The Need for a New Data Processing Interface for Digital Forensic Examination

Inikpi O. ADEMU
School of Architecture,
Computing and Engineering
University of East London
London, United Kingdom

Dr Chris O. IMAFIDON
Formerly, Head of Management of Technology Unit,
Queen Mary University of London,
Currently Senior Academic, School of Architecture,
University of East London,
London, United Kingdom

Abstract— **Digital forensic science provides tools, techniques and scientifically proven methods that can be used to acquire and analyze digital evidence. There is a need for law enforcement agencies, government and private organisations to invest in the advancement and development of digital forensic technologies. Such an investment could potentially allow new forensic techniques to be developed more frequently. This research identifies techniques that can facilitates the process of digital forensic investigation, therefore allowing digital investigators to utilize less time and fewer resources. In this paper, we identify the Visual Basic Integrated Development Environment as an environment that provides set of rich features which are likely to be required for developing tools that can assist digital investigators during digital forensic investigation. Establishing a user friendly interface and identifying structures and consistent processes for digital forensic investigation has been a major component of this research.**

Keywords-autonomous coding; intellisense; visual sudio; integrated development environment; relational reconstruction; data processing.

I. Introduction

Digital forensics plays an important part in the investigation of crimes involving digital devices. Digital forensic techniques are used primarily by private organisations and law enforcement agencies to capture, preserve and analyze evidence on digital devices. Digital evidence collected at a crime scene has to be analyzed and connections between the recovered information need to be made and proven. The search for digital evidence is thus a tedious task that consumes time. An extremely large amount of evidence needs to be processed in a very limited time frame which leads to delay in processing schedules. Digital forensic science provides tools, techniques and scientifically proven methods that can be used to acquire and analyze digital evidence (Ademu et al, 2012). Digital forensic investigators interact with digital evidence and digital forensic tools. The digital evidence can be used to backtrack or reconstruct illegal event.

Digital forensic investigators are constantly trying to find better and more efficient ways of uncovering evidence from digital sources. The problem here is that the research process itself is usually time intensive and consumes a lot of resources. Considering tools in forensic investigation also consumes time. The application of forensic technique is an extremely complex task, requiring an in depth understanding of the chosen digital devices. The development of a forensic application would typically require a researcher to develop hugely complex code that would perform tasks similar to those of the operating system or application in question in an attempt to discover stored data.

The law enforcement and corporate security professionals require tools for effective digital evidence acquisition. These tools already exist to capture, preserve and analyze data from hard drives, memory and network streams. These tools are available through open source licenses with their own unique user interface and feature and run on a variety of operating systems. This presents a challenge to digital forensic investigator since they must become acquainted with the operational characteristics and user interface of each tool they want to use. Also most of these tools are not online and are complicated to use, so it requires each investigative agency to set up their own suite of forensic tools.

The goal of this research is to provide an approach that supports digital forensic investigaors by identifying activities that facilitates and improves digital forensic investigation process. This research identifies the Visual Basic Integrated Development Environment (VBIDE) as a set of rich features that are likely to be required for developing tools that can assist digital investigators during digital forensic investigation.

II. Related Work

Digital evidence is defined by (Carrier and Spafford, 2006) as a digital data that supports or refutes a hypothesis about digital events or the state of digital data. This definition includes evidence that may not be capable of being entered into a court of law, but may have investigative value, this definition is in agreement to (Nikkel, 2006) definition that states, digital evidence as a data that support theory about digital events. Evidence can be gathered from theft of or destruction of intellectual property, fraud or anything else criminally related to the use of a digital device. Evidence, which is also referred to as digital evidence is any data that can provide a significant link between the cause of the crime and the victim (Perumal, 2009). Digital forensics is the science of digital crime investigation. The main purpose of digital investigation is to collect digital evidences, which could be unaltered (Palmer, 2001). The use of computer system and other electronic devices has been widely used in the last two decades. The large amount of information is produced, accumulated, and distributed via electronic means. The majority of organizations interact with electronic devices every day. For this purpose, there is a need for finding digital evidences in computer systems and other electronic devices. However, when looking for digital evidences, there are some problems faced by an investigator. There is usually a large amount of files stored in computer system devices, and only few of them may comprise the valid evidences, but if the investigators don't know the location, it could consume a lot of time. According to (Jones et al 2006) the information is not only stored in working devices, there is need of recovering data from a broken device. Another important issue is the need for digital evidence being unaltered. If it cannot be proven that evidence has not been altered, it cannot be used as a valid digital evidence for persecuting a crime. A particular case is different from another. Techniques that should be used and actions that have to be taken as well as a type of digital evidence needed are mutable factors. And also the computer environment such as the operating system, type of storage devices used and the authentication method is another issue.

