Automated Mode Changer for Portable Media Player from Media Transfer Protocol to Mass Storage Class

by

Nurul Ain binti Md Yazid

Dissertation submitted in partial fulfillment of
the requirement for the
Bachelor of Technology (Hons)
(Information and Communication Technology)

JANUARY 2011

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

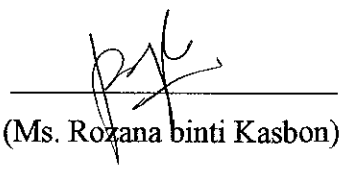
Automated Mode Changer for Portable Media Player from Media Transfer Protocol to Mass Storage Class

by

Nurul Ain binti Md Yazid

A project dissertation submitted to the
Information and Communication Technology Programme
Universiti Teknologi PETRONAS
in partial fulfillment of the requirement for the
BACHELOR OF TECHNOLOGY (Hons)
(INFORMATION AND COMMUNICATION TECHNOLOGY)

Approved by,

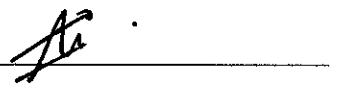


(Ms. Rozana binti Kasbon)

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK
January 2011

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.



(NURUL AIN BINTI MD YAZID)

ACKNOWLEDGEMENTS

First of all thanks to the Merciful full God of Allah to allow me to finish this project, without His bless this project should unable to reach the current progress and accomplish. All the devotion and effort were dedicate to Mrs. Norbaya as caring and supportive parent to encourage me in many ways to stay focus and reach the goal of the project and other study as complete the degree title.

The most wonderful, supportive and cooperative lecturers of Universiti Teknologi PETRONAS is part of the main contributor in this project. To name it few here, started with Ms. Rozana Kasbon as the most supportive and optimistic supervisor, Ms. Sarah Khadijah Taylor as industrial internship supervisor from CyberSecurity Malaysia who support the idea on Automated Mode Changer for Portable Media Player from Media Transfer Protocol to Mass Storage Class project and to all external lecturers during seminar presentation who gave the critics and moral insights on developing the project.

Thank you also to colleagues' and friends who please to lend their ear to listen on draft idea of the project and spare their time for critics and supports during project research and implementation. Lastly, thanks again to all the people who involved in this project and all the efforts which contributed are really appreciated.

ABSTRACT

Portable media player (PMP) is a digital device that used for playing audio, video and graphic files. Despite its popularity feature for storing and playing audio files; it can also store other types of data, namely .doc, .pdf or .avi. Its portability makes it easy for user to store any data into the device. Investigators now need to be prepared for such devices, as they might contain evidence of a crime. To complicate things further, each PMP may have its own proprietary file system, format and technology. Problem faced by forensic analyst is that forensic software could not access PMP with proprietary protocol and found a dead end. The aim of this project is to develop an application that can update or change media transfer protocol in a PMP to mass storage class to give access to forensic software without tempering any data or metadata from the devices. There are five phases in developing this application: Planning, Analysis, Design and Development, Testing and Further enhancement, and Delivering application phase. Media Transfer Protocol (MTP) player now is successfully converted to Mass Storage Class player, but it has to be done manually, which may consume time. This project proposes an application that can automate those steps to tackle the time advantage.

TABLE OF CONTENTS

CHAPTER 1:	**INTRODUCTION**		**1**
	1.1	Background	1
	1.2	Problem Statement	5
	1.3	Objectives	5
	1.4	Scope of Study	5
CHAPTER 2:	**LITERATURE REVIEW**		**7**
	2.1	Background: Portable media player	7
	2.2	Protocols in PMP	7
	2.3	Forensic Analysis on PMPs	8
	2.4	Further Enhancement	9
CHAPTER 3:	**METHODOLOGY**		**10**
	3.1	Development Life Cycle Agile	10
		3.1.1 Phase 1: Planning	10
		3.1.2 Phase 2: Analysis	11
		3.1.3 Phase 3: Design and Development	11
		3.1.4 Phase 4: Testing and Further Enhancement	11
		3.1.5 Phase 5: Deliver application	12
	3.2	Software/Tools	12
	3.3	Hardware	13
CHAPTER 4:	**RESULTS AND DISCUSSION**		**14**
	4.1	Planning phase	14
	4.2	Activity diagram	14
	4.3	Updating process	16
	4.4	System Architecture	16
	4.5	Functional decomposition diagram	17
	4.6	Graphical User Interface	19
	4.7	Implementation on USB Write-Protect Module	20
	4.8	PMP Detection Module	22
	4.9	PMP Driver-check Module	23
	4.10	PMP Driver-update Module	24
	4.11	Final Output	25
	4.12	Testing phase	25
	4.13	Testing with forensic software	27
CHAPTER 5:	**CONCLUSION**		**29**
	5.1	Conclusion	29
	5.2	Recommendation	29
REFERENCES			**30**
APPENDICES			**31**

LIST OF FIGURES

Figure 1.1 Sony Walkman NZ-E443
Figure 1.2 Apple iPod Shuffle
Figure 1.3 Phillips EXP250
Figure 1.4 Epson P-3000
Figure 1.5 Digital forensic methodology
Figure 2.1 Workstation recognized MSC player as Removable Drive
Figure 2.2 Workstation recognized MTP player as Portable Device
Figure 3.1 Adapted agile methodology to suit this project
Figure 4.1 Activity diagram
Figure 4.2 System Architecture
Figure 4.3 Functional decomposition diagram
Figure 4.4 Main GUI
Figure 4.5 Code snippet for main GUI
Figure 4.6 Code snippet for USB write-protect module
Figure 4.7 Current status of USB Write-Protect
Figure 4.8 Updated status of USB Write-Protect
Figure 4.9 USB Write-Protect is already turned ON
Figure 4.10 Connected PMPs were detected by DevCon
Figure 4.11 MTP devices found connected to the workstation
Figure 4.12 Driver identified for MTP player
Figure 4.13 Current driver status
Figure 4.14 Command for updating driver
Figure 4.15 Updated MTP player
Figure 4.16 Dialog box that visible to user at the end of process
Figure 4.17 Previously, MTP was identified as Portable Media Player
Figure 4.18 MTP player was recognized as Removable Disk
Figure 4.19 PMP was recognized under WinHex
Figure 4.20 PMP was recognized under DiskDigger
Figure 4.21 PMP was recognized by Recuva

LIST OF TABLES

Table 4.1 Result of application using convertible PMPs
Table 4.2 Result of PMP recognition using several forensic software

ABBREVIATIONS AND NOMENCLATURES

Term	Meaning
DAP	Digital Audio Player
GUI	Graphical User Interface
Image	Exact bit-by-bit copy of evidence
MSC	Mass-storage Class
MTP	Media Transfer Protocol
PMP	Portable Media Player
WPD	Windows Portable Device

CHAPTER 1
INTRODUCTION

"Portable media player (PMP) is a consumer electronics device that is capable of storing and playing digital media. Digital audio players (DAP) that can also display images and play videos are PMPs."

-iPod Source

1.1 BACKGROUND

Portable media player has evolved from the simple digital audio player (MP3 player) to high-storage capacity player that comes with colored-screen (MP4 player). This electronic device advanced from only capable of storing audio files to storing and viewing video files, pictures, recording voices, receiving FM radio transmission and some manufacturers even include games in their PMPs. Some PMPs even come with built-in speaker and touch screen feature. These players gain its popularity especially among the youth as it offers them to take digital content with them on the go since it is portable and small. There are four types of PMP available in the market. They are:

i. Flash-based player

   This player stored digital content in its internal flash memory. Example of flash-based player is Sony Walkman NZ-E443.

Figure 1.1: Sony Walkman NZ-E443

ii. Memory-card media player

This type of media player relies on external memory card to play media and store digital files. Example of memory-card media player is Apple iPod Shuffle.

Figure 1.2: Apple iPod Shuffle

iii. MP3 CD player

This type of player plays MP3 files directly from CDs, without storing any digital files within its player. Example of MP3 CD player is Phillips EXP2550.

Figure 1.3: Phillips EXP250

iv. Hard-drive based player

This type of player is the largest and heaviest among others as it contains hard-drive as a medium to store data. Example of hard-drive based player is Epson P-3000.

Figure 1.4: Epson P-3000

The capability of this player to store digital content and mass usage of it create new opportunities for criminal to manipulate the technology. According to London Evening Standard in 2007, MP3 player had been used by a gang to store information related to their crime. One team of hackers stole more than £200,000 after using MP3 player to tap in to transactions on free-standing cash machines in London and created dozens of cloned card on the Internet for cash withdrawals and online purchasing. One of the criminals, Parsons, attached his MP3 player at the back of an ATM (Automated Teller Machine) and illegally taps into telephone lines used by customer during transaction. Data was recorded into his MP3 player and transmitted down the phone lines. Then, computer technology was used to decode the tones from ATM transaction to clone new credit cards.

