UniTIME: Timestamp Interpretation Engine for Developing Unified Timelines

Sriram Raghavan
Secure Cyber Space (*www.securecyberspace.org*)
Email: sriram.raghavan@securecyberspace.org

Huzur Saran
Department of Computer Science & Engineering.,
IIT Delhi, New Delhi, INDIA
Email: saran@cse.iitd.ernet.in

Abstract— A critical part of many computer forensic investigations requires developing a unified timeline of activity from the timestamps of the artifacts involved, often involving digital artifacts from across multiple heterogeneous sources of evidence. However, generating such a timeline comes with its own set of challenges, especially if the provenance of the timestamps is not accurately recorded and tracked during an investigation. When sufficient provenance information is not recorded, it can result in inconsistent or ambiguous timelines.

In this paper, we propose the Provenance Information Model to address challenges related to timestamp interpretation across multiple time zones and present a provenance structure to accurately capture time zone information and validate time related assertions during analysis. We have developed a prototype implementation of the model, the UniTIME digital time-lining tool, which generates a unified timeline of events derived from across multiple sources. Our tool adjusts the timestamps obtained from multiple heterogeneous evidence sources using the provenance information to generate a unified timeline. We have validated our model and its prototype implementation using the dataset associated with the DFRWS 2008 challenge which included multiple heterogeneous sources of digital evidence with inherent timestamp interpretation challenges. Results have shown that the model is robust with respect to different time zones and varied timestamp representations. Additionally, the assertions recorded when using our PIM can be useful in identifying inconsistencies across artifacts during forensic analysis and digital time-lining.

Keywords— Digital Artifact, Provenance Information Model, Timestamp interpretation, Unified Timeline

I. INTRODUCTION

During an investigation, it is necessary to analyze the digital artifacts that were created, accessed or modified closer to the time of reported incident that is being investigated. A *digital artifact* is a self-contained unit of evidence such as a file, a log record within a log file or a network packet within a packet capture. Each digital artifact is associated with certain attributes that can be regarded as its *metadata*. A digital artifact can be regarded as the smallest unit of evidence during analysis. To conduct analysis, one can set up time windows and analyze the artifacts that were created, accessed or modified within it. However, time windows are relevant only if the artifacts' timestamps are digitally time-lined.

Timelines are usually generated using the timestamps recorded in the artifacts' metadata. However, merely sequencing timestamps across all sources cannot be relied upon. This is because timestamps have varied representations across different systems. Broadly speaking, there are three types of challenges that can arise when dealing with timestamps from across heterogeneous sources. Apart from basic syntax aspects, there are two other types of challenges, viz.,

1. *Time zone reference and timestamp interpretation; and*
2. *Clock skew, clock drift and synchronization*.

A consequence of these challenges is that a syntactic association (or timestamp value comparison) need not necessarily lead to a semantic association between the artifacts. For instance, two files with creation timestamps 09:30:00 AM July 25th 2011 AEST and 09:30:00 July 25th 2011 GMT have a syntactic association but may not share a semantic relationship as these timestamps are 10 hours apart. It is necessary to take cognizance of these interpretation challenges when metadata associations are applied to timestamps. In this paper, we examine such timestamp interpretation challenges.

A. Timestamps and Digital Events

A timestamp is the record of the time, according to some reference clock, of an associated event. A timestamp has a physical realization and a temporal interpretation [2]. Timestamps are an important part of metadata that are analyzed to determine when specific events of interest occurred. File systems typically record these three timestamps for each file that is stored within it. These timestamps indicate when a particular artifact was created, last accessed or last modified, as the case may be. Timestamps are also recorded on log files and network packet captures and these correspond to the events relevant to the respective logging context. In general, there are many types of events and in our research, we are concerned with five types of events; they are:

1. *File Create event: creation of a file in a file system*
2. *File Modify event: modification of a file in a file system*
3. *File Access event: accessing a file in a file system*
4. *Logged event: an event logged by some system or application (e.g., Web server, Internet browser)*
5. *Packet event: the arrival/receipt of a network packet on capture*

The first three events are specific to files on file systems, the fourth event is specific to records contained in log files and the last event is specific to network packets in a network capture file.

