# *FORENSICS VISUALIZATION OF WINDOWS 10 REGISTRY*

**MUHAMAD SAFWAN BIN AWANG**

**FSKTM 2019 31**

# FORENSICS VISUALIZATION OF WINDOWS 10 REGISTRY

By

**MUHAMAD SAFWAN BIN AWANG**

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Information Security

January 2019

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in
fulfilment of the requirement for the degree of Master of Information Security

## FORENSICS VISUALIZATION OF WINDOWS 10 REGISTRY

By

**MUHAMAD SAFWAN BIN AWANG**

January 2019

**Supervisor: Mohd Taufik Abdullah, Dr.**
**Faculty: Computer Science and Information Technology**

The increase with the volume of data created in digital devices has make the process of evidences analysis become difficult especially for forensic investigator. In addition, most of the existing forensic tools nowadays not all able to provide good visualization of registry information. Some of tools only able to provide the list of data but not the actual information that needed by forensic investigator. For example, Registry Viewer product of Forensic Toolkit (FTK) can display all the content of registry file but not all of the data can be view as it in hexadecimal. RegRipper tool also only provides the information of registry file in a textual result. The functions in these forensic tools not suitable if handling large number of data. Moreover, it will only cause mental fatigue for investigator if there is more than one computer they need to analyse. In this paper, a visualization forensics tool is proposed to help making the forensic analysis process become easy and faster. Proposed tool will cover the functions that the existing forensics tools do not have, especially in the visualization part. It is developed to cater for the Windows forensics in the analysis of registry hive files. Moreover, proposed tool trusted able to provide single representation of all registry hive files in one page.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia Sebagai memenuhi keperluan untuk ijazah Sarjana Keselamatan Maklumat

## VISUALISASI FORENSIC UNTUK REGISTRI WINDOWS 10

Oleh

**MUHAMAD SAFWAN BIN AWANG**

Januari 2019

**Penyelia: Mohd Taufik Abdullah, Dr.**
**Fakulti: Sains Komputer dan Teknologi Maklumat**

Peningkatan jumlah data yang dicipta dalam peranti digital telah membuat proses analisis bukti menjadi sukar terutama bagi penyiasat forensik. Di samping itu, kebanyakan alat forensik sedia ada pada masa ini tidak dapat memberikan visualisasi maklumat registri yang baik. Sesetengah alat hanya dapat menyediakan senarai data sahaja tetapi bukan maklumat sebenar yang diperlukan oleh penyiasat forensik. Sebagai contoh, Registry Viewer produk daripada Forensic Toolkit (FTK) boleh memaparkan semua kandungan fail pendaftaran tetapi tidak semua data boleh dilihat kerana ianya dalamnya format heksadesimal. RegRipper juga hanya menyediakan maklumat fail pendaftaran dalam format teks. Fungsi-fungsi dalam alat forensik terkini ini tidak sesuai jika melibatkan banyak data. Selain itu, ia hanya akan menyebabkan keletihan untuk penyiasat jika terdapat lebih daripada satu komputer yang mereka perlu analisis. Oleh itu, alat forensik visualisasi dicadangkan untuk membantu membuat proses analisis forensik menjadi mudah dan cepat. Alat yang dicadangkan akan mempunyai fungsi yang tidak ada pada alat forensik sedia ada, terutamanya dalam bahagian visualisasi. Ia dibangunkan untuk menampung forensik Windows dalam analisis fail registri. Selain itu, alat yang dicadangkan dapat memberikan satu perwakilan semua file registri dalam satu paparan.

## ACKNOWLEDGEMENTS

In the name of Allah, most Gracious, and Most Compassionate.

First of all, I would like to praise our thanks to Him for allowing me to finish this thesis. A special gratitude dedicated to my advisor, faculty supervisor Dr. Mohd Taufik Abdullah that have help and taught me to complete this thesis.

I highly thanked my supervisor because he taught and assist me on the right steps to complete this thesis. In addition, he helps me to gain idea to propose solution on current problem This help me avoid appoint a wrong title and focus on the right direction for the research. Without his help, this thesis could not be completed well.

Nonetheless, I would also like to thank our programme coordinator, Assoc. Prof. Dr. Nor Fazlida Mohd. Sani. She aids me in the thesis preparation with providing guideline to complete this thesis. This help me to get a clear view of what should be put and what should not be put into the thesis.

With their help by giving guidance, constructive comments, and encouragement have allow me to successfully complete this thesis.

# APPROVAL

This dissertation was submitted to the Information Security Department, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of **Master of Information Security**.

______________________________
**Mohd Taufik Abdullah, Dr.**
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
Date: Jan 1, 2019

# DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

**Muhamad Safwan Bin Awang**
(GS48010)
Date: Jan 1, 2019

# TABLE OF CONTENT

## LIST OF FIGURES

# CHAPTER 1 INTRODUCTION

## 1.1 Background

Throughout this paper, the topic that we will discuss is on the visualization of evidences in the Windows registry by developing a forensic visualization tool. This visualization tool will be use to visualize evidences found in Windows 10 registry. Based on definition from TechTarget website, they define data visualization as a way to assist people understand the meaning of data by placing it in a visual context. Patterns of crimes that not detected from text-based data can be produce and identified easier with the data visualization software.

