# Copycat Pi (Data Acquisition Tools)

Muhammad Ikhmal Hakim bin Mohd. Nazri
University of Kuala Lumpur Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
livernote@gmail.com

Dalilah Abdullah
University of Kuala Lumpur Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
dalilah@unikl.edu.my

***ABSTRACT*- Copycat Pi is a modified raspberry pi that will be turn into a data acquisition tools. The function of the Copycat Pi is to copy all the data from source drive to the targeted drive. The method that will be involved when copying the data is logical acquisition method. For this project, the type of the file be copied is disk to disk. The copied also will be verified with md5 hashing to ensure the integrity of the disk. Evidence data from the crime scene is vulnerable to the modification or being delete if the forensic team did not act fast enough.**

***Keywords—data acquisition, raspberry pi, disk to disk and disk to image***

## I. INTRODUCTION

This chapter contains the introduction to the research which the research is concerned, the problem statement of the issue that is studied, aim and objectives of the study, the scope of the project and the significance of the study.

Copycat Pi is a modified raspberry pi that will be turn into a data acquisition tools. The function of the Copycat Pi is to copy all the data from source drive to the targeted drive. The method that will be involved when copying the data is logical acquisition method. For this project, the type of the file be copied is disk to disk. The copied also will be verified with md5 hashing to ensure the integrity of the disk. Evidence data from the crime scene is vulnerable to the modification or being delete if the forensic team did not act fast enough.

The project will be on hardware platform and some codes that includes Raspberry Pi board, Ubuntu mate, Gtk dialog, DD scripting, and USB as source and target for copying to prove that copycat pi can be used to enhance security and creating more secure environment.

## II. LITERATURE REVIEW

Nowadays, the increasing of cyber-crime has catch a lot of attention in every part of the world. Therefore, cyber forensic team put a lot of effort to fight this cyber-crime to create a better way of living in the cyber world. The effort to preventing cyber-crime seems not ending because of the increasing of technology which creates more intelligent user to do many different type of cyber-crime. Furthermore, with the current economy status it is difficult for a new forensic team to involve in this area because of the cost to buy a forensic tool is so expensive.

### *2.1 What is Data Acquisition*

Data acquisition is the act of taking possession of or obtaining control of data and adding it to a collection of evidence. To do a data acquisition, a method called data duplication is being used. Based on (Ec-Council) data duplication is the act of making a copy of data of already acquired to preserve the original evidence in pristine condition.

### *2.2 Operating System (OS)*

There are two different popular operating systems that have been used to run this data acquisition process. Windows and Linux both have their pro and cons when doing the data acquisition process. There are several popular data acquisition tools for example xcopy, diskcopy, AcessData FTK and ilook.

### *2.3 Write Blocker*

To ensure there is integrity when the process of imaging, there are tool calls write blocker being used. Write blockers is a tool that read-only access to data device without compromising the integrity of the data. By using the write blocker, the protection of data can be guarantee when bringing the data into the custody. There are two type of write blocker which are hardware and software tool, this tools act the same way which is to prevent writes to the storage device.

Figure 2.0: Write Blocker.

### *2.4 Forensic Imaging Tools at Market*

One of the popular tools is Tableau TD3 Forensic Imager, this tools can receive input from Sata, USB, FireWire and Ethernet with an expansion that can be purchase which can receive input from SAS, IDE, Micro-SATA, additional storage device and many more. This tools also have around 7 inch of touch screen display to make it user friendly. The standard operation of this tools is Disk-to-disk clone, Disk-to-file, Format, Wipe, Hash, HPA/DCO detection and removal and Blank Disk Check. The imaging speeds for this tools is 6 GB/minute same with the wiping speeds which is 6GB/minute also. The price for this Tableau TD3 Forensic Imager is roughly around 2,500 dollar for the tools only.

Figure 2.1: Tableau TB3 Forensic Imager

Next popular forensic imaging tools that being sell at the market is Forensic Imager TX1. This tool also can receive input from Sata, USB, PCIe, SAS, FireWire, IDE and network shares. The difference that this tool can do is by doing two forensic job simultaneously. For the destination source, this tool can produce up to four destinations at once. It also provides LED information at the device. The standard operation that is provide still same, which is Disk-to-disk clone, Disk-to-file, Format, Wipe and Hashing. This tool also come with additional kit that come with additional price. For the basic kit of this tool will cost around 3,299 dollars and the additional kit will be around 89 dollar to 189 dollar.