Based on this situation, PMPs are not just another 'music player' that it used to be. Nowadays, PMP's are capable of storing multiple type and different sizes of data. Thus, PMPs are among the items that should be seized during raid or seizure alongside with hard-disks, thumbdrives, mobile phones, etc. Its technology and complexity should be studied in order to perform forensic analysis on it.

In forensics, best practices and procedures are followed closely as it will affect the result later on. Digital forensic methodology that was widely follows is as described, but not limited to:

(1) Identification,
(2) Collection and/or Acquisition,
(3) Preservation,
(4) Analysis and
(5) Reporting and/or Presenting.

Figure 1.5 below illustrates the five phases of digital forensic methodology stated earlier:

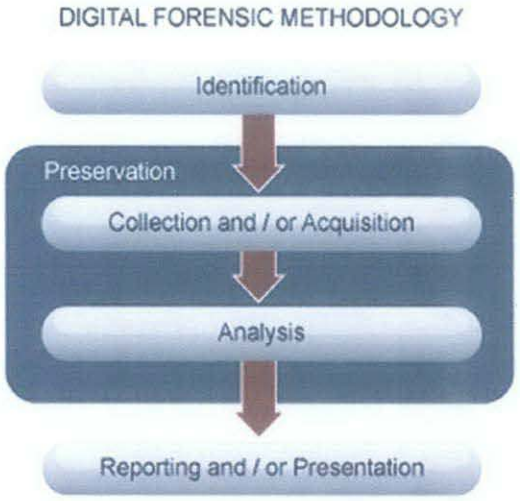


Figure 1.5: Digital Forensic Methodology

Source: Digital Forensics Services, CyberSecurity Malaysia, 2010

Under Identification, investigator must identify evidence that are available at crime scene and determine the best seizing method depending on type of evidence. For Collection and /or Acquisition phase, the investigator needs to collect evidence and bring it to analysis lab without altering it during the process. As for Acquisition, evidence will be imaged (copied bit by bit) into another working copy and analyzed in the lab. For Preservation phase, investigator will have to know how to preserve the evidence from being altered such as kept it in anti-static bag, bubble wrapper, etc. As for analysis, the working copies (evidence's image) will be analyzed by forensic analyst in the lab to extract, simulate and/or interpret findings. Finally, Reporting and/or Presentation will be mainly about the documentation of how the case being analyzed and/or solved and present it in the court of law.

In this paper, the term 'portable media player', 'PMP' and 'player' refer to both of MP3 player and MP4 player, unless it is specified beforehand. As result of this project, an application will be developed and will be used in the Analysis phase of the digital forensic methodology. The following section (Section 1.2) will elaborate further on the problem statement of this project.

1.2 PROBLEM STATEMENT

On 17th May 2010, Digital Forensics Department of CyberSecurity Malaysia received evidence from Royal Police of Malaysia. The digital evidence was a portable media player, Creative Zen Mosaic. The objective of the case was to extract all audio files from the device.

The device was connected to the forensic workstation for acquisition purpose using EnCase, but failed. EnCase is a commercial forensic software used in CyberSecurity Malaysia to help the organization in investigating cases. EnCase offers forensically sound acquisitions, analysis, data searching, internet and e-mail investigation, etc. To ensure that the workstation is in good working condition, another PMP with similar brand was tested using the same workstation, but the result was still negative. The player is using Media Transfer Protocol (MTP) as its transferring protocol, but forensic software was not able to access player with MTP mode. Thus, a conversion from MTP mode to Mass Storage Class (MSC) mode is needed.

There are several researches found on iPod technology forensic, but few or almost none literature review were found on other brands of PMPs. The next section outlines the objectives of this study and the expected outcome.

1.3 OBJECTIVE

The main objective of this project is to develop an application that can convert MTP player to MSC player so that forensic software can perform an acquisition on it without tempering any data or metadata from the devices. Application also shall be able to list drivers associated with the devices.

1.4 SCOPE OF STUDY

To cope with time provided, this project focuses on certain type of PMP to be tested. Type of PMP used to be tested is the flash-based player as this type of player uses

proprietary protocol, including MTP. Plus, the player must be a convertible player from MTP player to MSC player.

In addition to this flash-based type of player, it must be connected to computer via USB 2.0 port. Apart from that, application that developed at the end of this project is intended to be used with Microsoft Windows XP (pre-installed with Windows Media Player 10 or later version), Windows Vista and Windows 7 as these operating systems support MTP (Microsoft Corp., 2009).

This project is relevant to help and assist forensic analyst and crime investigator to perform conversation of MTP player to MSC player with time advantage. With this advantage, it will get them faster to acquisition phase to complete their tasks and makes tasks execution more efficient.

Apparently, the initial objective was to successfully convert all MTP players to MSC mode, but under certain circumstances the nature of the player does not allow the action to take place. In the end, to make this project's objective achievable, the study only focuses on the convertible type of MTP-MSC player.

CHAPTER 2
LITERATURE REVIEW

2.1 BACKGROUND: PORTABLE MEDIA PLAYER

Technology of PMP is rapidly changing to cope with today's modern world and the usage of PMP in daily lives is on rise. With its high capability and mass usage, it is not a surprise that it is listed among those items that needs to be seized (i.e. netbook, digital camera, USB drives) as it can contains valuable data for the law enforcement community apart from storing digital audio files. They should treat PMPs as similar and as important as they treat a seized hard drive.

Profound knowledge on PMP is a necessity to acquire enough amounts of important data on PMP. Knowledge on PMP especially its file structures are vital as one mistake could affect its integrity. For one to understand to gain the knowledge, there are little or almost none literature review on PMP forensic, but there are researches and studies on iPod forensics which are already available and well-known. Apparently, iPod forensic and PMP forensic are different, in a sense that certain PMPs transfer data through MTP. According to Marsico & Rogers (2005), "iPod uses the Apple HFS+ file system when the device is run with an Apple system and uses the FAT32 file system when used with a Windows PC". Thus, research conducted on acquiring data from iPod could not be used and applied on PMP which uses MTP as its transferring protocol.

2.2 PROTOCOLS IN PMP

PMP are divided into two types of player; MTP player and MSC player. MSC player functions as a mass storage device, and detected on computer as an external drive (e.g. "E:\"), similar to USB drive or portable hard drive (Morton, 2007). Additionally, MSC was also defined as a set of computing communications protocols

that run on the USB (Universal Serial Bus), (Creative Worldwide Support, 2010). As for MTP, this protocol is used to transfer media files and associated metadata to/from devices, with optional additional support for reading but restricted content (SanDisk, 2009), which means that host or computer cannot access and control the whole storage. MTP is a protocol that was design to replace MSC and has the ability to control media player from transporting/releasing protected digital content which protect the distribution of purchased or licensed digital audio and video. But when this MTP is enabled, forensic analysis is impossible to perform as it completely securing the content of particular media player.

2.3 FORENSICS ANALYSIS ON PMPS

Both of these types require different ways of performing forensics analysis on them. As for MSC player, the acquiring/imaging process is quite similar to acquiring/imaging process of the solid-state flash device as it allows computer to access and control its bulk mass storage. Thus, forensic tools, such as EnCase could easily detect it as storage device and do acquisition on it. Figure below illustrate how MSC player appears in My Computer as Removable Storage.

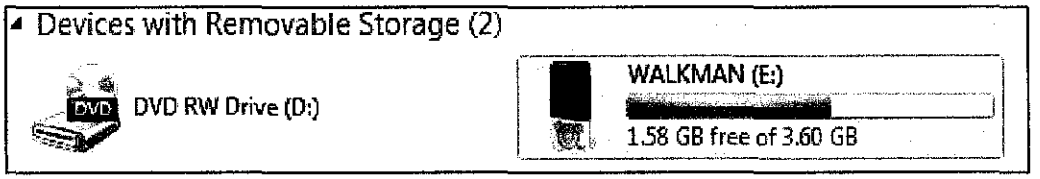


Figure 2.1: Workstation recognized MSC player as Removable Storage

But for MTP player, the protocol itself, makes sure that distribution of digital audio and video content are secure and protected (Kolokowsky & Davis, 2005). Hence, the device itself was recognized as 'Portable Device' in Windows PC and was not assigned to any letter. This is because MTP prevents any direct access to its device. Thus, forensic software fails to acquire MTP player. MTP needs to be disabled for MSC to be enabled in order to make workstation detect PMP as a disk drive and assigned a drive letter to it (i.e. E:\, F:\, G:\, etc) to make forensic analysis possible. Figure on the next page shows how MTP player appears in My Computer as the Portable Device.