Sponsored by IEEE Louisville Chapter.
978-1-4799-4061-5/13/$31.00 ©2013 IEEE

B. Ambiguitries in Timestamp Provenance

Different digital sources record events differently and therefore the representations and resolutions of the timestamps also differ. In fact, even if multiple sources were obtained from the same location, the values for their timestamps could differ greatly. For one thing, if the location information where an NTFS or an EXT file system image was found is not recorded, it may be lost forever, since these file systems only record time with respect to UTC. As a result, whether the timestamp was recorded in Sydney (UTC +1000) at 3:30:00 PM July 1st or in New York (UTC -0400) at 10:30:00 PM the previous night, the timestamp would record a value corresponding to July 1st 5:30:00 AM UTC. Hence if the appropriate provenance of the timestamps is not recorded, despite the time-shift that is applied to the evidence on forensic tools, it can result in ambiguous timestamps which can lead to inconsistent timelines.

II. Interpreting Timestamps Using Forensic Tools

On most forensic tools, the combination of source name and its type is sufficient to determine the timestamp representation format and its time reference. The event determines the specific event name or the file name as the case may be. These timestamps correspond to the MAC timestamps for documents on a file system. On Internet logs such as the history and cache, the semantics varies, but generally timestamps correspond to the last access of a URL (history) or the timestamp on the file system when a resource (represented by a URI) is saved (cache) on the file system. Typically, forensic analysis tools read the timestamps values and while rendering, apply a *fixed* time zone shift to obtain the UTC (Universal Coordinated Time) value. In the case of timestamps from the NTFS or EXT file system, the timestamps are available in UTC and the shift is applied to obtain the local timestamp. The time shift corresponds to the time difference between UTC and the local time where the evidence was acquired. This time zone information is obtained out-of-band and all timestamps are adjusted with a uniform translation. The forensic tools process an entire forensic image at a time and hence do not maintain separate time zone information for each artifact within the image. That is to say, when a file system is analyzed, the same time zone offset is applied to the files in the file system as is to the Internet logs discovered within it. However, often file systems and logs from different homogeneous sources do not maintain the same time reference. We illustrate a generic model (in XML) for representing timestamps in Fig 1. The model shown in figure is as represented in most forensic tools. The timestamp values that are not recorded are represented by null. Source name uniquely identifies the evidence source and the type identifies the type of source, such as hard disk image or log or network packet capture. The event identifies the specific event that is represented and created, modified and last-accessed refer to the timestamps with usual meaning.

```
<timestamp>
        <source-name> name </source-name>
        <source-type> type </source-type>
        <event> event-name </event>
        <modified> value </modified>
        <created> value </created>
        <last-accessed> value </last-accessed>
</timestamp>
```

Fig 1. Generic timestamp structure

The Timestamp Interpretation Problem

The time-lining tools, currently in existence, do not carry forward the time reference information for analysis. While forensic toolkits such as Encase, FTK or Sleuthkit can take a time-reference as input, it is usually a fixed offset value common to all the contents on a forensic acquired medium. Even within a single forensic medium, there are a wide range of artifacts storing timestamps differently. The time reference and the timestamp representation of these timestamps can vary greatly which can ultimately impact the timeline generated. For instance, if we consider a FAT file system with a Windows operating system, the files store timestamps as local system time while the Internet Explorer application stores the browser log event timestamps in UTC, rendered in local time zone. This results in two distinct problems with regard to timestamp interpretation. They are:

1. *timestamp in local time without zone information (in FAT file systems and ZIP file formats)*
2. *timestamp in UTC time without zone information (in NTFS/EXTx file systems)*

One important drawback with regard to present-day digital time-lining tools is that they do not interpret the value of timestamps obtained from the source during digital time-lining. The values are used as they are found on the source (in the appropriate representation format), except perhaps, when a fixed time zone shift is applied.

To address these challenges, it is necessary to distinguish the various homogeneous sources present even within a single forensic medium and develop a provenance model that is capable of recording sufficient provenance to facilitate accurate timestamp interpretation. The model should be capable of recording information relating to when and how a particular homogeneous source was acquired, its time zone shift with respect to UTC and ideally clock skew information. Such a provenance model will allow computing accurate timestamps to generate the unified timeline, is described in the sequel.

III. Provenance Information Model to Normalize Timestamp Interpretation

The *Provenance Information Model* (or PIM) parallels the concept of Turner's digital evidence bags [7], albeit with a practical outlook. While DEB records acquisition metadata such as date and time of acquisition, the size and contents of the source and so on, it fails to record time zone information especially when dealing with FAT file systems on hard disks or ZIP archive files and so on.