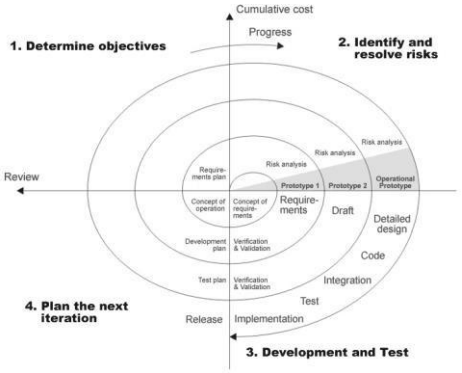
Figure 2.2: Tableau Forensic Imager TX1

### *2.5* Hashing

Hashing is the transformation of a string of character that use shorter fixed character to represent the original string. Hashing also being used as indexed to retrieved item from the database since shorter hashed key easier to find than searching the original value. Hashing is different from encryption because by doing hashing it is meant to never being reversed.

## III. RESEARCH METHODOLOGY

The chosen research model is spiral method. Starting with determining the objective of the study, then the risk that could happen will be identify. After that, start with the designing the interface of the program and start the code. After finished, the program will be testing whether it is qualified to perform without error. If there is error found, move to the next process, which is to plan the improvisation from the current program. The process will be spinning as the model until it reach its perfect condition that can make it released. Once have been release, the next iteration will be plan for upcoming progress.




(Boehm, 2000).

Figure 3.0: Copycat Pi Research Model

## IV. PROTOTYPE AND DEVELOPMENT

Project development are the most important part that need to be focus on when developing the Data Acquisition Tools using Raspberry Pi. From this chapter, prototype project is develop based on the planning and logical design that had been created to ensure it meet the requirements and also using the methodology that had been selected as the procedure to develop the prototype.

### *4.1 System Architecture*

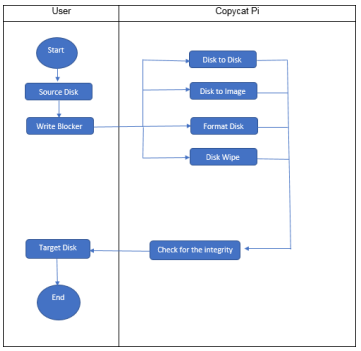



Figure 4.0: System Architecture.

### *4.2 Functional Requirements*

#### *4.2.1 Disk to Disk module*

This module is one of the main module that required in this tool. Below in Figure 7 shown us the part of coding that are required to do the disk to disk module.

```
export SELECT3_DIALOG=

<window title="Copycat PI" width-request="400" height-request="200">
<vbox>

    <frame Progress>
    <text>
      <label>Duplication process is happening.</label>
    </text>
    <progressbar>
      <input>dd if=/dev/sdd | pv -s 4G | dd of=/dev/sde bs=4096 </input>
    </progressbar>
  </frame>
```

Figure 4.2: Disk to Disk Coding

#### *4.2.2 Disk to Image module*

This other main module that is required in this tool is disk to image module. Below in Figure 8 shown us the part of coding that are required to do the disk to image module.

```
export SELECT1_DIALOG='

<window title="Copycat PI" width-request="400" height-request="200">
<vbox>


    <frame Progress>
    <text>
      <label>Duplication process is happening.</label>
    </text>
    <progressbar>
      <input>dd if=/dev/sda of=dev/sdb/your-backup.img</input>
      <action>launch:END_DIALOG</action>
    </progressbar>
  </frame>
```

*Figure 4.2:* Disk to Image Coding

### *4.3 Flow Chart*

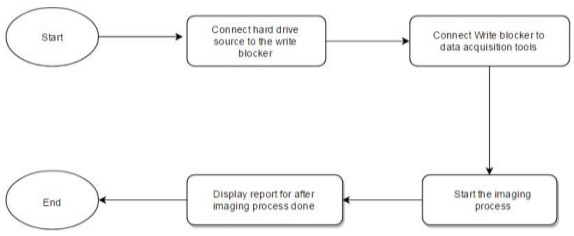



Figure 4.3: Flow Chart

This flow chart in figure 4.3 show the flow of the process when doing the data acquisition.

## V. TESTING RESULT AND DISCUSSION

### *5.5 Security Elements in System*

#### *5.1.1 Functional Testing*

The functional testing focusing on ensuring each of function that created on purpose project are properly working. This functional of purpose project was tested following the flow from one module to other then following testing the whole system function.

| Test Case Field | Detail |
|---|---|
| Test Case ID | T_F_T_Unit_03 |
| Test Case Name | Testing Copycat Pi File to Disk button function |
| Purpose | To test the function of the button |
| Initiation Criteria | The Copycat Pi program need to launch. |
| Executions Steps | 1. Launch Copycat Pi<br>2. Press the button on the interface |
| Expected Results | The button will copy data from source disk and convert the file into image type of disk function. |

Figure 5.1: Test Case for Copycat File to Disk button function

| Test Case Field | Detail |
|---|---|
| Test Case ID | T_F_T_System_02 |
| Test Case Name | Testing Disk to Image function in Copycat Pi |
| Purpose | To test function of Copycat Pi to do Disk to Image data acquisition |
| Initiation Criteria | The Copycat Pi program need to launch. |
| Executions Steps | 1. Launch Copycat Pi<br>2. Press the continue button on the interface<br>3. Press the Disk to Image function |
| Expected Results | The function will copy the data using Disk to Image technique |

