ISSN 2320-9984

Volume 3 Issue 1 | March 2015 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

A Forensic Profiling for Cyber Investigation

Ravindra Kumar Gupta
Research Scholar
Department of Computer Science & Engineering
Vindhya Institute of Technology and Science
Jabalpur (M.P.), [INDIA]
Email: ravindra.gupta38@gmail.com

Sanjay Gupta
Head of the Department
Department of Computer Science & Engineering
Vindhya Institute of Technology and Science
Jabalpur (M.P.), [INDIA]
Email: sanjiit@rediffmail.com

***Abstract*—*A Computer profiling is a record of personal data linked to a particular user or user profile. A profile represents a person on the computer system and it is a logical identity of a person. A user profile can also be considered as the computer representation of a user model. User profile may include private data, files, setting of software, application, and connections which are being used. A profile can be used to keep to the information of a person. This information can be used by systems that personalize the human computer interaction. User's profiles can be found at different level like operating systems, application software or dynamic websites such as social networking web sites. Computer profiling or user profiling can be lead to make right investigation. Automated computer profiling facilitates by producing a formal hypotheses of a computer system about the computer system's activity. These hypotheses can narrow the investigation.*

***Keywords:*—*Cyber Crime, Evidence Gathering, Automated Models, Forensic Analysis.*

1. INTRODUCTION

There Computer profiling is a new systematic computer forensic activity for automatically identifying computer systems of interest. It can be described as the automated forensic reconstruction of a computer system for the purpose of characterizing its behavior and usage. Such a process is worthwhile in scenarios where investigators obtain a computer system with no specific knowledge of a crime or event to investigate, and want to learn about its usage. Rather than commit significant human and technical resources in a full-scale manual investigation of the system, investigators in such a scenario would employ an automated computer profiling tool. This tool may then be used to determine whether the computer system in question warranted such an interactive investigation, and provide some context and direction for such an investigation. A practical computer profiling software tool needs to gather information from a wide variety of different data sources, and to employ a variety of techniques to assist in its data gathering. It incorporates a suite of modules designed to examine the file system and individual files with a similar level of detail to file analysis forensic tools such as those discussed above. Additionally, it incorporates a suite of modules designed to extract meta-information about files, applications, and users, in order to facilitate automated decision making about links and relationships between them. Known file filter (KFF) technology is employed not simply to eliminate so-called "uninteresting" files, as file analysis tools currently do, but to identify and categories files. Advanced implementations can employ data mining, as advocated by Beebe and Clark, in order to improve the effectiveness and quality of the data analysis of the contents of a target computer's file system. Marring ton et al undertook a prototype implementation of a

computer profiling tool, which aggregated the output of external tools originally built to extract a very specific type of information, especially about files and users, but did not incorporate KFF technology, formal data mining techniques, nor functionality to reconstruct an activity timeline for the computer system being examined.

2. COMPUTER PROFILE

A complete computer profile is composed of the elements described above, whose inter-decencies are illustrated in Fig.2.1. A computer profile CP consists of the finite sets of all objects O, all relationships AR, all times in the history of the computer system T and all events EVT. That is:

CP = (O, R, T, EVT)

O = Represent all set of Various Object.

R = All RELETION

T = All TIME.

EvT = All EVETN.

Such a computer profile provides a useful repository of information about the computer system. The nature of the model supports the formal expression of investigative theories at a layer of abstraction which is reasonably close to a user level view of the computer system. The computer profiling object model breaks down the computer system into objects representing entities which are discrete and typed from a user's perspective. The relationships between objects naturally support graphical visualization [17].

The computer profiling object model also captures event information, permitting the investigator to form timelines about interesting objects. The combination of all this information provides a logical framework for the formulation of hypotheses about a computer system and its history.

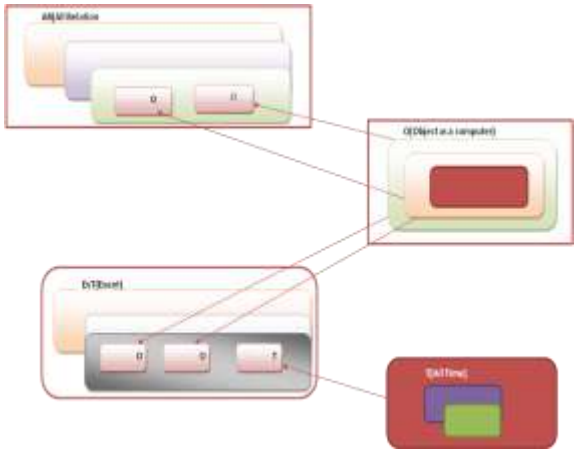

Figure 2.1: The Elements of the Computer Profile

Integral to the computer profiling process is the automated identification of the logical components of a computer system and the classification of those components according to an object model. Objects in the model correspond to identified logical components, and have a type which is part of a hierarchy of types.

Objects

A computer profile is a 4-tuple whose first element is a finite set of objects O (which are instances of the types in the type hierarchy) representing the entities discovered on a particular computer system. The set of objects belonging to a given object type is a subset of O. Let S be the set of all System objects, P be the set of all Principal objects, A be the set of all Application objects and C be the set of all Content objects:

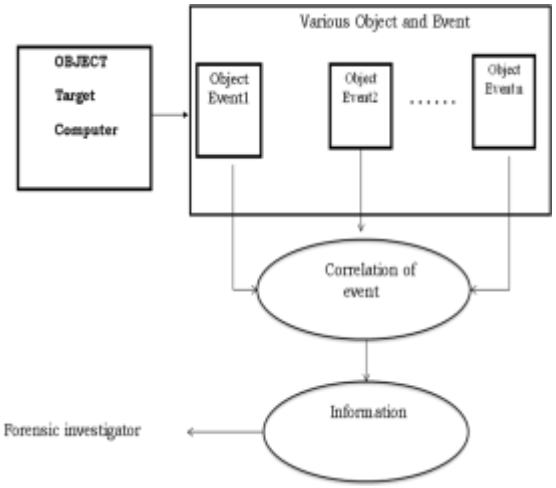

Figure 2.2: Object Interrelationship Diagram

There is no intersection between S, P, A and C. A given object can belong to one of these category sets but not to the others. Each object type has a set of its own, which is a subset of O. We follow a simple naming convention for sets of all objects of a given type, whereby the set is named by concatenating the names of the sets of all its super types, from the most general type to the most immediate super type, followed by the first letter of the type's name. For example, all User objects are elements of the set PIU, which is so named because the immediate super type of the User type is the Individual type, whose super type is the Principal type (Principal + Individual + User). The expression x PIU implies that the object x is a User type object.

The various attributes of the entities represented by objects are expressed in the computer profiling object model as the object's properties. A property is expressed as a predicate. The predicate asserts the accuracy of the description of the object or the presence of the attribute which is represented by the property. Properties shared by all objects of a type are referred to as attributes of that type.

Entities discovered on a target computer system are assigned an object type, belonging to one of the four categories. The types have a hierarchical structure, and an object can be understood to have all of its super-types as its type, in addition to its basic type. Each object type in the object type hierarchy represents an element of the computer system at a level of abstraction most understandable to a human investigator.

Relationships

The objects in a profile may be related to each other, representing some association between the respective entities they represent. Relationships are the second element of the computer profile 4-tuple. The discovery of relationships between objects is potentially of great benefit to an investigator, as relationships link a suspect object to other objects, and thus can point to probable sources of evidence. While the type hierarchy allows an object to be placed in the context of types of entities comprising a computer system, a relationship between objects allows an examiner to understand an object as a piece of evidence in the context of an investigation [17].

Let x and y be two objects, and let the predicate "related(x,y)" express the existence of a relationship between x and y. The generic relation R consists of all pairs of objects related by that predicate:

$$R = \{(x/y)|related(x,y)\}.$$

The expression xRy asserts that the objects x and y exist in the relationship set R, and are a pair of related objects. R refers to the most generic of all sets of pairs of related objects from O, constructed by the predicate "related". The predicate "related(x,y)" is true for all relationships of any description. The collection AR is a set of all sets of pairs of related objects, including the generic relationship set R. The collection AR is the second component of a computer profile. Specific sets of pairs of related objects are named by their predicate, with R as a prefix.

Events And Time

The set of events which occurred in the history of the computer system, EVT, forms an important part of the profile of the system. The inclusion of the set of all events in the computer profile allows for the reconstruction of timelines of computer activity. Connecting the events in the history of the computer system with the objects they concern facilitates the tracing of the history of particular objects. This permits selective time-lining, focusing on the object/s which is of most interest to a digital investigation [14]. Time-lining is an extremely important activity in many digital investigations, used to form and evaluate theories about the role of the computer system (and human suspects) in the crime or other event under investigation. The final elements of a computer profile are the set of all times in the history of the computer system, T, and the set of all events which have taken place in the

history of the computer system, EVT. An event in EVT consists of a 5-tuple:

$$evt = (t, O, tO, \in, \alpha).$$

The variable t refers to a time in T, o is the object which instigated the event, y is the object which was the target of the event, $\in$ is the action of the event, and α is the outcome of the event (successful, unsuccessful, or unknown).

There are three types of events in the computer profiling object model. The most straightforward is the recorded event (these were described as discovered events in [14], but we now prefer the term recorded events as more accurate). A recorded event has been found in one of the computer system's logs. A computer profiling software tool parses the system's logs and constructs a quintuple as described above for every event found in the logs. These events are all stored together in a repository for recorded events, represented by the set EVTR in the computer profiling object model. The set EVTR only represents the events in the history of the computer system which were recorded in the computer system's logs, however. Any events which are not explicitly recorded in a log must be inferred on the basis of other historical information found on the computer system, such as file system timestamps. The set of these inferred events is EVTI. The union of these two sets is the complete event history of the computer system for which some evidence remains. Nevertheless, there may still be some events in the history of the computer system of which no evidence remains, and likely some events for which some evidence remains but which were not inferred due to an imperfect software implementation. These are the unknown events, described by the set EVTU. The objective of the event inferring functionality of any software implementation of the computer profiling process is to minimize the set EVTU by inferring every event for which any evidence exists on the computer system at all.

3. CONCLUSION

Effective collection and analysis of digital evidence is a tedious task, which needs continuous analysis of data because Reliability, Security and Formality of collecting data as evidence is important legal basis or social consensus that recognizes legitimacy. In recent years the investigator had to use many forensics tools to perform investigation task. Integration of all types of forensics tools is a major challenge. The computer profiling models present a structure for development of automated computer forensic investigation. This collected evidence needs to be correlated so that, the correlation of events decides the success of forensic study and crime investigation in windows operating system environment.

4. ACKNOWLEDGMENT

The research presented in this paper would not have been possible without our college, at VITS, Jabalpur. The Authors wish to express our gratitude to all the people who helped turn the World-Wide Web into the useful and popular distributed hypertext it is. We also wish to thank the anonymous reviewers for their valuable suggestions.

REFERENCES

[1] http://en.wikipedia.org

[2] Anconelli M., "Introduzione al digital profiling," www.cybercrimes.it, 2010

[3] "A Model for Computer Profiling" International Conference in 2010.

[4] "Computer Forensics," US CERT Available www.us- cert.gov/ reading_room/forensics.pdf [Accessed: June10, 2010].

[5] Access Data, http://www. accessdata.com/