish, 1999).

SDDs store data using integrated circuit assemblies and, unlike HDDs, lack any moving parts (Bednar and Katos, 2011). They are innovative in the way they never write data to the same place, instead writing it to the translation layer, and subsequently to a lesser used location. This minimises damage to blocks when the file is updated multiple times.

Although the popularity of SSDs is increasing within the public domain, they have shortcomings which have the potential to jeopardise the full recovery of data during forensic investigation. The two functions of SSDs that this project will focus on are known as trimming and garbage collection. They often work alongside one another during the process of erasing blocks that have been marked by the operating system to be deleted. These functions can work in the background of an operating system and can have negative impacts on a forensic examination. Using the experimental investigation conducted in this project, I aim to discover how these functions the recovery of data and identify the point at which the loss of any data occurs.

The idea behind this project became apparent after Gwent Police suggested that research into this subject will provide useful insight into future forensic investigations. For the experiment, I have acquired 3 SSDs from different manufactures. Firstly, an image will be generated to be transferred to each SSD. The image will be exactly the same to maintain continuity throughout the investigation. Then files from the image will be deleted at different intervals and locations on each drive. These files will then be recovered to gain an understanding of how much data has been lost through garbage collection and trimming and if the MD5 has altered in any way.

Aims and Objectives

Primary

1. **Determine the differences between the effects of each SSD's garbage collection and trimming processes on an image**.
    - This will be achieved by deleting files from each SSD and then attempting to recover them at different intervals. Once recovered, the differences between the recovered images will be compared against each other to see which ones performed best.
2. **Understand what triggers garbage collection**.
    - Research will be conducted to gain insight on the technical processes of garbage collection to build an idea of the potential triggers.
3. **Suggest ways of preventing garbage collection**.
    - After research and experimental practice, I will make suggestions for potential ways in which garbage collection can be prevented or controlled during forensic analysis.

Secondary

1. **To discover whether different write blockers have differing effects when used on SSD image recovery.**
    - Previous research has suggested that the use of write blockers may have a positive impact on the recovery of data. Therefore, I theorised that different combinations of write blockers and SSDs may have the ability to prevent garbage collection in varying degrees. As a secondary aim, I will test this if time allows.

Project Constraints

1. In the experiment there will be 3 different SSDs and 1-3 different write blockers used. Although relations between them may be revealed during experimentation, it is a relatively small sample size. Therefore, to validate any claims made from this experiment, further research and testing would need to be conducted.
2. Each SSD manufacturer has a different secret algorithm for the wear levelling and garbage collection. Some manufacturers are more open with this information than others, therefore, challenges may be faced when attempting to find solutions.

Project Deliverables

The predicted outcome of this project is to find conclusive results from the experimental work, gaining an understanding of when and why garbage collection occurs and if it is preventable. Subsequently, a body of work will be produced outlining the methods and results of this experiment, with a critical discussion at the end. Any difficulties faced during the project will be stated alongside any recommendations for future research in this field.

Work Plan

Week 1 –

- Submit initial plan (05/02/2018)
- Research general background knowledge
- Check and prepare equipment

Week 2 –

- Research specific criterial for the experiment; including FDK, chipsets and garbage collection and trimming commands
- Set up equipment

Week 3 –

- Meet first milestone: complete background and experimental research
- Create an image of uncopyrighted material and transfer it to the SSDs in preparation for the experiment
- Have a supervisor milestone meeting to discuss research results before experimentation begins

Week 4 –

- Write introduction to dissertation, using the research found in the previous weeks
- Start experiment by deleting the data from the SSDs and attempting the process of recovery
- Review Gantt Chart and make any adjustments if needed

Week 5 –

- Begin methodology based on experimental methods used so far
- Continue experimentation, trying out different methods to gain the best results

Week 6 –

- Meet second milestone: Completion of all experimental practices
- Finish writing your methods based on your practices and ensure the first half of the dissertation write up is complete.
- If experimentation is complete and time allows, attempt to test the affects of write blockers on the garbage collection function
- Have a supervisor milestone meeting to discuss experiment results

