Roli Bolorunfe
Patience Jato
Davia McKenzie
Obi Oguh

Solution Design Description

Problem Statement:

Since commonly known attack methods have become increasingly sophisticated, we must help determine which memory forensic tool provides the best physical memory coverage against those common attack methods in order to support and secure operational environments

➢ *SECTION(1)*

Designs of Methods:

- Method 1 (Davia McKenzie):

The whole purpose of our research is to find the best memory forensic tool that will help to prevent attacks. This tool is detailed by the process of which we conduct forensics. I believe that the best way to tackle this problem can be detailed in 4 steps:

1. Identify and acquire the data that needs to be protected
2. Process the collected data, extracting important pieces of information
3. Analyze the extracted data
4. Report what was found from analyzing the data

- Method 2:

To prevent attacks the process of memory forensics should occur by:

1. Locate the memory or data within the specified memory that is needed
2. Identify the issues within the memory and what are you looking for during the memory forensics process.
3. Acquire the data
4. Extract pieces of information that will be used for further analysis
5. Analyze the extraction
6. Compare analysis to data that theoretically describes what it contents should look like
7. Provide a report that describes the result.

- Method 3 (Patience Jato):

Create a digital forensics tool with investigative techniques to identify and collect the information on a digital storage for maintenance, debugging, data recovery, and reverse engineering of computer systems in private settings. This third idea focuses on creating a tool for data forensics through live technique on the RAM

1. Collect available data and digital media that requires investigation
2. Examine the data through cloning or imaging the data, using method such as bit stream

Roli Bolorunfe
Patience Jato
Davia McKenzie
Obi Oguh

3. Analyze and make the recovery to store back the file and the folder
    a. RAM in the computer system will be analyzed
    b. RAM analysis capture is a process of capturing live memory from a running computer system.
    c. The goal is to find evidence of the intrusion from the attacker.
4. Create scientific reporting and to presenting the investigation report and evidence

- Method 4 (Roli):

Another design solution stems from the 'Investigation Model' technique. This model follows a step-by-step procedure of extracting volatile data and inspecting malicious code from suspicious programs.

1. The first phase is the 'preparation phase' wherein an application is compiled in order to derive the debugging information of the data we want to inspect. We make use of the 'Debug mode' feature in Visual Studio to produce debugging information during the compilation process
2. The next phase is the 'imaging phase' which basically involves taking in the memory dump of the computer while the target application is still running.
3. Following this is the 'parsing phase' wherein the Program Database file is parsed to to extract all global and local variable names as well as their virtual addresses and data types. The Microsoft PDB Parser is used to display the parsed information.
4. Finally, the 'inspection phase' involved mapping the parsed symbol from the Program Database file to the application's memory.

➢ *SECTION(2)*

Description of Method 1, 2,3 & 4

Method 1

Pros:

- The process description is straightforward
- Describes a process from start to finish
-

Cons:

- Process can be seen as vague
- Doesn't describe where we can locate or isolate the data needed for analysis

Roli Bolorunfe
Patience Jato
Davia McKenzie
Obi Oguh

Method 2

Pros:

- Has a more descriptive process
- Requires the process to be thorough

Cons:

- No Cons

Method 3

Pros:

- On trend with new investigative techniques
- RAM stores all the critical information needed for the analysis and evidence gathering process

Cons:

- If computer is shut down, there is a loss of critical information
- New concept that is still in development

Method 4

Pros:

- Provides an explicit breakdown of the data forensics process
- Includes an experimental setup procedure, thereby making it more reliable
- Easy to follow step-by-step process
- Relatively simple to implement due to easy accessibility to tools

Cons:

- May be time consuming

➢ *SECTION(3) (Roli)*

After conducting extensive research and weighing the pros and cons of the solution designs, we were able to successfully determine our top solution design: Method 4. Method 4 entails finding data within a given memory location and then compiling an application in order to derive the executable file we want to investigate.

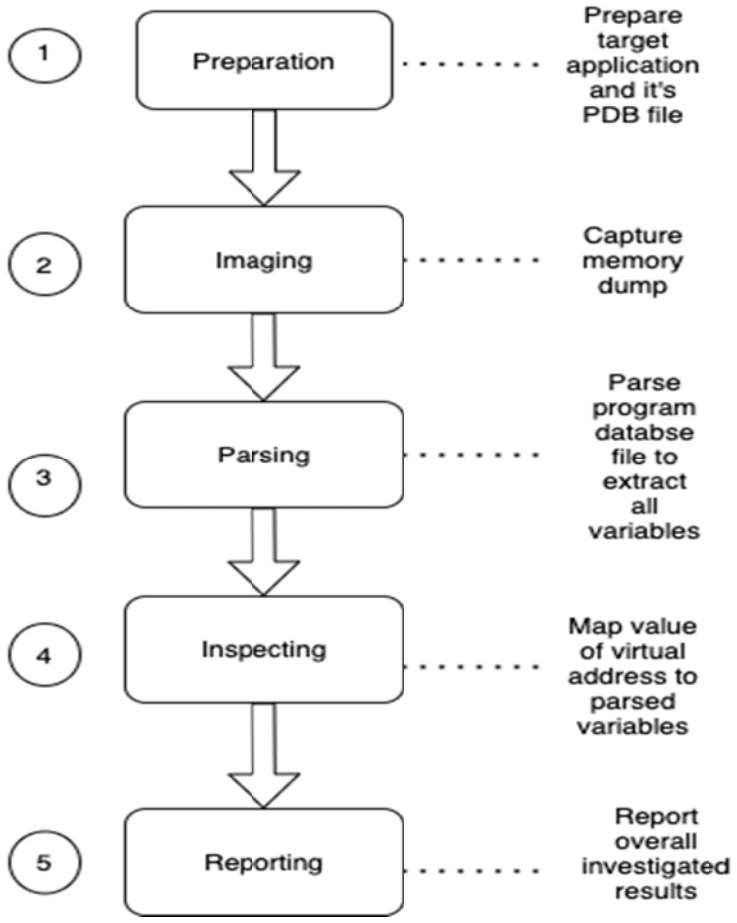
Our thought process for selecting Method 4 was heavily influenced by it's pros as well as it's very thorough process. We were able to recognize which method best suits our project's short and long term goals. In comparison to Method 1, Method 4 has a more detailed and clear process whereas Method 1's process was more obscure and less defined. Method 1 does give a

description of the process from beginning to end. It, however, does not have an experimental setup stage to prove it's credibility..

Weighing these pros and cons, while putting our end goal in mind, enabled us to select Method 4 as the best possible design solution for this project.

➢ *SECTION(4)(Roli)*

As discussed earlier, our top solution design for this project is Method 4. This is because we believe Method 4 is more descriptive and would provide us with an efficient method to extract critical data from digital devices.



In carrying out this study for memory forensics, the first step to be taken is **1** to prepare the target application and it's PDB file. The purpose of this study is to ensure the procedure for extracting

memory is well-defined and established. Having carried out phase **1 ,** the next step is to complete **2** the imaging phase. The imaging phase is where the memory dump of the target computer is taken. Next, parsing is carried out in phase **3.** Here, global and local variable names are extracted as well as relatively virtual addresses and primitive data types. Following this, in phase **4,** volatility capabilities are used to dump the virtual address space of the target application. The results of the first four phases is documented in a study report created to document all the processes taken, recommendations and lessons learnt in phase **5**