A. Structure for Provenance Information Model

PIM defines a structure for recording the time information associated with a homogeneous source for analysis that incorporates time zone shifts on individual timestamps to obtain values in reference to a single time zone. Each homogeneous source is associated with its own PIM to uniquely carry forward its time reference. The provenance information model for each homogeneous source records four important components that is carried forward along with the homogeneous source during analysis, viz.,

1. *time zone information from where the homogeneous source was obtained*
2. *any known clock skew for the homogeneous source when acquired*
3. *summary of the acquisition process*
4. *assertions about events recorded in the homogeneous source*

The time zone information records the time shift of the event timestamps on a particular homogeneous source from UTC. Day light savings, if applicable, are also recorded alongside the time zone information. The PIM corresponding to the source provided in the DFRWS 2008 forensic challenge[1] contains UTC -0500 to denote the time zone of the location in the eastern coast of United States where the events were recorded. This information is recorded as a part of each homogeneous source identified in the evidence source. It is applied to the timestamps on files within ZIP archives, FAT user folder and the contents of browser cache to obtain global reference values (e.g. UTC) to generate a unified timeline. Known clock skew is also recorded and separately represented as a shift denoting number of seconds each timestamp is skewed off the reference clock. Unlike clock skew, clock drift presents a greater challenge as it is necessary to determine the exact rate at which the timestamps started to drift and the accumulated drift at the time of the acquisition (w.r.t reference clock).

B. Resilient Timestamps

Reference clock information for evidence is typically obtained out-of-band from the evidence location and transferred through manual documentation. This information, applied through forensic tools, incorporates a fixed offset to the evidence contents, without discrimination. It is however, necessary to acknowledge that there can be multiple homogeneous sources within a single forensic medium and each source requires a separate storage mechanism to record the respective time zone shifts. *PIM forms that medium*; PIM is essential for FAT file systems where time zone information is not recorded. ZIP archives do not carry MAC information of their own, and only store the last modified timestamp of the files archived in them, that too in local time with reference to where the archive was created. Therefore, while examining ZIP archives, PIM can be important to trace the provenance of the archived files. In essence, the PIM recorded for a particular homogeneous source is applied to each timestamp to derive a referenced local timestamp and corresponding global (UTC) timestamp for:

- *a local timestamp with no time zone information; and*
- *a global timestamp with no local time zone information*

Besides, the reference clock information can also be used to reverse inadvertent time zone shifts caused by analysis tools while processing the homogeneous sources, rendering the timestamps resilient to time zone shifts which can produce a robust timeline. By virtue of the resilience imparted to the timestamps, PIM is not merely a place-holder for reference clock information; PIM can also be used to validate and identify, if not correct, ambiguous or uncertain timestamps. When assertions are recorded in PIM, those assertions can be validated during digital time-lining. A variety of assertions can be recorded in PIM; for example, one may assert that all documents in a user folder have the same value for the metadata 'Author'.

C. Identifying and Validating Inconsistent Timestamps

Maintaining the UTC and a local timestamp value for each timestamp serves two purposes; firstly, to digitally timeline the events with respect to global reference, the UTC is used to which all event timestamps, irrespective of the homogeneous source type are converted, and secondly, the local time zone can be used to allow for assertions and hypothesis within the PIM of each homogeneous source that can be tested and reported back to the examiner on the outcome. For example, the examiner may posit that documents should have been used between working hours, i.e., the timestamps should have been recorded after 9 AM and before 5 PM on a weekday. Note that the examiner need not be certain that these values are necessarily correct. If this hypothesis was indeed true, it can allow one to omit files considered irrelevant and focus on a narrower group.

An examiner can make assertions such as, "*All timestamps found on a particular homogeneous source should have timestamps less than the date and time when that homogeneous source was acquired*". When this assertion is satisfied, it guarantees that the homogeneous source has been processed according to proper procedures as a sanity check mechanism. On the other hand, if this assertion is not satisfied, one of two possibilities is likely, either the chain of custody is faulty, or the timestamps were intentionally tampered. While it is still possible for such timestamps to be found with no malicious intent, such decisions are left to the examiner.