## 1.2 Problem statement

There are lots of issues faced by forensic investigator when acquiring data that relevant to the crime. Large amount of data obtained caused problem when we want to view specific data. In order to solve the problem above, this project propose filter method to view and sort the specific data to be analysed. The work done by Lapso et. al. (2017) could be followed to carry out the filtering method. In the paper by Lapso et. al. (2017), they implement the whitelisting method which allow only the “known good” files and application are view in order to shrink the search space. This action helps reduces time and effort to analyse specific data that relate to the crime. So, in this project we would like to use the method where user can filter and view certain data from the Windows registry such as software.

Moreover, there is an issue to analyse the digital information obtained when collecting the data contained in a device. There will be a lot of different numbers of information stored in the suspected device. This may cause visual fatigue to the forensic investigators. To solve this issue, a good forensic tool is needed to ensure the information can be presented and visualized in a simple form for the forensic investigator. The proper development of visualization tool will not only helps produce result of the right information but able to be used as evidences to prove crimes have occurred on court hearing.

### 1.3 Research objectives

The primary purpose of the project is to propose a mechanism in visualizing the evidence found in Windows 10 registry. One of the mechanism is by filtering the result obtained. Filtering can be done in two ways, first by select type of data want to view, and by query the data want to view. Using the simplest way to view the data would help the investigation to progress more easy and efficient.  Current forensic tools may require the user a lot more steps to be taken before can view the data.

Next, to develop visualization tool that help visualize the evidence in a simple visual form. With the complexity of digital information obtained, it difficult for forensic investigator when want to view and get the required data. Thus, with the propose tool, we want to ensure that the tool able to produce a visual and graphical representation of digital information of the suspected device in more simple and easy to understand view interface. Moreover, it can assist the forensics investigators to easily determine the correlation of the data and crime events.

## 1.4 Research scope

This proposed forensic visualization tool focus on Windows 10 platform. The target items use for analysis are the Windows registry hive files which are SAM, security, software, and system. To ensure the integrity of the hive files is not modified, we will use the Forensic Toolkit (FTK) Imager to obtain them from Windows registry. forensic visualization tool application will be develop using Python programming language. This programming language is great to use as it contains modules which can support the process of parsing registry hive files.

# REFERENCES

[1] M. Debinski, F. Breitinger, and P. Mohan, "Timeline2GUI: A Log2Timeline CSV parser and training scenarios," *Digit. Investig.*, vol. 28, pp. 34–43, 2019.

[2] M. Egan, "What is the Dark Web & How to Access it," 2018. [Online]. Available: https://www.techadvisor.co.uk/how-to/internet/dark-web-3593569/.

[3] M. Rouse, "What is data visualization?," 2017. [Online]. Available: http://searchbusinessanalytics.techtarget.com/definition/data-visualization.

[4] J. A. Lapso, G. L. Peterson, and J. S. Okolica, "Whitelisting system state in windows forensic memory visualizations," *Digit. Investig.*, vol. 20, pp. 2–15, 2017.

[5] R. A. Alteiro, "Digital Forensics Tool Interface Visualization by Robert A . Altiero A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Information Systems," 2015.

[6] "About Sequoiaview," 2007. [Online]. Available: http://www.win.tue.nl/sequoiaview/.

[7] A. Barakat and A. Hadi, "Windows forensic investigations using powerforensics tool," *Proc. - 2016 Cybersecurity Cyberforensics Conf. CCC 2016*, pp. 41–47, 2016.

[8] PowerForensics, "Get-ForensicMasterBootRecord." [Online]. Available: https://powerforensics.readthedocs.io/en/latest/modulehelp/Get-ForensicMasterBootRecord/.

[9] B. Singh and U. Singh, "A forensic insight into Windows 10 Jump Lists," *Digit. Investig.*, vol. 17, pp. 1–13, 2016.

[10] R. Adams, M. Graham, and H. Valerie, "ISEEK, a tool for high speed, concurrent, distributed forensic data acquisition," *Res. Online*, no. December, 2017.

[11] Python Software Foundation, "winreg – Windows registry access," 2012. [Online]. Available: https://docs.python.org/3.1/library/winreg.html.

[12] B. Singh and U. Singh, "A forensic insight into Windows 10 Cortana search," *Comput. Secur.*, vol. 66, pp. 142–154, 2017.

[13] W. Ballenthin, "Python-registry," 2017. [Online]. Available: http://www.williballenthin.com/registry/.

[14] "Hex dumper (Python recipe)," 2018. [Online]. Available: http://code.activestate.com/recipes/142812/.

[15] "Python (programming language)," 2017. [Online]. Available: https://en.wikipedia.org/wiki/Python_(programming_language).

[16] "wxPython: Learning about TreeCtrls," 2017. [Online]. Available: https://www.blog.pythonlibrary.org/2017/05/16/wxpython-learning-about-treectrls/.

[17] J. J. Barbara, “Windows 7 Registry Forensics: Part 4,” 2012. [Online]. Available: https://www.forensicmag.com/article/2012/04/windows-7-registry-forensics-part-4.

[18] “wx,” 2018. [Online]. Available: https://docs.wxpython.org/wx.1moduleindex.html.

[19] Stackoverflow, “Why wxPython carshes while using ID_OPEN, wx.OPEN?,” 2014. [Online]. Available: https://stackoverflow.com/questions/21373936/why-wxpython-carshes-while-using-id-open-wx-open.

[20] S. Chavhan and S. M. Nirkhi, “Visualization Techniques for Digital forensics : A Survey,” *Int. J. Adv. Comput. Res.*, 2012.

[21] G. Osborne and B. Turnbull, “Enhancing computer forensics investigation through visualisation and data exploitation,” in *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 2009.