Automating the Generation of User Activity Timelines on Microsoft Vista and Windows 7 Operating Systems

Stephen O’Shaughnessy, Institute of Technology Blanchardstown, Ireland
Anthony Keane, Institute of Technology Blanchardstown, Ireland

ABSTRACT

For many computer forensics investigations, the discovery of the complete activity history of users is an essential part of the process; however, due to the complexity and variety of current modern personal computer operating systems, the availability of useful tools is limited. This limitation is based on the tools ability to retrieve the relevant data and present it to the investigator in a user friendly format. The current software tools that claim to extract user activity information put the onus on the investigator to construct the timeline from the data which can introduce errors and is time consuming. This paper discusses the development and evaluation of a new tool, the User Activity Tracker (UAT), which automates the visual presentation of the timeline process by retrieving and consolidating user activity data into a single source and producing as accurately as possible, the timeline of user activity on that computer. The UAT tool was tested against a modern commercial forensic tool and the results of this preliminary testing showed that the UAT tool was faster and required less manual intervention to produce a greater level of detail of the user’s activity than the commercial tool.

Keywords: Computer Forensics, Data Retrieval, Forensic Timelines, User Activity, User Activity Tracker (UAT)

1. INTRODUCTION

As computing technology advances, the volume of data that is produced from general computer use is increasing at a rapid rate. In just 10 years, the average capacity of a computer primary storage disk has seen a million fold increases from 100MB to terabytes. Consequently, computer forensics investigators have to process enormous volumes of data in order to correctly identify and extract the user activity data and this adds greatly to the cost of any investigation.

The history of development of Computer Forensics Process Models shows that most models are designed in a rigorous format for presentation of evidence in legal proceedings (Casey, 2011). These models are designed for a lengthy and detailed process that can often have an unhelpful result. These types of investiga-
tions can be potential time wasting and costly exercises that are best avoided but to do so requires a new stage in the Process Model that allows for the rapid acquisition of sufficient knowledge to indicate whether a more fuller investigation is needed or not.

In this paper we propose to introduce a new step in the digital investigation methodology that allows for a preliminary evaluation of the system to establish if a further fuller investigation is needed. The goal of this stage is to provide sufficient information to either stop the investigation or evaluate the scale (and cost) of a fuller investigation.

For the purposes of clarity, we adopt Casey’s distinction between *forensics examination* being the process of extracting and viewing information from the evidence and making it available for analysis and *forensics analysis* as the application of the scientific method and critical thinking to address fundamental questions in an investigation: who, what, where, when, how and why.

The “who” question is concerned with which user is responsible for certain actions on the system. “What” addresses what actions actually were performed on the system; “when” looks at the time these actions took place, and “how” examines what manner those actions were executed. The “where” question determines both where the responsible users were located when they initiated the actions as well as where the data on the system, i.e., files, came from. Finally, the “why” question is concerned with the motives that lie behind the actions. As a computing system cannot know the intentions of its users, the answer to this question is one that the investigator must infer from the answers to all the other questions (Buchholz & Spafford, 2004).

An important aspect in the creation of timelines of activity is the precedence of timestamps in the computer system. Looking at the recorded timestamp information associated with a file can be a great source of information to a forensic examiner. By gathering user activity information and sorting it by timestamp into a timeline allows the examiner to effectively see the order of events. Timeline analysis is used to establish what time a particular event took place and in which order those events occurred. Effective timeline analysis can either solve a case or at least shorten an investigation by reducing the amount of data to be examined (Guðjónsson, 2010). There are several steps in the process for producing a timeline of activity:

- The first step is to identify how and where user activity information is stored on a system. Under scrutiny here are the various locations that could store data, are the Registry, file system, system log files and Internet browsing history databases.
- Next, data must be collected and parsed into readable text. Many files in the Windows operating system are stored in custom binary format. As there is no one process that can extract information from all binary files, custom parsers must be implemented.
- Data must then be consolidated into a single format. Although the parsed data is in readable format, different files have different file attributes and metadata. Therefore it is important to implement a solution whereby the metadata associated with the data collected could be stored in a single format. By allowing this, the information is stored in a database for ease of sorting and retrieval. The data retrieved by the UAT tool is stored in a single format called an Evidence Object.
- The last step involves the generation of timelines of user activity. The automation of the construction of timelines of activity from the retrieved data eliminates much of the manual work involved in most forensic investigations and allows the forensic examiner can focus on a particular time span of interest, allowing them to identify any suspicious activity that occurred at a particular time with relative ease.

The UAT tool allows for a new step between the *Acquisition and Analysis stages* as illustrated in Figure 1. Here the UAT tool can be used to quickly analyse the acquired suspect