IV. Design of UniTIME unified time-lining tool

The UniTIME tool was designed to accept the sources of digital evidence as input and convert them into one or more homogeneous sources with corresponding PIM information. The timestamps within and across multiple homogeneous sources were adjusted using the respective PIM's to generate a unified timeline. The contribution of UniTIME is three-fold:

1. *Computing unambiguous UTC time value for timestamps by overlaying PIM to corresponding homogeneous source*
2. *Computing location or local time zone information based on PIM; and*
3. *Validating timestamp-based assertions that are recorded in PIM for each homogeneous source*

[1] http://www.dfrws.org/2008/challenge/submission.shtml

A. Design Overview

UniTIME was developed in Java to traverse sources of digital evidence, such as forensic hard disk images, Internet browser logs and network packet captures and harmonize them using provenance information to generate a unified timeline. UniTIME can parse timestamps from file system and document metadata on files, the Internet Explorer and Mozilla Firefox browser history and cache logs, PCAP packet captures. To parse timestamps from browser logs and network packet captures, we integrated third party applications to export log records and network packet trace as events in XML. The timestamps are then converted to UTC, validated against *related* timestamps for consistency and sorted to generate the timeline. The relationships are determined based on grouping the events determined through metadata associations. The interpretation logic for acquiring the true timestamp from different homogeneous sources using PIM, implemented in UniTIME is shown in Fig 2 which shows the time reference embedded in the PIM for each homogeneous source and their respective resolution. Two values, one UTC timestamp and the other, the local timestamp, are computed.

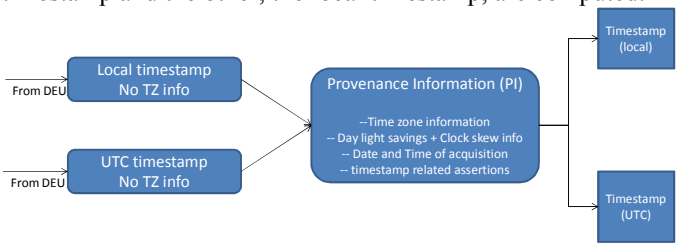

Fig 2. Timestamp interpretation logic for the digital time-lining tool

Additionally, provenance metadata of the source are included in PIM to identify inconsistencies. Tag information included with homogeneous sources in UniTIME includes:

1. *date and time of the homogeneous source acquired,*
2. *size and content list of folders; and*
3. *total size of each homogeneous source*

B. UniTIME tool architecture

The UniTIME tool architecture is shown in Fig 3. The design of the UniTIME tool was based on *f*-FIA [4] which can be divided into two parts, viz., cross-correlation layer identifying related artifacts based on metadata value matches for analysis [5] and a knowledge representation layer that address logical consistency of events and their reasoning. The *metadata match and grouping* shown in Fig. 3 addresses the former while this paper focuses on the latter for developing a unified timeline.

The tool traversed the sources and identified the homogeneous sources from which the digital artifacts and their timestamps are accessed. These artifacts, if extracted, were stored in the *Homogeneous source and Digital Artifact* repository. If it was necessary to only generate a timeline from the sources, it was sufficient to traverse the artifacts and parse the timestamps from metadata for run-time computation. On the other hand, if it was expected that the digital artifacts would be re-used (or possibly combined) with other information during analysis, then the extracted artifacts were stored into the repository. Separate file metadata parsers, Internet browser history and cache log parsers and network packet parsers were implemented to parse the metadata from the artifacts. If the metadata were expected to be re-used, they were extracted and stored into the *Metadata & Timestamps* repository. For each homogeneous source traversed, a reference PIM is created which stores the relevant information for timestamp interpretation. The PIM was populated from out-of-band information.

