IGI PUBLISHING **ITJ 4721**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Digital Crime and Forensics, Volume 1, Issue 2
edited by **Chang-Tsun Li © 2009, IGI Global**

A Model Based Approach to Timestamp Evidence Interpretation

Svein Yngvar Willassen, Norwegian University of Science and Technology, Norway

ABSTRACT

Timestamps play an important role in digital investigations, since they are necessary for the correlation of evidence from different sources. Use of timestamps as evidence can be questionable due to the reference to a clock with unknown adjustment. This work addresses this problem by taking a hypothesis based approach to timestamp investigation. Historical clock settings can be formulated as a clock hypothesis. This hypothesis can be tested for consistency with timestamp evidence by constructing a model of actions affecting timestamps in the investigated system. Acceptance of a clock hypothesis with timestamp evidence can justify the hypothesis, and thereby establish when events occurred in civil time. The results can be used to correlate timestamp evidence from different sources, including identifying correct originators during network trace. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: *Actions; Affects; Clock Hypothesis; Digital Forensics; Time Evidence; Timestamps*

INTRODUCTION

Investigations are inquiries into past events. The purpose of an investigation is to find evidence of previous events. Investigation of digital media with the purpose of finding evidence is commonly referred to as *digital investigation*. In recent works, efforts have been made to make the digital investigation based on scientific principles, by using a hypothesis-based approach. (Carrier, 2006) In this approach, the investigator formulates his hypothesis about the occurred events, and tests them using the available evidence.

A timestamp is a recorded representation of a specific moment in time. Timestamps play an important role in digital investigations. The identification that a certain event on a computer took place at a specific time makes it possible to correlate the event with events occurring outside the computer system. These may be events occurring in another digital system, or in the physical world. A particularly important application of timestamps in digital investigation is attribution; the ability to attribute events to a

specific person. This is important, because most investigations aim at placing the responsibility for occurred events on one or more individuals. If evidence of the investigated events is digital, it may be necessary to place the event at a specific point in time in order to be able to attribute it to the correct person. If the time of the event inferred from the evidence is incorrect, it may not be possible to attribute it to anyone, or the event may be attributed to the wrong person. The prevalence of dynamic network addresses on the Internet makes timing important in all types of investigations of events that occurred on the Internet. In many such investigations, attribution relies on the identification of which computer was using an IP-address at a particular time. If the IP-address is dynamically assigned, the originating computer can only be identified if a log of the usage of the address exists, and the time of the event can be established with sufficient certainty and accuracy. Only in this case can the originating computer be identified from the usage log by selecting the correct IP-address and time entry.

A timestamp always refer to the clock from which it is generated. Since the timestamp is a function of the clock, it is always relative to the adjustment of the clock. Unfortunately, clocks are not fully reliable. Clocks may drift, thereby generating timestamps gradually more different from those generated from other clocks. Clocks may also fail, and produce completely incorrect timestamps. (Buchholz & Tjaden, 2007; Schatz, Mohay, & Clark, 2006) Further, clocks on most systems may be adjusted at any time by the user of the system to show a different date and time than civil time. The uncertainty associated with digitally stored timestamps implies that timestamps should not be relied upon as evidence without justification of these factors. In particular, it should not be blindly assumed that timestamps are based on a clock that is adjusted to civil time. These uncertainties are worrying for investigators. If timestamps cannot be relied upon, then it is in many cases not possible to trace the use of an IP-address, since identification of the time of the event is necessary to find the correct originator.

This work takes the approach that time stamps can be tested in the hypothesis based investigation model. We utilize the concepts of a clock hypothesis and consistency tests defined by Willassen (2008). A clock hypothesis is the investigator's formulation of a hypothesis about historical settings of the clock. We define a model of how an investigated system updates timestamps. We then utilize this model to test a clock hypothesis for consistency with observed timestamp values. Such testing can provide justification for a clock hypothesis. When a clock hypothesis is justified, the time of the events on the computer can be interpreted accordingly, and can then be used for correlation with other sources.

ACTIONS AFFECT TIMESTAMPS

We can build a model of the investigated system, by representing the operations in the system that can possibly change the timestamps as *actions*. A model of a system with timestamps can then be described as a table listing the timestamps and the actions that affect them. We call this an affects table.

Definition 1. *An action affects a timestamp if and only if an occurrence of that action sets a new value for the timestamp and removes the previous value for the timestamp. An affects table is a table listing all possible combinations of timestamps in a system, and all actions in the system and timestamps they affect. An affects table for a system with n timestamps has* 2^n *entries.*

Example 1. *Create an affects table for the following simple file system: the file system contains files, and each file has a Created timestamp, an Accessed timestamp and a Modified timestamp. Files can be Created, Read or Written. Reading a file causes the Accessed timestamp to be updated. Writing a file causes both the Accessed timestamp and the Modified timestamp to be updated, and Creating a*