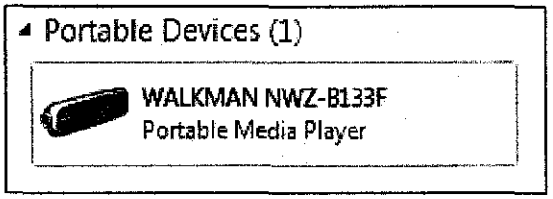


Figure 2.2: Workstation recognized MTP player as Portable Devices

2.4 FURTHER ENHANCEMENT

In review, to adapt with this technology, advance research had to be done as certain types of PMP uses proprietary file system to store and manage data. Hence, the problems that are exist in PMP forensic are the issue of MTP and how to make forensic software to be able to read data from MTP player or for Windows PC to recognized it as storage device and assign drive letter to the player.

CHAPTER 3
METHODOLOGY

3.1 DEVELOPMENT LIFE CYCLE: AGILE

Methodology that adopted in this project is the agile methodology. The reason for choosing agile methodology is based on the ability of agile methodology to adapt with new added requirement and revised design. This project will be conducted in five phases, (1) Planning, (2) Analysis, (3) Design and Development, (4) Testing and Further Enhancement, and (5) Deliver Application. Figure 3.1 below shows the graphical presentation of the steps taken:

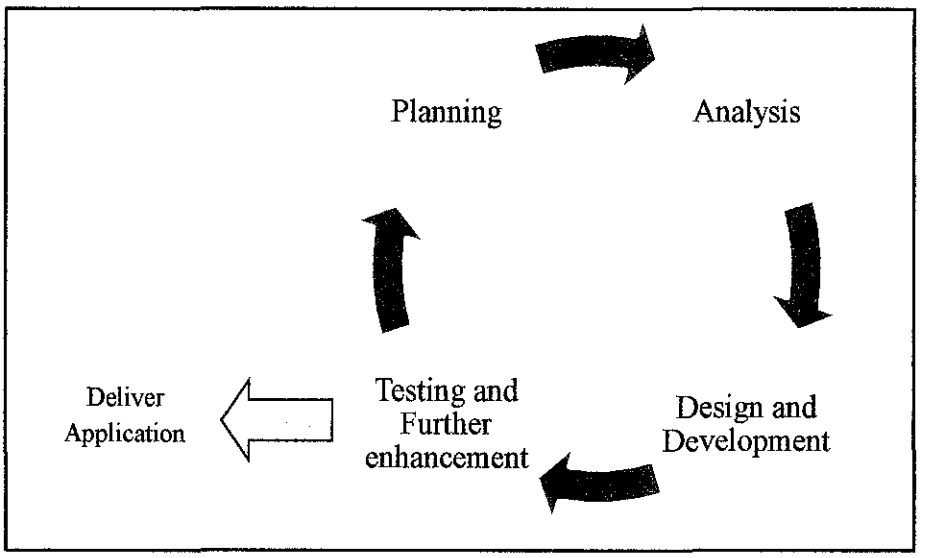


Figure 3.1: Adapted Agile Methodology to suits this project.

3.1.1 PHASE 1: PLANNING

This phase mainly is about the understanding of current situation and problem from related works. Even though PMP forensic is not highly available, but almost similar media player forensic is available, the iPod forensic. Apart from that PMP file structure and protocols are also being studied. Fundamental knowledge on MTP is essential as it was the reason why forensic tool fails to acquire from the device. In

this stage, work plan (Gantt-chart) has been set up to assist and guide project from drifting in timeline. Scope was also determined during this stage.

3.1.2 PHASE 2: ANALYSIS

For analysis stage, requirements of the application are determined and defined. Requirement gathering technique that was chosen for this project is interview. Interview was conducted with Pn. Sarah Taylor; the Industrial Advisory from CyberSecurity Malaysia through instant messaging. During this stage, activity diagram was developed to guide this project. Development tools and hardware for study and development are also being determined during this phase. Further explanation on tools and hardware are discussed in **Section 3.2**.

3.1.3 PHASE 3: DESIGN AND DEVELOPMENT OF APPLICATION

Under this phase, MTP player was successfully converted to MSC player but it is done manually and consists of many steps before conversion was successful. After conversion, player is tested using forensic software to ensure that it is accessible for further forensic analysis.

In this phase, application is designed and developed according to requirement gathered. Application interface was determined throughout this phase. User-friendly and easy to use interface will be implemented as users for this application might vary from forensic analyst (expert) to police officer (novice). This phase also involved development and coding for this application. Further details are discussed in **Chapter 4.**

3.1.4 PHASE 4: TESTING AND FURTHER ENHANCEMENT

After the application is build, it needs to be tested by user with various types of PMPs to make sure that the application was build as per user requirement. The user is the end-user/target audience who will be using the application. Iteration of phase 3 and 4 will be conducted if there is a need to do so, in term of changing the

requirement(s) or application being upgraded before the final product to be released. Further details of this phase can be found on **Chapter 4.**

3.1.5 PHASE 5: DELIVER APPLICATION

After met all requirements and being upgraded up to user's expectation, plus after passing the testing phase, application are delivered and ready to use. The outcome of phase 5 would be the final dissertation.

3.2 SOFTWARE/TOOLS

There are two categories of tools that were determined during the analysis phase, (1) development tools for developing the application, and (2) forensic software to test and determine the succession of PMP's mode changes, i.e. whether or not the forensic software able to access the PMP.

Development tools used are:

(1) **DevCon**, Version 5.2, is a command-line utility that act as an alternative to Windows Device Manager (Microsoft Support, 2010). DevCon is used to detect any PMPs attached to the workstation, determine its driver and change the PMP mode.

(2)  **AutoIt**, Version 3, is a BASIC-like scripting language designed for automating the Windows GUI (Bennet J., 2010). AutoIt is used to implement the USB write-protect module, which created to prevent any data and/or metadata changes towards connected PMPs. AutoIt also used to give graphical representation of DevCon command line for action stated previously.

Forensic freeware used to determine MTP-MSC mode change succession are:

(1)  WinHex, Version 15.6

(2)  Disk Digger, Version 1.0.3

(3)  Recuva, Version 1.39

3.3 HARDWARE

Hardware used to assist this study is an Acer Aspire 4738G workstation with mentioned details:

(1) Windows 7 Home Premium operating system,

(2) Intel(R) Core(TM) i5 CPU, 2.53 GHz processor, and

(3) 4.00 GB RAM.

Apart from that, PMPs selected to assist during this project is MTP-MSC convertible PMP, Sony Walkman NWZ-E443 (4GB) and PMP, Sony Walkman NWZ-B133F (1GB).

CHAPTER 4
RESULTS AND DISCUSSION

4.1 PLANNING PHASE

As results for phase 1, a Gantt-chart is created to guide this project throughout these two semesters (see Appendix 4-1). For the first semester, it covers up planning, analysis and design phases. Preliminary research work starts right after projects topics were accepted and released. Later on, preliminary report was submitted to supervisor. After that, progress report was submitted to supervisor with completion work still in the early design phase. At the end of the semester, a seminar on progress reporting was held and interim report was submitted.

For the second semester, design and development phase will be continues alongside with evaluation and testing. Progress report is sent out for evaluation by supervisor. Later on, poster exhibition and oral presentation (viva) were held. Finally, final dissertation and technical report were submitted at the end of semester.

4.2 ACTIVITY DIAGRAM

For phase 2, an activity diagram was created to guide this application's development. This diagram combines activities from users and functions from the application. First, user need to launch the application. Then, turn on the write-protect mode and plug in PMP(s). Next, the application will detect any PMPs attached and return its current driver status. If it is MTP mode and convertible to MSC mode, it will perform the conversion. If the current driver is in MTP mode but not supported for MSC mode, the application will notify user that the PMP is not convertible to MSC mode. Application will notify user once conversion is done and user can continue

with further forensic analysis. Figure 4.1 below shows the activity diagram for this application.