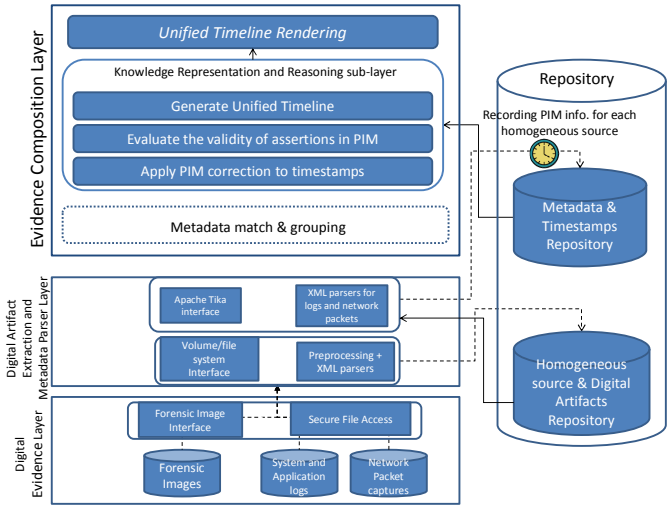

Fig 3. UniTIME architecture

C. Dataflow in UniTIME

The timestamp corrections using PIM were applied as follows: If the homogeneous source was a FAT file system, then the document metadata and the MAC file system metadata were time shifted to denote the time in local time zone where the homogeneous source was acquired and in UTC. If the homogeneous source was a homogeneous NTFS file system or an Internet browser log, then the UTC timestamp was duly recorded and the local timestamp was computed using its PIM information and validated against the assertions. Files stored in an NTFS file system, which could have originated from a FAT file system or ZIP file archives, were identified[2] prior to the timestamp corrections and treated as such. Fig 4 depicts the data flow corresponding to the timestamps corrections and validations conducted using PIM.

D. Maintaining Resilient Timestamps

When the timestamps across all homogeneous sources were corrected, the events were digitally time-lined. The tool provided the examiner the option to view these timestamps in UTC or in a selected local time zone according to its source. Additionally, the tool also provided the examiner the option of choosing to assert statements in the PIM after applying corrections to the timestamps. If the examiner chose to assert, then the timestamps were validated against the assertions, else

[2] We applied the hypothesis that timestamps within NTFS/EXT file systems which had 2-second resolution and represented timestamps in even-second intervals are likely to have originated from a FAT file system or a ZIP file. All such files are isolated and a correspondence is established to determine their PI.

the tool proceeded to the sorting of each list followed by the generation of the unified timeline. This ability enabled the examiner to initially analyze the timestamps in an unbiased manner and assert afterward, to determine the differences, if any exist. To illustrate this feature, consider a scenario where an examiner was examining a set of emails and some documents from a file system. Let the assertion state, "*the document metadata in documents found as attachments in emails should occur before the corresponding email server timestamps*". Once the appropriate PIM corrections were applied, the examiner chose not to assert and generated a timeline of all activities, both the file timestamps and email timestamps from mail servers. While the activities may all *appeared* consistent, if the examiner had asserted the statement, the examiner could have discovered that the documents were created after the email was received according to the timestamps in document metadata. Such anomalies are flagged by the tool.

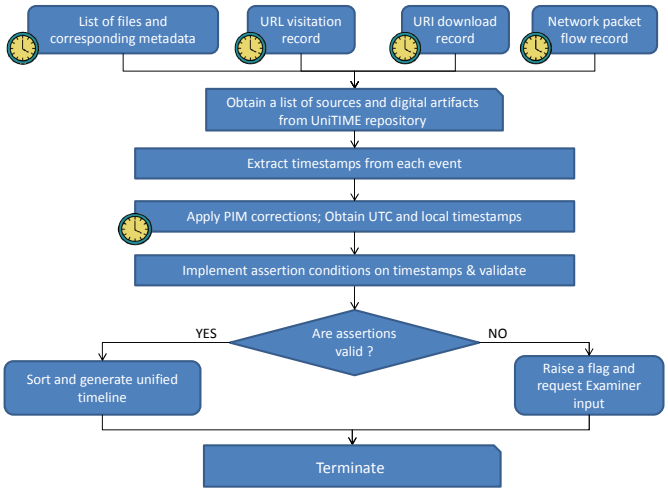

Fig 4. UniTIME Dataflow during Timestamp analysis

V. DISAMBIGUATING TIMESTAMPS FOR GENERATING A UNIFIED TIMELINE

In this section, we present a case study that uses the UniTIME digital time-lining tool. This case study is based on the DFRWS forensic challenge 2008 which contains 4 distinct homogeneous sources, 3 of which have a local time zone reference and one with UTC time reference. In order to generate a unified timeline, it was necessary to add PIM for each of the sources separately, and this was later used by UniTIME to adjust the timestamps to UTC. The evidence was provided as a ZIP archive of the user folder, the Internet browser logs from Mozilla Firefox browser containing history and cache data and a network packet capture. The original forensic image provided for the DFRWS 2008 challenge also contains a memory capture from Mr. Steve Vogon's computer. However, for the purpose of this case study, the memory capture is not used. The 4 components are treated as distinct sources of digital evidence, each with their own time zone reference:

1. *a user folder (with US/Eastern time zone reference),*
2. *the Firefox*[3] *browser history (with US/Eastern time zone reference),*
3. *the Firefox browser cache (with US/Eastern time zone reference); and*
4. *a network packet capture file (with UTC time zone reference).*

Case Outline

Mr. Steve Vogon, an employee at Saraquiot Corporation, is suspected of smuggling confidential Saraquiot information to an outsider. Based on the case brief provided on the DFRWS website, we took the location of the activities to be the east coast of the United States and accordingly the PIM for the homogeneous sources, i.e., the user folder and the browser logs was set as UTC -0500 and the network capture, to UTC. The activities recorded on the source provided (i.e., the user folder and the browser logs) occurred between May 2007 and December 2007. The network capture contains a network session in December 2007 and was captured on the IP assigned to the user's machine according to the company records.

To perform analysis, we extracted the contents of the archive and separated out the different homogeneous sources, added the appropriate PIM information, and analyzed them independently. Each homogeneous source was provided as a separate input to our tool which extracted the timestamps and applied adjustments according to the added the PIM. The detailed list of significant findings is reported in Cohen et al [1]. A merged timeline of the activities from the sources is reported in Jokerst et al [3]. Jokerst et al. extracted the source evidence in the east coast of the United States of America and sorted the resulting (rendered) timestamps using a Perl script. No explicit time zone adjustments were made to the file and browser log timestamps before or after generating the timeline. All network packet capture timestamps were adjusted with a backward shift of 5 hours before generating the timeline. In the case of Jokerst et al.'s analysis report however, since the evidence was extracted in the same time zone to that in which the activities were reported, incorrect rendering was not an issue. However, this may not always be the case. For instance, when we retraced the steps reported in [3] in Brisbane, Australia, it resulted in an inconsistent timeline where the network activities were found to occur after the time of source acquisition. We had extracted the ZIP source to the local file system but did not account for the time zone shift that would be introduced on the contents of this archive caused by the rendering. This demonstrates that, to generate a unified timeline when the timestamps are not restricted to a single time zone, it is necessary to integrate each homogeneous source with its own PIM and of course, to avoid any inappropriate rendering of this sort.

[3] Although the Firefox browser stores history and cache log timestamps internally in UTC with a local time zone offset, the timestamps were all converted into local time zone when there were compressed into the ZIP format. Besides, the time zone information was not encapsulated within the archive and hence lost.

A. Applying PIM corrections to the sources

Since the source evidence was provided as a compressed ZIP archive, the files contained within the recovered user folder had only one reliable timestamp, namely, the LAST_MODIFIED timestamp and that too, with only a 2-second precision. The timestamps on the browser logs, however, are stored differently[4] and hence were stored with 1-second precision. Most importantly, the time zone information was lost during the archival since ZIP format does not accommodate this information. The provenance for timestamps stored in the source evidence sans the network packet capture was identified as UTC -0500 and the PIM added accordingly. The timestamps of browser events and documents in the user folder were not in sync with the network packet capture timestamps. As specified earlier, the network packet capture timestamp corresponds to the time instant in UTC when the capture process sensed the packet on the network, and is inserted by the application responsible for generating the capture file.

In order to obtain the UTC values for the timestamps, all timestamps excepting those in the network packet capture had to be adjusted, i.e., by a forward shift by 5 hours. The network packet capture stored as a PCAP file, internally records timestamps in UTC and the UTC values were readily available. Correspondingly, to compute the local time zone value for the timestamps, those in the network packet capture had to be shifted back 5 hours, while the other homogeneous source timestamps did not need adjusting. Thus, each event in each of the homogeneous sources had one timestamp in UTC and a corresponding timestamp in local time (UTC -0500).