Week 7 –

- Collate and analyse the results gathered from experimentation

Week 8 –

- Complete analysis and write up of results
- Prepare notes for discussion
- Review Gantt Chart and adjust if needed

Week 9 –

- Finalise all the results found and ensure that the previous chapters including introduction and methods are complete
- Outline the plan for the discussion and begin the write up of findings

Week 10 –

- Continue write up of discussion, drawing on previous research to critically analyse the results and outcomes of this project

Week 11 –

- Continue write up of discussion, drawing on previous research to critically analyse the results and outcomes of this project

Week 12 –

- Meet third milestone: Completion of all write up
- Finish the write up of discussion and conclude the project
- Ensure all chapters include all relevant information and implement the final structure of the written report
- Have a supervisor milestone meeting to ensure report structure and direction of report are correct

Week 13 –

- Gather all chapters together and ensure they are in order and include all relevant information
- Format and proof-read dissertation

Week 14 –

- Meet forth milestone: Hand in dissertation project
- Complete final formatting
- Print and bind project

Gantt chart

Gantt chart					Weeks													
ID	Task	Start date	End date	Duration	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	**Research and Background**			3 weeks	🟦	🟦	🟦◆											
1.1	Completion of project plan	05/02/2018	11/02/2018	1 week	🟩													
1.2	General background and application of SSDs	05/02/2018	18/02/2018	2 weeks	🟩	🟩												
1.3	Research FDK recovery programme	11/02/2018	25/02/2018	2 weeks		🟩	🟩											
1.4	Research the 3 SSDs and their chipsets	11/02/2018	25/02/2018	2 weeks		🟩	🟩											
1.5	Research garbage collection and trimming commands	11/02/2018	25/02/2018	2 weeks		🟩	🟩											
2	**Implementation**			9 weeks	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦◆		
2.1	Write introduction	25/02/2018	04/03/2018	1 week				🟩										
2.2	Detail a step by step methodology	04/03/2018	18/03/2018	2 weeks					🟩	🟩								
2.3	Collate and analyse the results	18/03/2018	08/04/2018	3 weeks							🟩	🟩	🟩					
2.4	Critically analyse the results within a discussion and conclude the findings	01/04/2018	22/04/2018	4 weeks									🟩	🟩	🟩	🟩		
3	**Experiments**			6 weeks	🟦	🟦	🟦	🟦	🟦	🟦◆								
3.1	Prepare equipment and ensure everything is available	05/02/2018	18/02/2018	2 weeks	🟩	🟩												
3.2	Create images and transfer them to SSDs	18/02/2018	25/02/2018	1 week			🟩											
3.3	Delete then attempt to recover images and recording the results	25/02/2018	11/03/2018	2 weeks				🟩	🟩									
3.4	Write blocker testing	11/03/2018	18/03/2018	1 week						🟩								
4	**Final Report**			3 weeks	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦◆
4.1	Implement final report structure	15/04/2018	29/04/2018	2 weeks												🟩	🟩	
4.2	Formatting and proof reading	22/04/2018	06/05/2018	2 weeks													🟩	🟩
5	**Continuous tasks**			14 weeks	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
5.1	Supervisor meeting	Start date		7 weeks	🟩		🟩		🟩		🟩		🟩		🟩		🟩	
5.2	Review Gantt Chart			6 weeks		🟩		🟩		🟩		🟩		🟩		🟩		

Key	
Milestones	◆
Task Targets	🟩
Weekly Scale	🟦

References

Bednar, P., & Katos, V. (2011). SSD: New Challenges for Digital Forensics. In A. D'Atri, D. Te'eni, & M. De

Bell, G. and Boddington, R. (2010). Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?. *Journal of Digital Forensics, Security and Law*.

McKemmish, R. (1999). *What is forensic computing?*. Canberra: Australian Institute of Criminology.