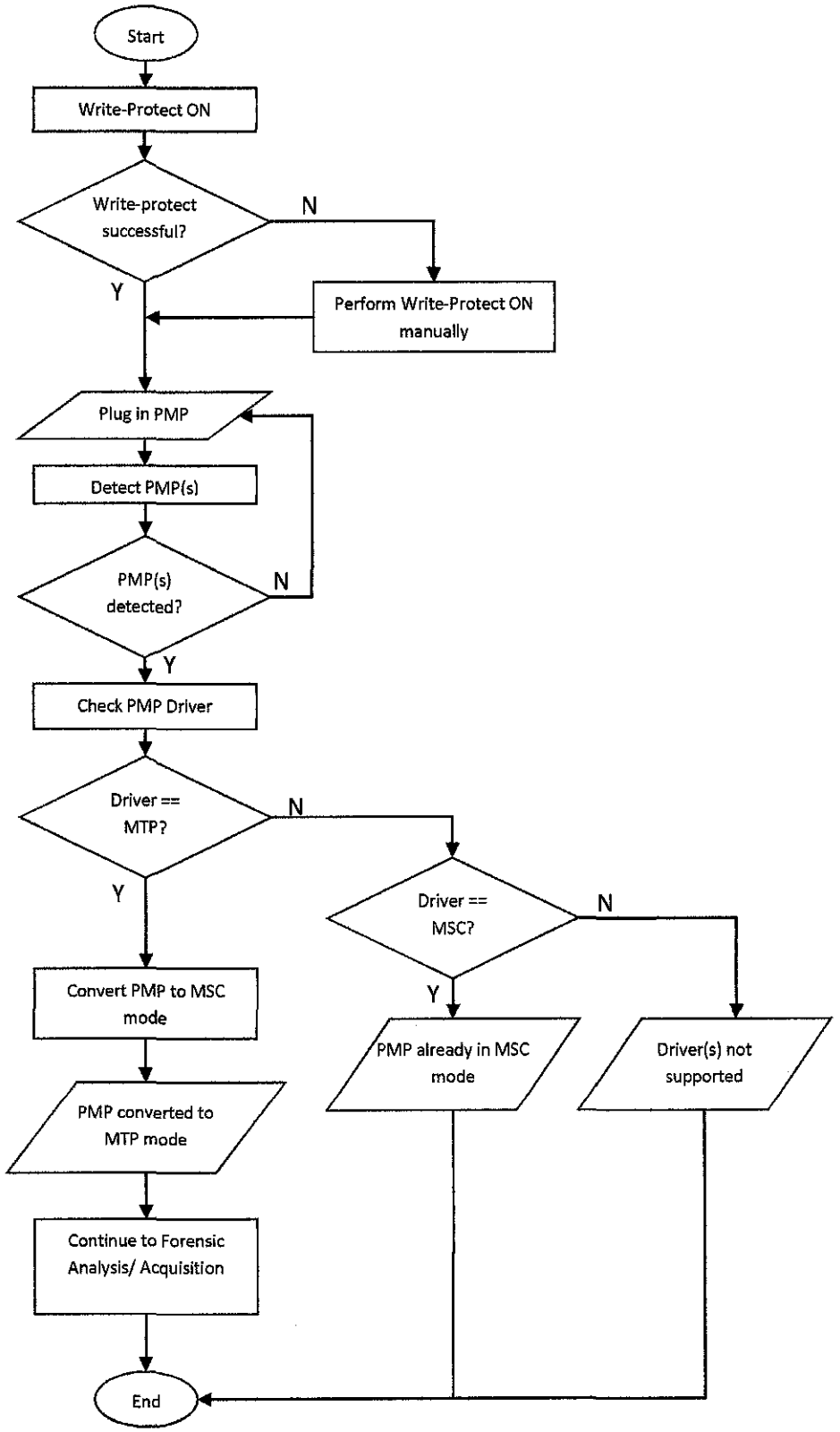


Figure 4.1: Activity diagram

4.3 UPDATING PROCESS

In phase 3, MTP player (Sony Walkman NWZ-E443) was successfully updated into MSC mode player and it was assigned a drive letter by Windows XP SP3, but it was done manually through Windows Device Manager. Conversion process can only be done with convertible MTP-MSC player. Below are simplified steps taken to update MTP player to MSC mode (see Appendix4-2 for details):

(1) Attach PMP to workstation.
(2) Open 'Device Manager', and search for PMP.
(3) Click 'Update Driver'.
(4) Choose '*USB Mass Storage Device*' and click 'Next'.
(5) PMP now is also detected under *Disk drives* in Device Manager.
(6) At My Computer PMP is now detected as removable disk.

After this conversion, MTP player now are updated to MSC player and is detected as 'Removable Disk'. This means that forensic software is able to perform forensic acquisition onto it.

4.4 SYSTEM ARCHITECTURE

In analysis phase also system architecture being recognized and determine. Figure 4.2 below is the graphical presentation of the system architecture:

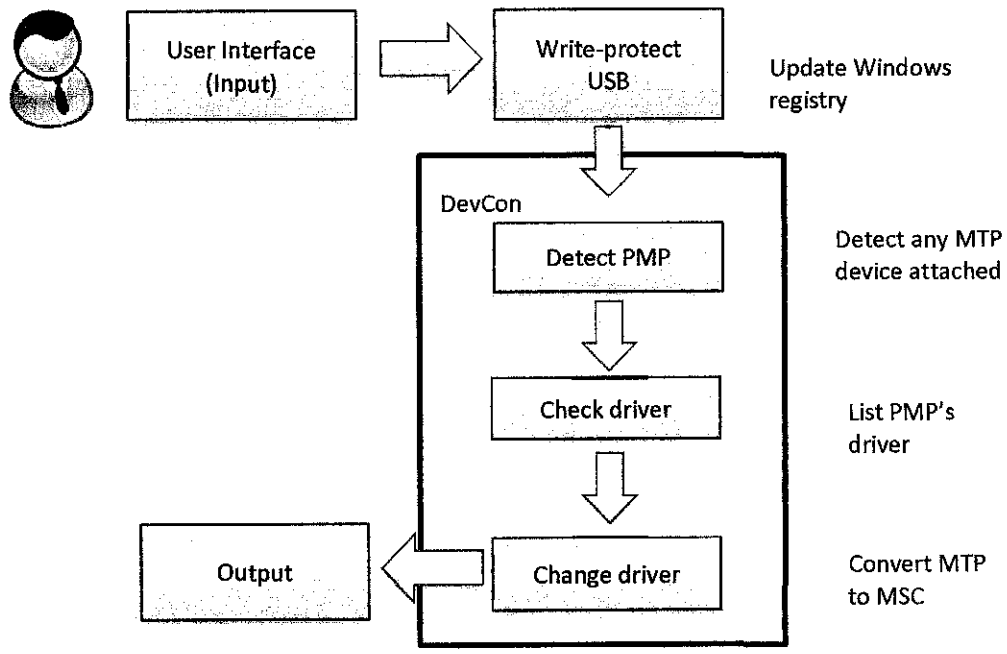


Figure 4.2: System architecture

Based on Figure 4.2, the application basically interacts with the user through easy and understandable graphical user interface (GUI). Sequential instructions were given as guide for users to use the application. Windows registry will be updated to enable USB write-protect so that the evidence remain secure and valid throughout the mode updating process. DevCon was used as a third-party command-line utility to perform device detection, device driver listing, and device driver updating. After driver updating was successful, user will be notified through visual notification. Details of the architecture will be break down in more details and discussed in **Section 4.5** below.

4.5 FUNCTIONAL DECOMPOSITION DIAGRAM

Apart from that, functional decomposition diagram was also created. Functional decomposition diagram as shown in Figure 4.3 was developed from combination of module or functions derived from activity diagram earlier. There are four main modules used in developing this application, they are:

(1) USB Write-Protect ON (Read-Only) Module,
(2) PMP Detection Module,
(3) PMP Driver-Check Module, and
(4) Driver-Update Module.

Under USB Write-Protect ON Module, USB port will be turn to read-only mode, and any access to PMP will not change it metadata. This is intended to prevent any overwrite of data towards the evidence itself and maintain its validity. After that, user will need to attach PMP to the workstation. Then PMP Detection Module will start to detect how many PMPs are being attached and PMP Driver-Check Module will determined drivers used by each PMP. Once drivers for a PMP were identified and listed, user might need to click on 'Update' button to trigger Driver-Update Module. This module then will update/change the mode of the PMP. Then the application will notify user once conversion of MTP player to MSC player is successful.