B. Validating Timestamps

After applying the PIM adjustments, the timestamps are checked for consistency to evaluate their validity based on assertions known to the investigator at that time. This case study has only one assertion, viz., the last network packet capture timestamp occurred earlier than the last timestamp recorded by the file system in the user folder in reference to a single (local or UTC) time zone, that required to be validated. However, there are many potential assertions that can be made in a similar context. Some examples of such assertions are as follows:

1. *all timestamps associated with a URI download should be later than that of the first TCP request on the history log on that domain*; and
2. *all timestamps associated with the last visit to a domain should be later than timestamps associated with downloads from that domain*

In this case study, such consistency checks correspond to validating the file system timestamps against the packet capture timestamps in the network packet capture file. Basically, the timestamps obtained from the user folder correspond to one of three file activity events (create, modify or access) as listed in Section I. The timestamps obtained from the network packet capture file correspond to the instant of packet capture. The network capture file resided within the user folder; therefore the network packet capture was created no later than the last file activity event in the user folder. After applying the PIM adjustments, the timestamps from the respective sources were sorted and we compared the last timestamp obtained from the user folder against the last timestamp obtained from the network packet capture. As long as the PIM adjustments were applied correctly to each homogeneous source, these checks would always be valid, assuming no forging of timestamps. Once the timestamps passed the consistency checks, they were digitally time-lined and presented on the console.

[4] The Firefox browser log timestamps were recorded as UNIX timestamps, number of seconds past Jan 1st 1970 UTC

VI. Discussion

In recent times, it is not uncommon to find multiple sources of digital evidence in a digital investigation and determining a unified timeline to generate a sequence of events from across all evidence sources is an important step in the forensic analysis process. In this paper, we addressed the challenge of timestamp interpretation across different time zones and representations to generate unified timelines across heterogeneous sources. A PIM is a placeholder to track timestamp provenance and record assertions for validation. Our tool incorporate the timestamps obtained from application metadata in addition to file system timestamps for corroboration during analysis.

We utilize the time zone information not only to allow the generation of unambiguous timelines but also for validating location specific assertions recorded in the PIM. This model is particularly useful when investigators need to deal with embedded file systems or file formats within other evidence sources. For instance, the PIM allows treating an archive or a log file differently from the forensic disk image within which it was discovered. Besides, the assertions within the PIMs can be validated to identify the inconsistent timestamps and alert an examiner.

VII. Conclusion & Future Work

In this paper, we introduced the concept of *provenance information model* to accurately capture time zone associations of separate bodies of digital evidence. We have developed a prototype implementation of the concept, the UniTIME tool that integrates PIM to overcome time zone ambiguities and determine timestamp inconsistencies.

In the future, we are planning to develop advanced indexing algorithms to improve the efficiency of identifying timestamp inconsistencies across heterogeneous sources. Besides, we intend to build clock drift and skew factors into the PIM that can help compute the timestamps accurately during digital time-lining. This requires us to conduct detailed studies to understand the factors that affect timestamp skew and drift in existing clocks, particularly under the influence of temperature variations. We intend to incorporate a timestamp prediction model like the Stevens' model [6] into PIM.

References

[1] Cohen M I., Collet D J., & Walters A., (2008), Submission for Forensic Challenge 2008, *Forensic Challenge 2008,* I Place,

http://sandbox.dfrws.org/2008/Cohen_Collet_Walters/, last retrieved on July 12, 2011

[2] Dyreson C. E. & Snodgrass R. T., (1993). Timestamps semantics and representation, *Journal of Information Systems*, Vol. 18(3), pp. 143-166.

[3] Jokesrst R M., Kouskoulas Y A., Saur K J., Snow K Z., & Whipple B M., Recreating Malicious Network User Activity, *Submission to the Forensic Challenge 2008*, II Place, http://sandbox.dfrws.org/2008/JHU_APL/, last retrieved on July 12, 2011

[4] Raghavan S., Clark A J., and Mohay G. (2009). FIA: An Open Forensic Integration Architecture for Composing Digital Evidence., *Forensics in Telecommunications, Information and Multimedia, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2009*, Volume 8(1), pp. 83-94, DOI: 10.1007/978-3-642-02312-5_10

[5] Raghavan S. and Raghavan S. V. (2013). *AssocGEN: Engine for Analyzing Metadata Based Associations in Digital Evidence, In Proceedings of the 2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE)***,** IEEE 978-1-4799-4061-5, Hong Kong, China, Nov 21-22, 2013.

[6] Stevens M W. (2004). Unification of relative Time Frames for Digital Forensics, *Digital Investigations,* Vol. 1(1), pp. 225-239.

[7] Turner, P. (2005). Unification of digital evidence from disparate sources (Digital Evidence Bags). *Digital Investigation,* Vol. 2(3), pp. 223-228.