The investigative process is structured to encourage a complete, accurate investigation, ensure proper evidence handling and reduce the chance of mistakes created by preconceived theories and other potential pitfalls (Ademu et al, 2011). This process applies to criminal investigations as well as public and private inquiries dealing with policy violations or system intrusion. Investigators and Examiners work hand in hand in a systematic and determined manner in an effort to present an accurate and relaible evidence in the court. While in the court evidence are handed over to the prosecutors who scrutinize the findings and decide whether to continue or discontinue the case. In this research the digital forensic investigation processes are mentioned below:

- Planning / Preparation
- Identification /Interaction
- Documentation
- Collection and Preservation
- Examination
- Exploratory testing
- Relational Reconstruction
- Analysis
- Result Reporting
- Presentation

The size of data problem can be lessened by using automated tools. The manual analysis of hard drive images due to available sizes in gigabytes is really not realistic. Therefore, it is important to provide a tool to perform parts of the analysis automatically while shielding investigators from unnecessary details. According to (Moore, 2006) a vital problem of digital forensics is economics. This is the employment and training of investigators, this places a financial weight on the agencies that carries out investigations. These agencies can only employ limited amount of investigators therefore leading to backlogs in digital forensics. In an attempt to solve these problems, some form of automated processing must be introduces to lessen the problem faced by digital investigators.

The data processing methodology involves several steps to reduce the number of files that require analysis and translate unreadable data into a readable form. One approach is using command line utilities. Command line remains a powerful tool for digital forensic examiners. Command line tools enable examiners to perform very specific, auditable tasks, also by scripting a series of commands together, examiners can create very powerful set of files to automate a significant portion of evidentiary processing, thereby increasing productivity while reducing the chances of human errors during routine tasks. Graphical User Interface (GUI) tools such as Encase and FTK are another approaches used for filtering data but theses tools are very complicated for most users.

The New Technologies Inc. (NTI) developed an intelligent Filter program known as the Filter_1 which has the ability to make binary data printable and to extract potentially useful data from a large volume of binary data (Middleton, 2004). The intelligent filter program or Filter_1 tool help to reduce the size of the bitstream files without sacrificing useful information. IP Filter is possibly the most interesting and useful of the Forensic Utilities. It was developed by NTI to help law enforcement track down and investigate child pornography cases. It has a simple DOS user interface and is used in almost the same way as the Filter_1 (Stephenson, 2002). The difference is that it searches for instances of email addresses, Web URLs, and graphic or Zip file names. TextSearch Plus is a utility for searching a disk for text strings. It can search both allocated space and unallocated space (slack space). When used to search the physical disk, it can be used against any file system. TextSearch Plus makes an excellent tool for parsing very large logs in an internet backtracing investigation. It uses fuzzy logic and is designed to process a large amount of data in a relatively short time.

In considering setting up a working build environment on a Windows system can be abit complex, an out-of-the-box Windows system does not have a complier or interpreters and a native capability to mount or examine image files, it only supports a handful of file systems. According to (Altheide and Carvey, 2011) compiling native Windows code will usually require the use of Microsoft's Visual Studio. Although the complete versions of Visual Studio is commercial software, Microsoft releases the Visual Studio Express versions targeted towards specific langauge at no cost.

III. The Digital Forensic Examination Platform

The forensic examination involves preparing digital evidence to support the analysis phase. The nature and extent of a digital evidence examination depends on the known circunstances of the crime and the constraints placed on the digital investigator (Casey, 2004). With the reduction in the cost of data storage amd increasing volume of commercial files in operating system and application software, forensic digital forensic examiners can be devastated easily by huge number of files on even one hard drive ot backup disk.

Therefore, digital forensic examiners need procedures, to focus in on potentially useful data.

Different digital forensic tools have unique system requirements and usually have certain requirements as to the type of operating system they can run on. According to (Casey, 2002) computers may be running completely different operating systems and file systems in the future, it is therefore important that digital investigators should not become excessively dependent on tools and must develop a solid understanding of the underlying technology and related forensic investiagation techniques.

Visual Studio is a professional tool that provides a fully Integrated Development Environment (IDE) for visual C++, Visual C#, Visual J# and Visual Basic . IDE integrated all kinds of different codes written in C++, C#, J# or the Visual Basic programming language to create Windows application. The IDE also provides a wide range of productivity enhancements, such as intelligence, code validation, an assortment of wizard that writes code and element to create and manage databases (Schneider, 2004).