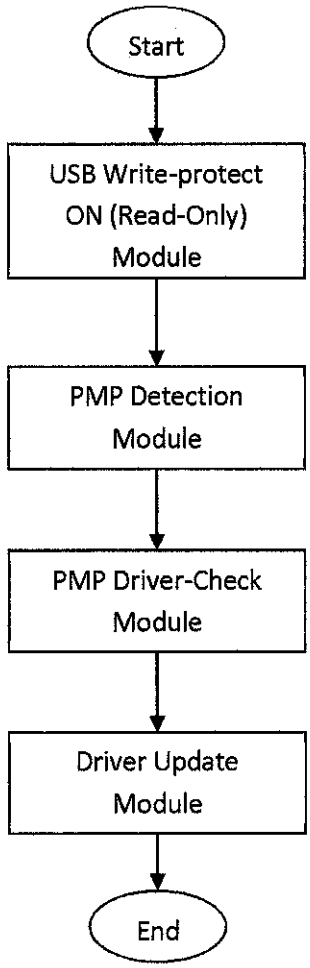


Figure 4.3: Functional decomposition diagram

4.6 GRAPHICAL USER INTERFACE

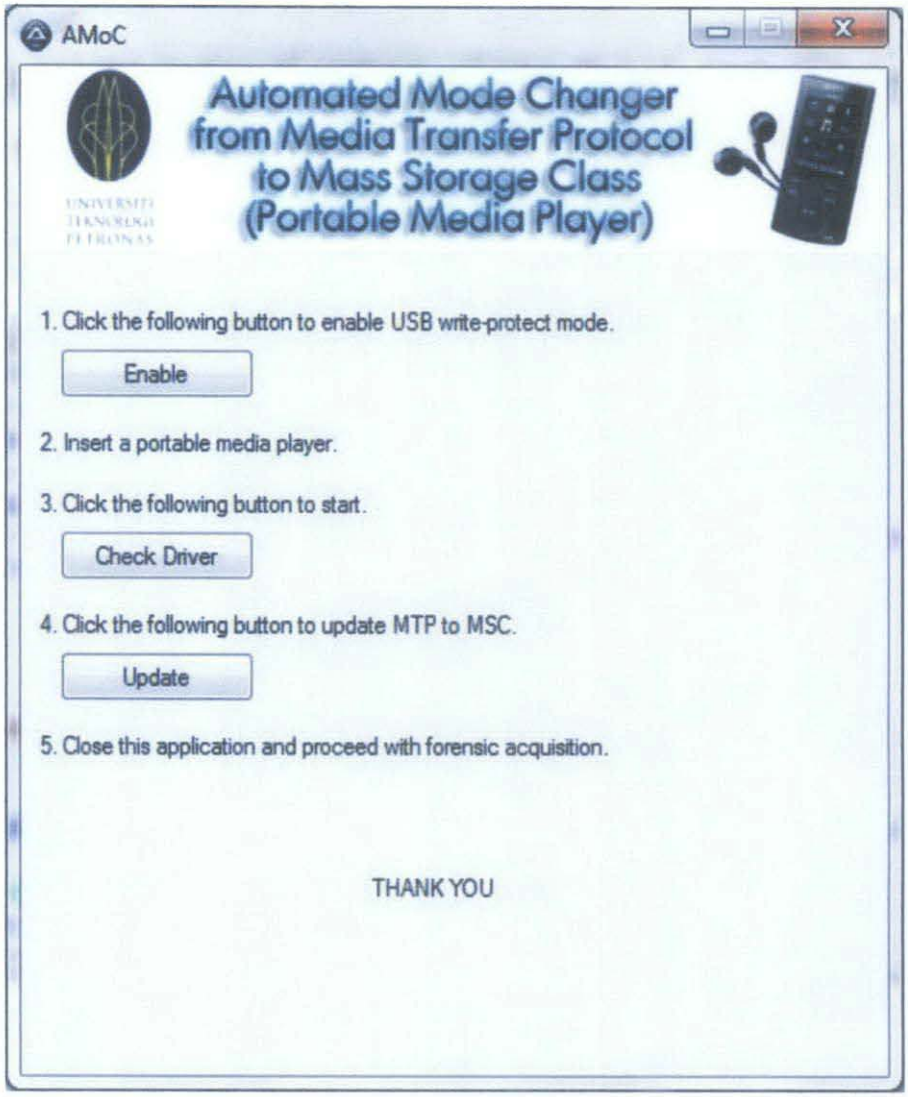


Figure 4.4: Main GUI

Figure 4.4 above illustrate the main GUI that will interact with the user throughout the process. 'AMoC' was abbreviation for 'Automated Mode-Changer' given to this application as title of its dialog box instead of its original long title. However, to avoid any confusion, the original title was placed at the top center of this application for user awareness. There are three buttons that represent USB Write-protect Module, PMP Driver-Check Module and Driver Update Module from the functional decomposition diagram stated earlier. Details of each module will be explained further in the next section.

Figure 4.5 below shows a code snippet of the main GUI using AutoIt:

```
Func _Main()

    GUICreate("AMoC", 445, 500)
    GUISetState()
    GuiCtrlCreatePic("head2.jpg",0,0,0,0)
    GuiCtrlCreateLabel("1. Click the following button to enable USB write-protect mode.", 10, 120)
    Opt("GUICoordMode", 1)
    $mode1 = GUICtrlCreateButton("Enable", 20, 140, 100)
    GuiCtrlCreateLabel("2. Insert a portable media player. ", 10, 180)
    GuiCtrlCreateLabel("3. Click the following button to start.", 10, 210)
    $mode2 = GUICtrlCreateButton("Check Driver", 20, 230, 100)
    GuiCtrlCreateLabel("4. Click the following button to update MTP to MSC.", 10, 270)
    $mode3 = GUICtrlCreateButton("Update", 20, 290, 100)
    GuiCtrlCreateLabel("5. Close this application and proceed with forensic acquisition.", 10, 330)
    GuiCtrlCreateLabel("THANK YOU", 180, 400)
```

Figure 4.5: Code snippet for main GUI

4.7 USB WRITE-PROTECT MODULE

Below is code snippet for USB write-protect module:

```
While 1
        $msg = GUIGetMsg()
        Select
            Case $msg = $GUI_EVENT_CLOSE
                ExitLoop
            Case $msg = $mode1
                local $var = RegRead("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies",
"WriteProtect")
                ;MsgBox(0, "Status", "Write Protect is : " & $var)
                If $var = 0 Then
                    MsgBox(0, "Status", "Write Protect is : OFF")
                    RegWrite ("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies",
"WriteProtect", "REG_DWORD", "0x00000001") ;writeprotect ON
                    $var = RegRead("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies",
"WriteProtect")
                    MsgBox(0, "Status", "NOW Write Protect is : ON")
                ElseIf $var = 1 Then
                    MsgBox(0, "Status", "Write Protect is already turned ON")
                        ;RegWrite ("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies",
"WriteProtect", "REG_DWORD", "0x00000000") ;writeprotect OFF
                    ;MsgBox(0, "Status", "NOW Write Protect is : " & $var)
                EndIf
```

Figure 4.6: Code snippet for USB write-protect module

This module is triggered when the button 'Enable' was clicked from the main GUI (refer to Figure 4.4). This module will update the workstation's registry. First, it will check the workstation current status for USB write-protection at Windows registry, HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies. If the value is true (0x00000001), it means that the USB write-protect is already turn ON. Then it will prompt user to continue and connect PMP to the workstation. However, if the return value is false (0x00000000), it means that the USB write-protect of OFF and this module will turn it on and notify the user to continue.

This scenario can be explained by illustrations below:

(1) The module is triggered and checks the registry value at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevice Policies and return the current value as shown (in this case it is false (0), USB wirte-protect is OFF).

Figure 4.7: Current status of USB Write-Protect

(2) After modifying the registry and turn on the write-protect mode, the application will return the current value to user, as shown below:

Figure 4.8: Updated status of USB Write-Protect

(3) This means that user now can safely connect any USB device to the workstation without any data and/or metadata changes to be made on the devices.

(4) Apart from that, if the workstation's write-protect is already enable from the beginning, USB Write-Protect module will be triggered and return as Figure 4.9 illustrate and hence no modification towards Windows registry.

Figure 4.9: USB Write-Protect is already turned ON

4.8 PMP DETECTION MODULE

This module detects any connected PMPs to the workstation by returning device's name and ID. PMPs can be detected using DevCon application. Figure 4.10 below is a screenshot of DevCon with command of `devcon /hwids *usb*`, which will return every USB devices connected to the workstation. Among the devices listed, two of them are PMPs connected earlier.

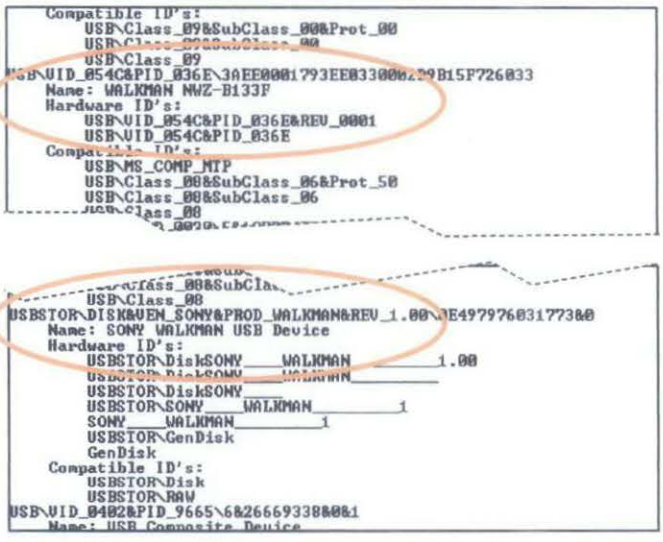


Figure 4.10: Connected PMPs were detected by DevCon

To narrow down USB devices found, command `devcon /hwids *MTP*` is executed. With this command, DevCon only detect devices that contain the word *MTP* in its ID. From above situation, two PMP were detected. Figure shown below is the return of MTP player connected to the workstation.

```
C:\>devcon /hwids *MTP*
USB\VID_054C&PID_036E\3AEE0001793EE0330002D9B15F726033
    Name: WALKMAN NWZ-B133F
    Hardware ID's:
        USB\VID_054C&PID_036E&REV_0001
        USB\VID_054C&PID_036E
    Compatible ID's:
        USB\MS_COMP_MTP
        USB\Class_08&SubClass_06&Prot_50
        USB\Class_08&SubClass_06
        USB\Class_08
USB\VID_054C&PID_03FD\0E497976031773
    Name: USB Mass Storage Device
    Hardware ID's:
        USB\VID_054C&PID_03FD&REV_0001
        USB\VID_054C&PID_03FD
    Compatible ID's:
        USB\MS_COMP_MTP
        USB\Class_08&SubClass_06&Prot_50
        USB\Class_08&SubClass_06
        USB\Class_08
2 matching device(s) found.
```

Figure 4.11: MTP devices found connected to the workstation

This module shall not be viewable by the user, as this module are not important for the user to know since by default, any attached device to Windows workstation will be notified by Windows OS itself.

