International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:3, 2014

The Use of Ontology Framework for Automation Digital Forensics Investigation

Ahmad Luthfi

***Abstract*—**One of the main goals of a computer forensic analyst is to determine the cause and effect of the acquisition of a digital evidence in order to obtain relevant information on the case is being handled. In order to get fast and accurate results, this paper will discuss the approach known as Ontology Framework. This model uses a structured hierarchy of layers that create connectivity between the variant and searching investigation of activity that a computer forensic analysis activities can be carried out automatically. There are two main layers are used, namely Analysis Tools and Operating System. By using the concept of Ontology, the second layer is automatically designed to help investigator to perform the acquisition of digital evidence. The methodology of automation approach of this research is by utilizing Forward Chaining where the system will perform a search against investigative steps and atomically structured in accordance with the rules of the Ontology.

***Keywords*—**Ontology, Framework, Automation, Forensics.

I. Introduction

THE development of computer crime investigations and computer forensics is affected by several external factors, such as advances in technology, social issues, and legal issues. The incidence of computer-related crime and telecommunications fraud has increased significantly over the last few decades [1]. Nevertheless, due to the esoteric nature of crime in the field of computers and the Internet is very dynamic, the investigators now required not only have the knowledge and experience itself, but also rather must master particular techniques and strong in knowledge management in order to investigate the process can be done briefly and precisely [1], [2].

Rapid progress in the field of Internetworking and the increasing use of the Internet, and at the same time also the number of potential sources of evidence in forensic investigations of computers has evolved as evidence of the occurrence of the relevant event which is not only of a few computers, networks, and electronic systems, but also for dissimilar organizations. In some cases, investigators will usually do a significant improvement on the results of forensics, including the complexity of the process circuit to have to do a fresh probe into the mass of data [3]. Therefore, it takes a strong semantic representation models and automated methods in the investigation of links between processes and data as evidence.

Furthermore, the fields of computer forensics rely on knowledge management systems as a source of important and critical. With this background, the fact that changes in digital technology in a case investigation, and knowledge management allows to make the right standards and procedures. Under these conditions it is necessary to establish a new framework derived from existing knowledge. Ontology composition plays an important role in creating a common definition of the domain among different information. This research will produce a contribution to the job description (framework) to automatically detect and use the computer forensics scenario approach has the ability to manage the issues of scalability and semantics that arise in forensic inter-domain. Semantic domain model to be used is a Forensics Ontology Framework, which will support the application of this approach to the standard rules of the scenario process of investigating a case of computer forensics that show flexibility in the context of a single domain. In normal conditions, when investigating a case of a forensic, investigator still have problems to acquire and analyze the digital object. There is no assurance that such evidence can be detected and retrieved resources in it [4], [5]. While using Ontology Framework approach, the system is able perform early diagnosis and directing the investigative steps to automatically process hierarchy will produce a level of better accuracy.

In a study of literature are studied, there is an important point that is very limited attention of researchers to make Ontology concept for digital investigation process is done automatically. In principle, this paper focuses on generating automated framework by using Ontology Framework that can be used by researchers as well as investigators in the context of the efficiency of the total time of the investigation.

II. Ontology Framework Approach

A. Ontology Model

Ontology has been creating a common definition among particular domain in the field of science. Simply put, this is the concept of a common information structure can be formed, reusable knowledge, assumptions in a domain can be created, and the most important is that in each section at a stage can be analyzed [6]. In the field of computer forensics, one of the vital roles the concept of Ontology is used to describe and classify specific stages in the process of investigation.

The proposed model of Ontology Framework consists of a two layers hierarchical structure where the layer has atomic construction in Technology focused on Hardware and Software (See Fig. 1).

Ahmad Luthfi is with the Islamic University of Indonesia, Yogyakarta, Indonesia (phone: +62 274895287; fax: +62 274-895007; e-mail: luthfi.informatics@ gmail.com).

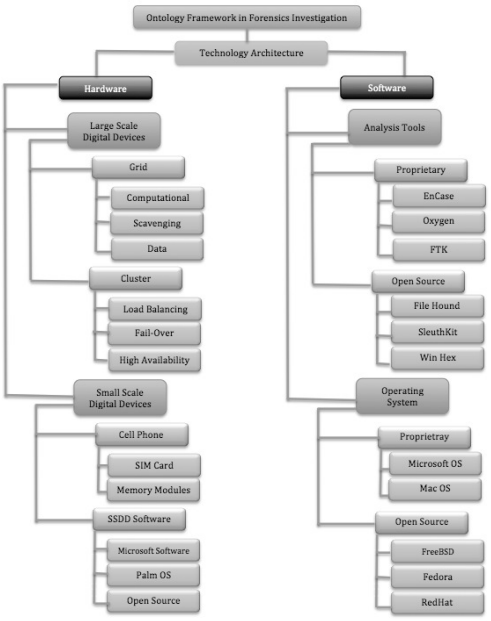

Fig. 1 Ontology Forensics Framework

In Ontology Forensic Investigation Framework, Technology is the main terminology that has two essential layers (Hardware and Software). By using the concept of the Ontology of the layers becomes more atomic as well as specified to facilitate the analyst in performing a series of investigation activities [2]. Some of the important aspects that must be considered in making the classification of sub-layers on each component are deliberated in some stage of flexibility because examiners will look for previous sub-layer during the investigation process changes or any additional activities.