Digital forensic investigators must also keep pace with new developments in area such as .NET Framework. The .NET Framework can be considered of as operating system within an operating system. It is an execution environment similar in concept to java, that is designed to run on Windows 98/ME/NT/2000/XP etc. operating systems and to provide a common environment for programs. This enables programmers to write applications in their preferred language such as visual Basic, C++, Perl etc and compile them for the .NET environment, provding greater flexibility and functionality. There are variety of operating system and applications, it is not possible to describe or even identify every possible source of information that might be useful in an investigation. Also, each case in forensic investigation is different, requiring digital investigators to explore and research components. This Chapter provides examples of important aspect of an integrated development environment, providing greater flexibility and functionality enabling programmers to write application in their preferred languaues and compile with ease and less time consumption. The integrated development environment can be a digital forensic suite for future development.

IV. Setup Of The Examination System

The setup required to perform examination with the Visual Basic Integrated Development Environment will go through the following steps.

1) Building Application

There will be one or more working build environment on the system. In this Chapter of this research there will be a generic developemnt environment that can be used to build open source applications written in the C and C++ langauges.

2) Installing Interpreters

In this resesrch some of the applications that will be used are written in interpreted languages such as Visual Basic. To run this program the appropriate interpreter and a way to install the prerequisite modules that the application rely upon is needed.

3) Working with image files

One main part of forensic examination is working with image files, which is the forensic copies of media. This is easier on some platforms than on others. It is important to be able to open a container inorder to get the content. An important part of setting up an examination system is ensuring that you can access image files directly.

4) Working with file system

This is the ability to interact with the file systems contained in image files using system functionslity.

a) Visual Basic Integrated Development Environment

The Visual Basic's Integrated Development Enviroment (IDE) enables to create, run and debug Windows programs without the need to open additional program.

Visual Basic was designed to make user-friendly programs easier to develop. Previously, programmers use language such as C or C++ etc. requiring hundred of lines of codes to get a window to appear on the screen. Recently, the same program can be created with much less time and fewer instructions.

Once Visual Basic (VB) is started the Microsoft Visual Page appears, this page tells that VB is starting. Next, the new project window appears on the screen. From this window a choce can be made to choose to create a new project or work on an existing project that is listed under the Recent tabs. A new project can be Standard executable files, ActiveX dynamic link libraries (DLLs), ActiveX controls, and Add-Ins are a few of the most commom project types. In this research standard executable file is used.

The Visual Basic Integrated Development Environment is a collection of menus. Toolbars and windows that make up a programming environment. The menu bar allows general management of programming, it is a typical drop down menu that is activated by clicking on a selected menu heading. The toolbar contains icons that provide a shortcut way of performing various tasks found on the menu bar, toolbar enables the accessing of the menu bar functionality through various toolbar buttons. Forms are the main building block of Visual Basic programs. ToolBox is used to add controls to the forms and the project explorer displays the projects, properties windows are customized within the Properties Window. The project explorer window displays a hierarchical list of open projects and the items contained in these projects. Each project is a different Visual Basic program. Therefore, Visual Basic allows a programmer to simultaneously have multiple programs open in the IDE. A form is a default container for Visual Basic controls. It involves the user interface of the program, forms is viewed on screen within the Form Layout Window. All controls in Visual Basic are objects, therefore, Visual Basic is an Object Oriented Language. All objects have different properties associated with them.

b) Code Overview

In order to write the source code, the command button on the form was double clicked. A code window opened and VB automatically places the code headings in the window. As the code was typed in, there appears a pop-up menu. This pop-up menu lists the available methods and properties of the object. Desired method or property can be selected from this pop-up menu or desired method or property name can be typed and VB will automatically scroll in the pop-up menu to method or property name. This feature is the auto code-completion feature (intellisense) of VB. This Saves a lot of time from doing numerous and rigorous coding.

The implementation code was divided into different Visual Studio programming suite, according to the functional tasks of the classes. These programming languages provided an easy way of structuring the code into clear and distinct logical groups of classes. The programming languages used in the implementation is Visual Basic.