4.9 PMP DRIVER-CHECK MODULE

This module will be executed once the button 'Check Driver' was pressed on the main GUI (refer to Figure 4.4). This module will check and list any associated driver to attached PMPs. Figure below shows associated driver to the attached PMP:

```
C:\>devcon drivernodes *mtp*
USB\VID_054C&PID_03FD\0E497976031773
    Name: USB Mass Storage Device
DriverNode #0:
    Inf file is C:\Windows\INF\wpdmtp.inf
    Inf section is MTP
    Driver description is MTP USB Device
    Manufacturer name is (Standard MTP Device)
    Provider name is Microsoft
    Driver date is 6/21/2006
    Driver version is 6.1.7600.16385
    Driver node rank is 16719872
    Driver node flags are 00102040
        Inf is digitally signed
DriverNode #1:
    Inf file is C:\Windows\INF\usbstor.inf
    Inf section is USBSTOR_BULK
    Driver description is USB Mass Storage Device
    Manufacturer name is Compatible USB storage device
    Provider name is Microsoft
    Driver date is 6/21/2006
    Driver version is 6.1.7600.16778
    Driver node rank is 16719873
    Driver node flags are 00142044
        Inf is digitally signed
1 matching device(s) found.
```

Figure 4.12: Driver identified for MTP player

From Figure 4.12, we can see that the device supported both MTP and MSC driver, hence updating back-and-forth between these two drivers are possible. By executing the following command, user can determine current driver used for the PMP as shown:

```
C:\>devcon stack *mtp*
USB\VID_054C&PID_03FD\0E497976031773
    Name: WALKMAN
    Setup Class: {eec5ad98-8080-425f-922a-dabf3de3f69a} WPD
    Controlling service:
        WUDFRd
    Lower filters:
        WinUsb
1 matching device(s) found.
```

Figure 4.13: Current driver status

As per see, the setup class is WPD (Windows Portable Device) which means that the controlling driver is MTP. Hence, PMP attached was in MTP mode.

4.10 PMP DRIVER-UPDATE MODULE

This module will be executed once the 'Update' button was pressed on the main GUI (refer to Figure 4.4). This module updates MTP to MSC and assigned drive letter to the PMP. Update command can be found as follow:

```
C:\>devcon updetni C:\Windows\inf\usbstor.inf *mtp
```

Figure 4.14: Command for updating driver

After executing the command, result as below could be found:

```
C:\>devcon stack *mtp*
USB\VID_054C&PID_03FD\0E497976031773
    Name: USB Mass Storage Device
    Setup Class: {36fc9e60-c465-11cf-8056-444553540000} USB
    Controlling service:
        USBSTOR
1 matching device(s) found.
```

Figure 4.15: Updated MTP player

This indicates that MTP player was successfully updated into MSC player with the proof of USBSTOR as its controlling service, which is the driver for USB Mass-Storage and its setup class is USB. Hence, the updating process was successful.

4.11 FINAL OUTPUT

As the final output, users are notified with a dialog box to indicate that the updating of driver or mode from MTP to MSC was success. Figure below shows the notification that is visible to the user:

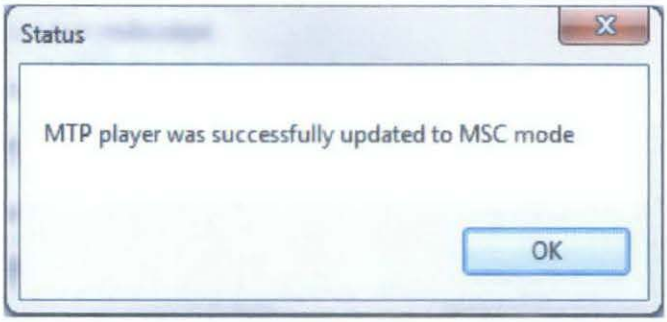


Figure 4.16: Dialog box that visible to user at the end of process

Apart from that, user also will be able to see the difference in My Computer. Previously, MTP player was identified as 'Portable Media Player' as shown:

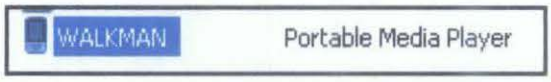


Figure 4.17: Previously, MTP was identified as Portable Media Player

After the updating process, user will be able to find the following replacing the 'Portable Media Player':

Figure 4.18: Now, MTP player was recognized as Removable Disk

4.12 TESTING PHASE

For Phase 5 (testing phase), three testing was conducted namely, unit testing, integration testing and system testing. With agile methodology as the project's methodology, continuous enhancement and deployment is possible. Hence, testing phase is important to make sure that the project achieves its objectives.

In unit testing, each module was tested individually by providing the input and expected output. While in integration testing, two or more modules were combined

to make sure that the modules were able to work together. Integration between the module and DevCon also was tested to ensure that it is working. As for system testing, the system was tested as a whole by covered all possible paths within the application as per stated in activity diagram (refer to Figure 4.1), i.e. tested while computer was on USB write-protect mode, and tested while computer was not on USB write-protect mode, etc.

Apart from that, several PMPs were tested to make sure that the application works and able to update MTP mode to MSC mode. Table 4.1 below shows a summary of testing conducted:

Table 4.1: Result of application using convertible PMPs

Type of PMP	Sony Walkman NWZ-B133F	Sony Walkman NWZ-E443
Able to write-protect?	Yes	Yes
Able to identified driver(s)?	Yes	Yes
Able to update driver? (MTP-MSC)	Yes	Yes

4.13 TESTING WITH FORENSICS SOFTWARE

Under this phase, updated PMP from MTP player to MSC player was tested using several forensic software stated earlier (refer to Section 3.2). Below are the illustrations for results of detecting the PMP using stated forensic software:

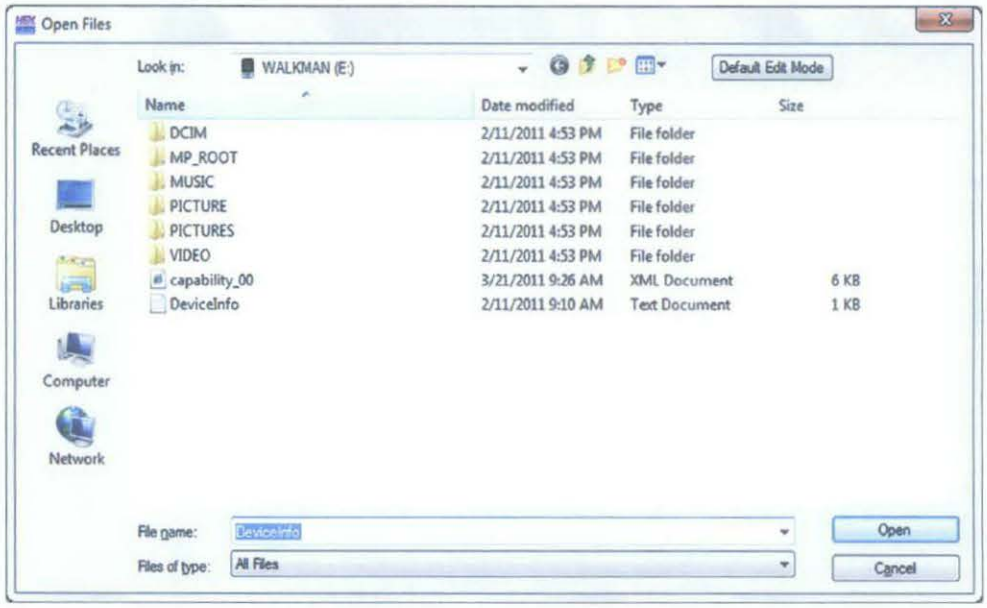


Figure 4.19: PMP was recognized under WinHex

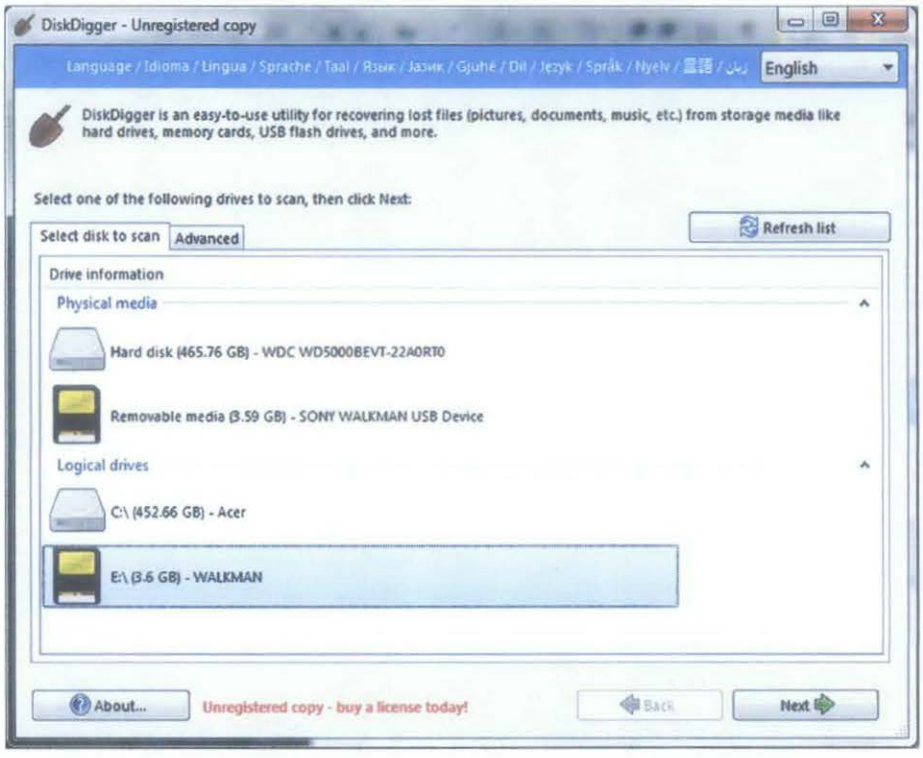


Figure 4.20: PMP was recognized under DiskDigger

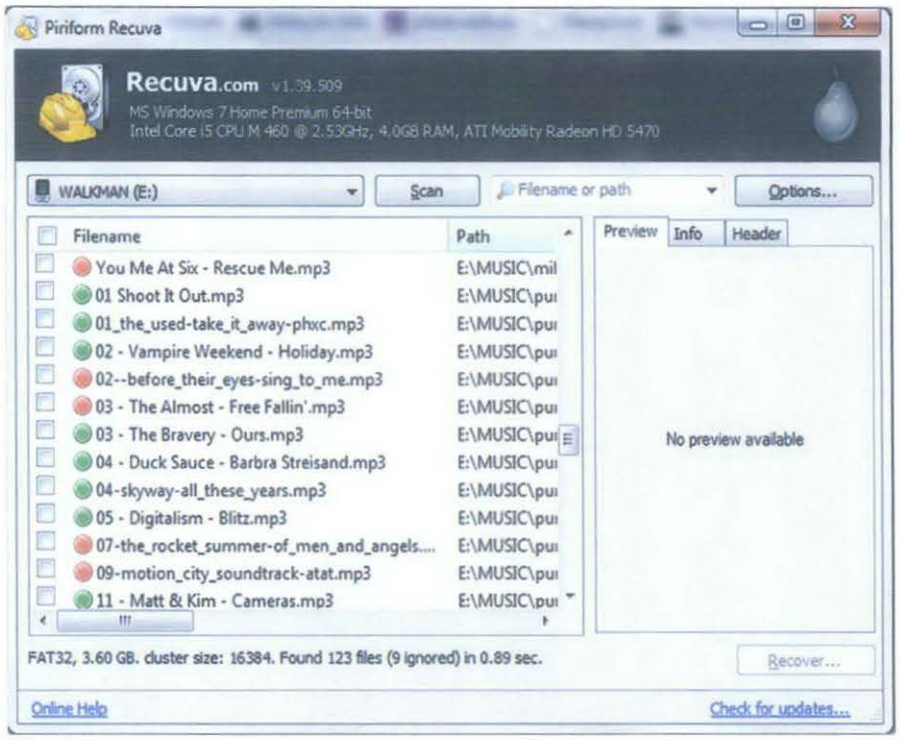


Figure 4.21: PMP was recognized by Recuva

Table 4.2 below shows the summary of PMP recognition using several forensic software after being updated using 'AMoC':

Table 4.2: Result of PMP recognition using several forensic software

Software used	WinHex (Ver15.6)	Disk Digger (Ver1.0.3)	Recuva (Ver 1.39)
Able to detect PMP?	Yes	Yes	Yes
Able to identified deleted file(s)?	Yes	Yes	Yes
Able to recover deleted file(s)?	Yes	Yes	Yes

After undergoing this testing, it is proven that MTP player was successfully converted into MSC mode as these forensic softwares are able to detect the player. Forensic analyst or investigators now are able to perform forensic acquisition on MTP player after being updated into MSC mode.

CHAPTER 5
CONCLUSION

5.1 CONCLUSION

This project highlights on the conversion of MTP player to MSC player which will enable forensic software to perform acquisition onto it as MTP denies any direct access towards its player. This project will contribute to the world of PMP forensic and will ease the work investigator and forensic analyst to perform forensic analysis onto it. At the end of development stage, application was tested against criteria/requirement collected throughout the project and several forensic software was used to proof the updating of MTP player into MSC mode was successful.

5.2 RECOMMENDATIONS

This project was focusing on developing an application that will update MTP mode to MSC mode, with the condition that both drivers are being pre-installed in the PMP. But during this dissertation was written, there are no method or official paper available for non-convertible MTP player to be updated into MSC mode. Hence, none forensic software are able to perform forensic acquisition on non-convertible MTP player. For further enhancement, studies and research shall be made in order to make all PMP are convertible to MSC mode or by forensic software to be able to recognized MTP player.

REFERENCES

Bennet J. 2010 < http://www.autoitscript.com/site/autoit/>

Creative Worldwide Support. 21 May 2010
<http://support.creative.com/kb/ShowArticle.aspx?sid=83635>

CyberSecurity Malaysia. 2010
<http://www.cybersecurity.my/en/services/digital_forensics/services/main/detail/1628/index.html>

Kolokowsky, S., & Davis, T., 2005. "Introduction to MTP: Media Transfer Protocol" in *Analog ZONE.*

Lim, K.-S., & Lee, S., 2008, " A methodology for Forensic analysis of Embedded System," *Second International Conference on Future Generation Communication and Networking* , 285-286.

London Evening Standard. 30 Jan 2007.
<http://www.thisislondon.co.uk/news/article-23383609-sophisticated-thieves-bugging-chip-and-pin-machines-with-mp3-players.do>

Mark M., Harold D., 2009. *Windows Embedded: MTP Responder Development Guide.* Microsoft.

Marsico, C. V., & Rogers, M. K., 2005, "iPod Forensics," *International Journal of Digital Evidence* , 2.

Microsoft Corporation. 29 Aug 2009
<http://blogs.msdn.com/b/wpdblog/archive/2009/08/29/mtp-over-various-transports.aspx>