Figure 5.2: Test case for Disk to Image function in Copycat Pi

| Test Case Field | Detail |
|---|---|
| Test Case ID | T_F_T_System_03 |
| Test Case Name | Testing Disk Wipe function in Copycat Pi |
| Purpose | To test function of Copycat Pi to do Wipe Disk |
| Initiation Criteria | The Copycat Pi program need to launch. |
| Executions Steps | 1. Launch Copycat Pi<br>2. Press the continue button on the interface<br>3. Press the Disk Wipe function |
| Expected Results | The function will wipe the source disk. |

Figure 5.3: Test case for Disk Wipe function in Copycat PI

#### *5.1.2 Non-Functionality Testing*

The Non-Functional testing is focusing on the ability and the performance of any hardware involve in this project. This Non-Functional test involve many different aspects to be test to know the limit of the program.

| | |
|---|---|
| **Test Case ID** | T_NF_T_Performance_01 |
| **Test Case Name** | Testing Copycat Pi performance |
| **Purpose** | To test the speed data transfer for the Copycat Pi during data acquisition process |
| **Initiation Criteria** | Choose Disk to Disk or Disk to Image function to test the data transfer speed |
| **Executions Steps** | 1. Launch Copycat Pi<br>2. Press the ok button at the introduction page<br>3. Press Disk to Disk or Disk to Image button |
| **Expected Results** | The interface will show the current speed of data being transfer. |

Figure 5.4: Test case for Copycat Pi performance

| Test Case Field | Detail |
|---|---|
| **Test Case ID** | T_NF_T_Security_01 |
| **Test Case Name** | Testing Copycat Pi Security |
| **Purpose** | To test the integrity of the source disk by using write blocker |
| **Initiation Criteria** | The source disk must connect with the write blocker before the data acquisition process |
| **Executions Steps** | 1. Insert source disk into the write blocker<br>2. Ensure the write blocker is connected to the source disk<br>3. Check the status of the source disk |
| **Expected Results** | The source disk can be read as read-only and cannot be tamper. |

Figure 5.5: Test case for Copycat Pi security

| Test Case Field | Detail |
|---|---|
| **Test Case ID** | T_NF_T_Usability_01 |
| **Test Case Name** | Testing Copycat Pi Usability |
| **Purpose** | To test the resemblance of the hexadecimal between the source disk and the target disk after data acquisition process. |
| **Initiation Criteria** | The data acquisition process must be complete before comparing the hexadecimal of the disk |
| **Executions Steps** | 1. Open the source disk in the hex editor program<br>2. Open the target disk in the hex editor program<br>3. Compare the arrangement of the disk hexadecimal |
| **Expected Results** | The source disk can be read as read, write, execute, and can be tamper. |

Figure 5.6: Test case for Copycat Pi usability

### *5.4 Discussion*

Copycat Pi had been tested based on the two methods that had been used. From the testing, we can assure that the Copycat Pi had been tested based on the two methods that had been used. From the testing, we can assure that the project objective are met. We do observe the functionality of the Copycat pi doing four function that is assigned to it. The compatibility, usability and performance also studied and noted. And from the security testing point of view, with the addition of write blocker the data from source disk can't be tampered.

## VI. CONCLUSION AND RECOMMENDATION

It can be concluded that this project has achieve its' objective with successful functioning after done to do the main function that have been set which is to do data acquisition using two different kind of method which is disk to disk method and disk to image method. This project also fulfills its objective which is to create a new kind of data acquisition tools where it could lead to giving a chance to student or lecture that before this only learned about it and now they can use it for their study and can prepare before use it in the real work situation.

### *6.1 Recommendations*

For this project, several improvements can be add in this project for future enhancement. Due to several limitations in this project, some modification and improvement can be added. Below are several recommendations can be implement in the future:

i) Create a new function which is to generate report after done data acquisition process.
ii) Create a new function to capture a picture of person that do the data acquisition using Copycat pi.
iii) To use another type of input other than USB to be used with Copycat Pi.

## REFERENCE

[1] Barry Boehm "Spiral Development: Experience, Principle and Refinements" (Boehm & Hansen, 2000).

[2] Nelson, B., Phillips, A., & Steuart, C. (2015). *Guide to computer forensics and investigations*. Boston, MA: Course Technology Cengage Learning.

[3] EC-Council (2016) "Computer Hacking Forensic Investigator v8 ", EC-Council Official Certification.

[4] Computer Forensics, Computer Forensics Training, Forensic Training, Forensic Computers, Forensic Hardware, and Forensic Software Solutions for the Computer Forensic Community. (n.d). Retrieved April & May 2017, from https://www.digitalintelligence.com/.