The code view in this research is shown below:

```
Public Class Form1
    Private Sub Button1_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs)
Handles Button1.Click
        'Analyze the first character of a
string
        Dim anyString As String
        anyString = Button1.Text.ToUpper
        Select Case anyString.Substring(0, 1)
            Case "S", "z"
                Button1.Text = "The string
begins with a sibilant."
            Case "A" To "z"
                Button1.Text = "The string
begins with a nonsibilant."
            Case "0" To "9"
                Button1.Text = "The string
begins with a digit."
            Case Is < "0"
                Button1.Text = "The string
begins with a character of " & -"ANSI value
less than 48."
            Case Else
                Button1.Text = "The string
begins with : ; < = > " & -" ? @ [ \ ] ^ _ or
' . "
        End Select
    End Sub
End Class
```

c) *Installing Interpreters*

Through the installation of Microsoft Visual Studio, Visual Basic has already been installed.

d) *Working with image files*

The application of Visual Basic allows display of object. It can also allow the display of animations, play sounds, music and videos etc.

e) *Working with file system*

The VB project is composed of two main file types known as project files and form files. A VB project can contain multiple forms, but in this thesis one form is used. The project file tells VB which forms are associated with a specific project and the form file lists the objects on the form, the object property settings and the source code associated with the form.

In this research, below is a simple scenario of acquisition of data by the help of introducing simple programs in the Visual Basic environment during digital forensic investigation.

The following program has the string selector 'anyString.Substring (0, 1)'.

TABLE 1: OBJECT AND PREFIX

OBJECT	PREFIX	EXAMPLE
FORM	Frm	frmAnalyze
LABEL	Lbl	lblEnter
TEXT BOX	txt	txtString
BUTTON	btn	btnAnalyze

Object applied and their three letter Prefixes

In this scenario, the form is to analyze the first character of a string where once a string is entered in the text box and the button cliked result will be read only if the string begins with a particular selector. Below are the steps in designing the graphical user interface.

After clicking on Microsoft Visual Basic Express Edition, the first page that appears is known as Start Page.

The next step is to click on File, and then click on New Project to produce dialog box as shown in figure 4.3 and then renamed.

By using the Common Controls in the Toolbox a form is created. This is as shown in Figure 1

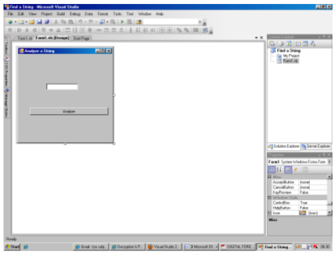
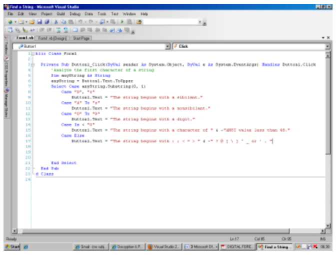


Figure 1: Text property for entering string

The next step is designing the Code Editor by clicking the right mouse button anywhere on the Main area and click on View Code. The Form Designer IDE is replaced by the Code Editor also called Code View or Code Window as shown in Figure 2



```
blic Class Form1

    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles Button1.Click
        'Analyze the first character of a string
        Dim anyString As String
        anyString = Button1.Text.ToUpper
        Select Case anyString.Substring(0, 1)
            Case "S", "z"
                Button1.Text = "The string begins with a sibilant."
            Case "A" To "z"
                Button1.Text = "The string begins with a nonsibilant."
            Case "0" To "9"
                Button1.Text = "The string begins with a digit."
            Case Is < "0"
                Button1.Text = "The string begins with a character of " & -"ANSI value less than 48."
            Case Else
                Button1.Text = "The string begins with : ; < = > " & -" ? @ [ \ ] ^ _ or ' . "



        End Select
    End Sub
d Class
```

Figure 2: Visual Basic Integrated Developer Environment Code Editor mode

In the Code Editor, lines of code will be written for the event procedure. In the case of this thesis, the first line is the header for the event procedure named `Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles Button1.Click.`

```
This procedure is triggered by the event,
Button1.Text = "The string begins with a
sibilant."
```

That means, whenever there is a sting according to the condition entered in the text box and once button is clicked the code between the two lines will appear

The program is run by pressing F5 and a dialog box is shown in Figure 3 as follows:

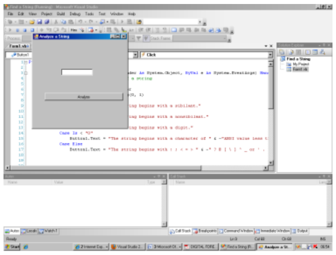


Figure 3: The code view

In the next step a string according to the second condition is entered into the text box e.g. Saturday is entered in the box and the code between the first line of condition is displayed as shown in Figure 4 below:

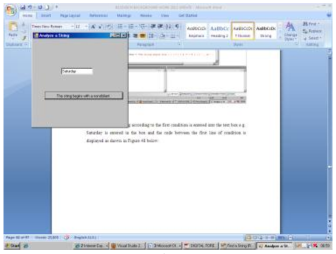


Figure 4: Text result from the string entered

In order to make a decision the investigator needs to specify a condition that determines the course of action. A condition can be said to be an expression involving relational operators such as < AND =) that is either true or false. The Visual Basic Integrated Develoment Environment facilitates a structured and disciplined approach to computer program design.