Microsoft Support. 2 July 2010 < http://support.microsoft.com/kb/311272>

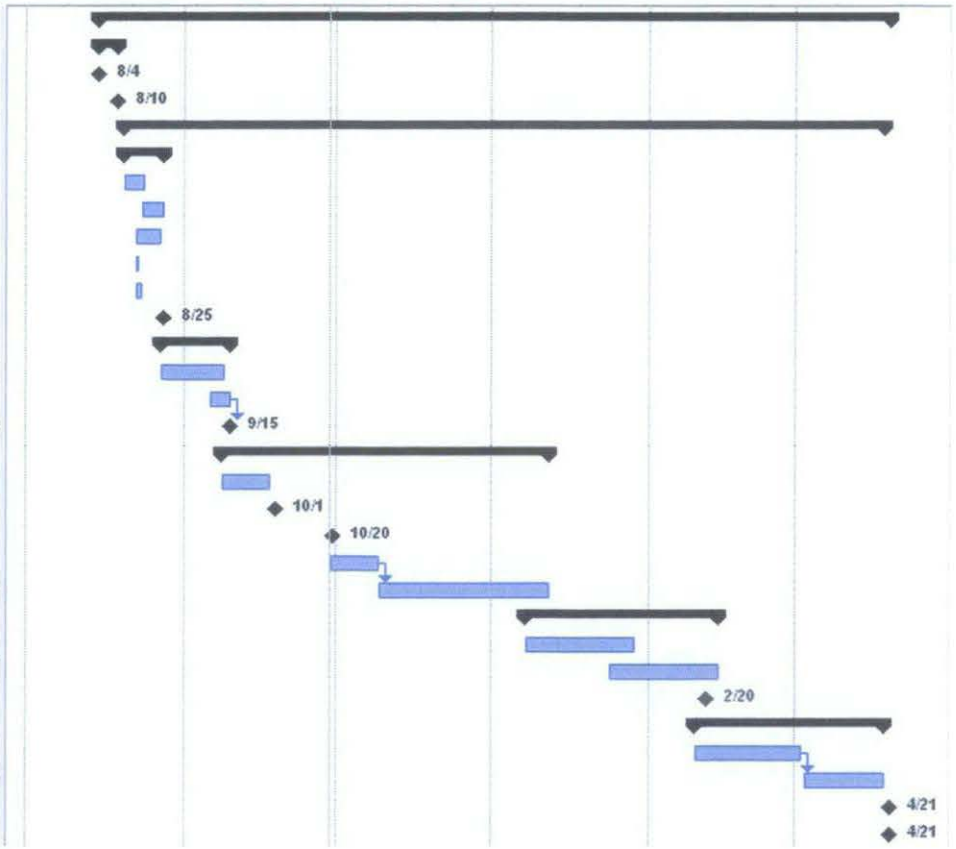
Morton, E. 20 April 2007 <http://www.cnet.com.au/what-is-the-difference-between-mtp-ums-and-msc-mp3-players-339275003.htm>

SanDisk Support. 26 Sept 2008 <http://kb.sandisk.com/app/answers/detail/a_id/162>

APPENDICES

Appendix 4-1: Gantt-chart for project

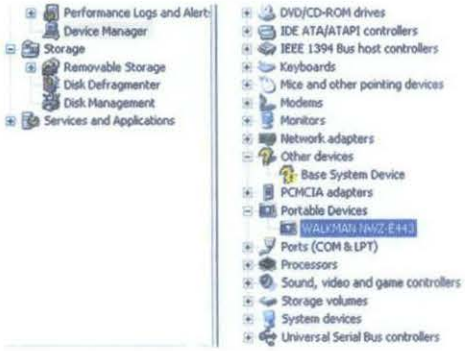
		Task Name	Duration	Start	Finish
1		**- Protocol Converter for Portable Media Player**	**186 days**	**Wed 8/4/10**	**Thu 4/21/11**
2		**- Proposal and Approval**	**4 days**	**Wed 8/4/10**	**Tue 8/10/10**
3		Submit project proposal	0 days	Wed 8/4/10	Wed 8/4/10
4		Gain approval on project's topic	0 days	Tue 8/10/10	Tue 8/10/10
5		**- Research and Development**	**178 days**	**Thu 8/12/10**	**Mon 4/18/11**
6		**- Phase 1: Planning**	**9 days**	**Thu 8/12/10**	**Wed 8/25/10**
7		Understand current situation	5 days	Thu 8/12/10	Wed 8/18/10
8		Study and analyze related work	5 days	Wed 8/18/10	Tue 8/24/10
9		Research on USB protocol	6 days	Mon 8/16/10	Mon 8/23/10
10		Create workplan	1 day	Mon 8/16/10	Mon 8/16/10
11		Define scope	2 days	Mon 8/16/10	Tue 8/17/10
12		Submit Preliminary Report	0 days	Wed 8/25/10	Wed 8/25/10
13		**- Phase 2: Analysis**	**17 days**	**Tue 8/24/10**	**Wed 9/15/10**
14		Gather requirements	15 days	Tue 8/24/10	Mon 9/13/10
15		Create an activity diagram	5 days	Thu 9/9/10	Wed 9/15/10
16		Submit Progress Report	0 days	Wed 9/15/10	Wed 9/15/10
17		**- Phase 3: Design and Development**	**78 days**	**Mon 9/13/10**	**Wed 12/29/10**
18		Convert MTP player to MSC player	12 days	Mon 9/13/10	Tue 9/28/10
19		Presenting Seminar 1 on Progress Report	0 days	Fri 10/1/10	Fri 10/1/10
20		Submit Interim report	0 days	Wed 10/20/10	Wed 10/20/10
21		Develop application interface	12 days	Tue 10/19/10	Wed 11/3/10
22		Develop application	40 days	Thu 11/4/10	Wed 12/29/10
23		**- Phase 4: Testing and Further enhanceme**	**46 days**	**Wed 12/22/10**	**Wed 2/23/11**
24		Evaluate application	26 days	Wed 12/22/10	Wed 1/26/11
25		Conduct testing based on several test ca	26 days	Wed 1/19/11	Wed 2/23/11
26		Submission of Progress Report	0 days	Sun 2/20/11	Sun 2/20/11
27		**- Phase 5: Deliver application**	**44 days**	**Wed 2/16/11**	**Mon 4/18/11**
28		Deliver final application	25 days	Wed 2/16/11	Tue 3/22/11
29		Produce dissertation	18 days	Thu 3/24/11	Mon 4/18/11
30		**- Submission**	**0 days**	**Thu 4/21/11**	**Thu 4/21/11**
31		Submit project dissertation	0 days	Thu 4/21/11	Thu 4/21/11



Appendix 4-2: Steps of conversion from MTP player to MSC player

1. Attach PMP to workstation.
2. My Computer will detect as such:

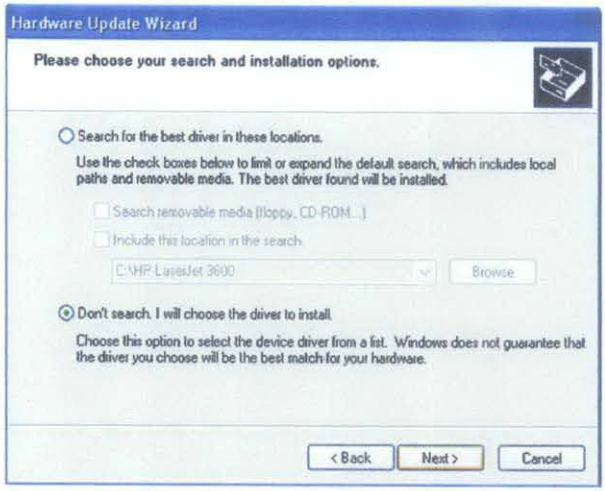
3. Then, right click on My Computer (Desktop icon), Click Manage.
4. Computer Management window will open.
5. Click on Device Manager, and search for PMP.



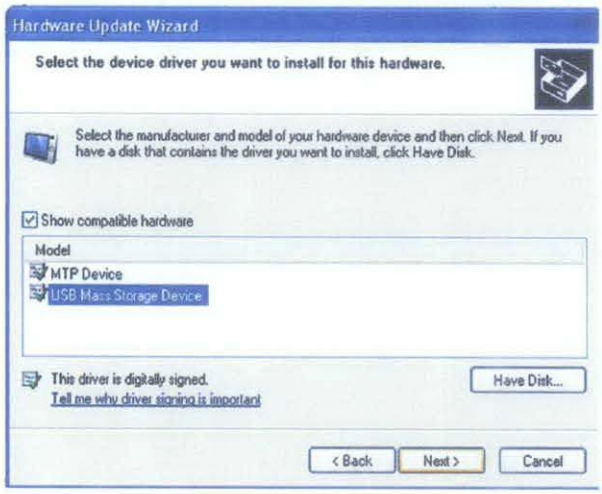
6. Right click on the PMP.
7. Click Update Driver.

8. Choose '*Install from a list or specific location [Advanced]*', and click Next.

9. Choose '*Don't search. I will choose driver to install*', and click Next.

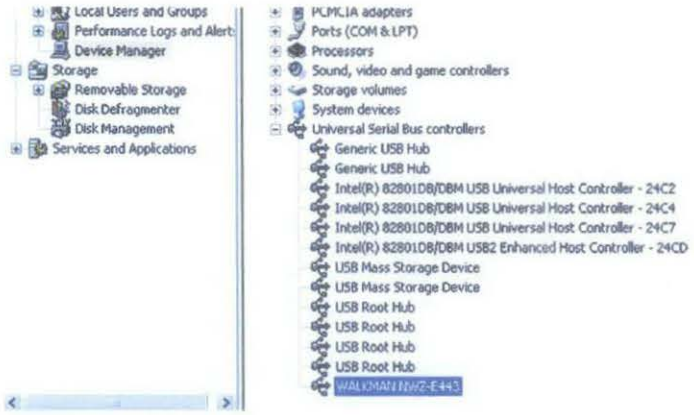


10. Choose '*USB Mass Storage Device*' and click Next.



11. Wait until the installation is done (Wizard will notify once it is done).

12. Click 'Finish' button, and notice the change under *USB controllers*..



13. ..and *Disk drives*.

14. Now, go to My Computer and PMP is detected as removable disk.