B. Hardware Sub-Layer

In this paper, the Hardware as a first layer that will be considered by a forensic analyst has two sub-layers, namely the Large Scale Digital Device (LSSD), and Small Scale Digital Device (SSSD) [2]. Determination and selection of the second sub-layer is to consider the results of a review of some earlier sources that are common to Hardware category, LSSD and SSSD are able to represent at the same time cover the majority of the components or digital device forensics. LSSD can also be broken down into two parts, namely Grid and Cluster. The main justification of this sub-layer is to show that the terminology to make the process of investigation has to consider its study field first. Grid, for instance, analysts have been able to classify that device to be acquired are included Computational, Scavenging, or Data. While Cluster, have Load Balancing, Fail-Over, and High Availability as a derivative component. Consequently, LSSD structures are able to represent in general digital devices on a large scale, which becomes dynamically guide for examiners to perform a series of investigative process. SSSD, on the other hand, also has an important role in the sub-layer hardware is split into two parts, namely Cellphone and SSSD Software. Cellphone preference is due to a trend or mode of evidence that is widely used by the investigation team is currently using smartphone technology. Basically, there are two ways to get information on the acquisition of the smartphone is through the SIM Card as well as Memory Modules. Software SSD sub-layer is responsible for comparing the specifications of software installed on each Smartphone.

C. Software Sub-Layer

There are two classifications of Ontology Forensic model: Analysis Tools and Operating System. At the time of the digital evidence acquisition phase, examiners are required to have the knowledge and expertise is very good on Analysis Tools and Operating System in different platforms. By definition, data integrity can be guaranteed and acquired, including knowing where the location and history are hidden system files once deleted even before. Furthermore, an analyst must also be required to master both the manifold Analysis Tools Proprietary and Open Source platform. On the basis of the experience of the analyst team that the choice of tools not only in light of the economic value, but also in terms of services or completeness of the existing modules in the software.

Analysis tools such as EnCase, Oxygen, and FTK has modules and entire service from the device to the rooting stage analysis reports. Nevertheless, sometimes there are cases where there is evidence of communication media suspects using the latest software that has not been recognized by the Analysis Tools Proprietary. Here is an important function of the Open Source Analysis Tools such as File Hound, SleuthKit, and WinHex can be used because it is open and the analysis of the network will be able to communicate with the community as well as group to be able to develop his latest findings. In line with the Operating System that is used, for example Proprietary Software are Microsoft Windows, MacOS, typically has more complete features and services in terms of price though of course more expensive. Open Source software such as FreeBSD, Fedora, and Red Hat are able to function as an alternative Operating System is more economical and easier organization. However, the Open Source Operating System cannot be used as a reference due to different from Proprietary Operating System is licensed and examiners have usually also been certified in this field.

III. Automation Framework

In the same manner as an expert system, the process of investigation on the digital evidence can also be done using a rule-based analysis or using an expert system approach. Forward Chaining, in particular, can be used as a guide to explore the variance between digital objects into the knowledge based. Ontology will be utilized as an intelligent system that will track all of the conditions at specific stages of analysis as well as atomic. With the background of the field of semantics, it is possible for an investigator to conduct a logical and systematic analysis of the digital evidence in a case. Automation terminology used in this paper is how to make a working system analysis take advantage of the framework automatically using rules Ontology models.

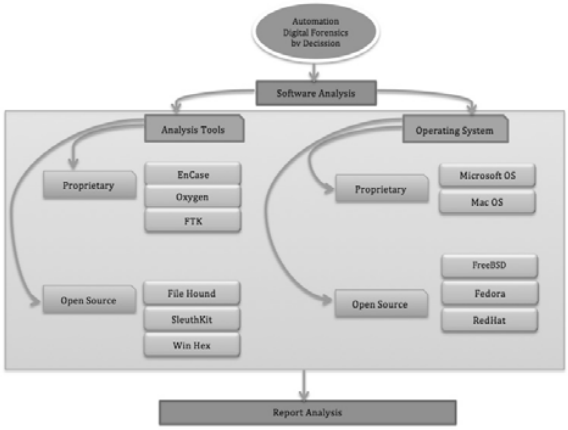

Fig. 2 Ontology Framework Automation

In Fig. 2 it can be seen how the Automation Framework work using Ontology concept where the use of expert systems approach is able to used as guidance for the examiner to undertake an investigation. The process starts from the initiation of the analysis software used are Analysis Tools and Operating System. When the system behavior examine to digital evidence, will be directed if the data can be identified by the use of Proprietary Analysis Tools as well as Operating System or not. Otherwise, Open Source system is possible to operate well. Accordingly, the system will automatically provide information to analyze sub-stages, which should be passed by the system.

IV. Conclusion

The approach presented in this paper shows that science in general Ontology can be used to assist the process of digital forensic investigations. The simplicity of the mechanism and rules that are used becomes an important factor for the development of automated systems to render this framework into a system that can automatically integrate the phases of digital forensic investigations using Ontology framework.

References

[1] Auerbach. "Computer Crime Investigation & Computer Forensics." Information Systems Security 6 (2011): 56.
[2] Ashley Brinson, Abigail Robinson, Marcus Rogers. "A Cyber Forensics Ontology: Creating a New Approach to Studying Cyber Forensics." Digital Investigation (Elsevier), 2006.
[3] Sanin, Cesar. "An OWL Ontology of Set of Experience Knowledge Structure." Journal of Universal Computer Science 13 (2007): 209-223.
[4] Bradley Schatz, George Mohay and Andrew Clark. "Rich Event Representation for Computer Forensics." Proceedings of the Fifth Asia Pacific Industrial Engineering and Management Systems Conference. Queensland: APIEMS, 2004. 2.12.1.
[5] Victor Raskin, Christian F. Hempelmann, and Katrina E. Triezenberg. "Semantic Forensics: An Application of Ontological Semantics to Information Assurance." 2011.
[6] Noy N, McGuinness D. Ontology Development 101: A Guide to Creating Your First Ontology. Available from: http://protege. stanford.edu/publications/ontology_development/ ontology101-noy-mcguinness.html; 2001 [retrieved 15.01.06]