UNIVERSITI TEKNOLOGI MARA

COLLECTING DIGITAL EVIDENCE THROUGH END-DEVICE IN CLOUD COMPUTING

SITI NUR EDAYU BINTI HASHIM

MSc

January 2019

ABSTRACT

Cloud computing is a platform for many people to store their files in the cloud storage. By having this platform, it enable users to access their personal files or even share their files to anyone wherever they are and whenever they want. Due to the easy access factor the cloud storage is opened to a high security risk. There are a lot of storage services available in cloud computing and every services faces different issue in collecting forensic digital evidence .There are a few problem that would occur when collecting the evidence such as Data Acquisition problem and Log Data Acquisition problem. This paper emphasis on how end-device can act as a proxy to cloud storage services and to provide a residual data of evidence in cloud storage. This paper focuses on the extraction of potential evidence on the end device by using DD command for obtaining the image of the end device storage. The image obtain would be use in the Autopsy tools for evidence extraction. This paper give an explanation about the result obtain by two different cloud storage (Dropbox and Google Drive) and two different end devices. Throughout the experiment on this research paper, investigator able to extract residual evidence on the end user side by obtaining the evidence 86% of the evidence from end-device that have access to the cloud storage application.

ACKNOWLEDGEMENT

Alhamdullilah, praises and thanks to Allah because of His Almighty and His utmost blessing, I was able to finish this research within the time duration given. Firstly, my special thanks goes to my supervisor Dr. Kamaruddin Mamat

Special appreciation also goes to my beloved parents which is my mom and my dad Hashim bin Sudin. Also not to forget my precious auntie Raja Noor Azam binti Raja Ali.

Last but not least, I would like to give my gratitude to my dearest friends which is the members of CS7083 class.

TABLE OF CONTENT

Page

CHAPTER ONE
INTRODUCTION

1.1 Research Background

Could computing technology is evolving into one phenomena due to the advance technologies in communication, the growth of the internet usage allows the access of both software and hardware application to be use as resources by the cloud user (Mishra, S. K., Sahoo, B., & Parida, P. P., 2018).

The evolution of the computing environment has change from uni-processing environment to parallel processing, distributed computing, grid computing, ubiquitous computing, pervasive computing and now cloud computing (Burney, A., Asif, M., & Abbas, Z., 2016). In term storage to keep all information are also evolving from manual to digital which can be seen as previously all those information are store in a file and put it on the cabinet, but now all those information can be store digitally in the computer storage. Now those information can also be store in to a virtual storage which also known as a cloud storage.

Cloud computing enable a computer resource to be assessable through services on the network. Cloud computing is a platform for many people to store their files in the cloud storage. By having this platform it enable users to access their personal files or even share their files to anyone wherever they are and whenever they want through personal devices that is connected with the internet (Blakeley, B., Cooney, C., Dehghantanha, A., & Aspin, R., 2016). There is a relationship between a working devices and the wireless traffic network. Because of this properties it can inform the investigator about the communication of the end device and the wireless connection (Amundsen, A. E., & Ovens, K. M., 2017). There are variety of cloud storage services such as Dropbox™ and Google Drive™. These services can be access by users end devices by installing the application or by browsing the web services.