V. CONCLUSION

Digital evidence must be precise, authenticated and accurate in order to be accepted in the court. Digital evidence is fragile in nature and they must be handled properly and carefully. Detailed digital forensic investigative processes provide important assistance to forensic investigators in establishing digital evidence admissible in the court of law.

It is good practice to begin a new investigation by preparing an organised working environment. In digital forensic analysis, this involves preparing adequate and safe media on which to copy the data to be processed. This research describes the application of a techniques that can facilitates the process of digital forensic investigation, therefore allowing digital investigators to utilize less time and fewer resources.

The research introduces a structured and consistent approach for digital forensic investigation. The research provides an investigative process that helps improve digital forensic investigation identifying Visual Basic Integrated Development Environment as an environment that provides a basis for the development of techniques and especially tools to support the work of investigators. The purpose of identifying the Visual Basic Integrated Development Environment is to provide easy to use and a set of rich features which are likely to be required for developing tools that can assist digital investigators during digital forensic investigation. This technique provides a basis for future work in the development of techniques and especially tools to support the work of investigators.

ACKNOWLEDGEMENT

The authors would like to thank Dr David Preston, University of East London, and School of Architecture, Computing and Engineering and the University of Cambridge Computer laboratory for providing support during this research.

REFERENCES

[1] Ademu, I. Imafidon, C. Preston, D., (2012) Intelligent Software Agent applied to Digital Forensic and its Usefulness Vol. 2 (1) Available (online): http://interscience.in/IJCSI_Vol2Iss1/IJCSI_Paper_21.pdf Accessed on 10th April 2012

[2] Ademu, I. Imafidon, C. I. Preston, D. (2011) A New Approach of Digital Forensic Model for Digital Forensic Investigation Vol. 2, (12) Available (online): http://thesai.org/Downloads/Volume2No12/Paper%2026-A%20New%20Approach%20of%20Digital%20Forensic%20Model%20 for%20Digital%20Forensic%20Investigation.pdf Accessed 28th April 2012

[3] Altheide, C. Carvey, H (2011) Digital forensics with open source tools Pp 26 – 27 Elsevier-Waltham

[4] Carrier, B. Spafford, H. (2006), Categories of digital investigation analysis techniques based on the computer history model. Available (Online): http://dfrws.org/2006/proceedings/16-carrier.pdf Accessed on the 12th April 2012

[5] Casey, E (2004) Digital evidence and computer crime forensic science, computers and the internet 2nd Edition Pg 101 Academic Press – London

[6] Casey, E. (2002) Handbook of computer crime and investigation Pg 116 Academic Press - London

[7] Jones, K. Bejtlich, R. Rose, C. (2006) Real digital forensics: Computer security and incident response Pg 172

[8] Middleton, B. (2004) Cyber Crime Investigator's Field Guide 2nd Edition Pp 53-54 Auerbach – Florida

[9] Moore, T. (2006) The Economics of Digital Forensic Available (online): http://people.seas.harvard.edu/~tmoore/weis06-moore.pdf Accessed on 30th April 2012

[10] Nikkel, B. (2006) the role of digital forensic with a corporate organisation Available (online): www.digitalforensics.ch/nikkel/06a.pdf Accessed on 25th February 2012

[11] Palmer, G. (2001) a road map to digital forensic research Available (online): http://www.dfrws.org/2001/dfrws-rm-final.pdf Accessed on 25th April 2012

[12] Panda labs Annual Report (2009) Available (online):

[13] http://www.pandasecurity.com/img/enc/Annual_Report_Pandalabs2009.pdf Accessed on 5th May 2012

[14] Perumal, S. (2009) Digital forensic model based on Malaysian investigation process Vol. 9 (8) Available (online): http://paper.ijcsns.org/07_book/200908/20080805.pdf Accessed on 7th April 2012

[15] Schneider, D (2004) An introduction to programming using Visual Basic 6.0 4th Edition Pp 32 Prentice Hall – New Jersey

[16] Stephenson, P. (2000) Investigating Computer-Related Crime Florida: CRC pg 32.