International Journal of Computer Science and Informatics

Volume 2 | Issue 4 Article 10

April 2013

Intelligent Software Agent Applied To Digital Forensic and Its Usefulness

Inikpi O. Ademu
School of Computing, Information Technology and Engineering, Docklands Campus University of East London E16 2RD. London, United Kingdom, Iniademu2011@gmail.com

Chris O. Imafidon
School of Computing, Information Technology and Engineering, Docklands Campus University of East London E16 2RD. London, United Kingdom, c.o.imafidon@uel.ac.uk

David S. Preston
School of Computing, Information Technology and Engineering, Docklands Campus University of East London E16 2RD. London, United Kingdom, d.preston@uel.ac.uk

Recommended Citation

Ademu, Inikpi O.; Imafidon, Chris O.; and Preston, David S. (2013) "Intelligent Software Agent Applied To Digital Forensic and Its Usefulness," *International Journal of Computer Science and Informatics*: Vol. 2 : Iss. 4 , Article 10.
DOI: 10.47893/IJCSI.2013.1105
Available at: https://www.interscience.in/ijcsi/vol2/iss4/10

Intelligent Software Agent Applied To Digital Forensic and Its Usefulness

Inikpi O. Ademu, **Chris O. Imafidon & David S. Preston**

School of Computing, Information Technology and Engineering,
Docklands Campus University of East London E16 2RD. London, United Kingdom
E-mail : Iniademu2011@gmail.com, c.o.imafidon@uel.ac.uk, d.preston@uel.ac.uk

***Abstract* -** Due to the large amount of information produced, accumulated, and distributed via electronic means, it is necessary for forensic experts during crime investigation to increase their abilities to search for important evidence in a timely manner because this is essential to the success of digital forensic examinations. The inadequacy of resources both in tools and human and also limitation in time have a negative impact in result obtained during digital forensic investigation. Previous researchers state that the chances of success in criminal prosecution by law enforcement agencies depend heavily on the availability of strong evidence. The coming out of intelligent software agents that function autonomously with little or no human intervention during crime investigation is significant to the success of digital forensic investigation. Better use of tools is necessary, beyond the capabilities of the currently used forensic tools. In this paper, we discuss the usefulness of intelligent software agent in digital forensic. The goal of the paper is to provide a better knowledge and understand the concepts of intelligent software agent in digital forensic. The findings presents in this paper came from thoroughly review of previous digital forensic literature.

Keywords- *Autonomy, Case-Relevance, Digital evidence, Intelligent tools, Multi-Agent.*

I. INTRODUCTION

Large amount of information is produced, accumulated, and distributed via electronic means. It is necessary for forensic experts to increase their abilities to gather evidence from digital devices. Recent study identifies an increasing number of forensic expert’s use of standard tool in their continuing struggle against digital criminality. Sommer (2009) states that the chances of success in criminal prosecution by law enforcement agencies depend heavily on the availability of strong evidence, and failure in civil proceedings means financial loss, because a failed criminal prosecution can generate reputation damage to businesses and organizations leading to huge financial loss. The emergence of intelligent software agents that operate autonomously with little or no human intervention during crime investigation is important to the success of digital forensic investigation. Better use of software agents is necessary, beyond the capabilities of the currently used forensic tools. This paper is organized as follows: section 2 present the definition of digital forensics. Sections 3 briefly discuss Intelligent Agent and some characteristics of agent related to forensic examinations. Section 4 present related works in the use of intelligent software agent to perform forensic examination and section 5 concludes.

II. DEFINITION OF DIGITAL FORENSIC

Nikkel (2006) defined digital forensics, as the collection, preservation, analysis, and presentation of digital evidence usable for internal disciplinary hearings, digital evidence as a supporting data for internal incident report and digital evidence admissive in the court of law. The term digital forensics comprises a wide range of computer activity, not just evidence from computer, e.g. disk drive and computer memory, but including all sorts of generic media, cell phones, memory sticks, PDA’s, network traffic etc.

Palmer (2001) defined digital forensic as the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. This definition covers the broad aspects of digital forensics from data acquisition to legal action. The definition is not just narrowed to digital evidence recovered from computer but it covers digital evidence recovered from devices that are not traditionally considered to be computers Ademu, Imafidon, Preston

(2011). In agreement with this, Reith et al (2002) describe digital forensics as a synonym for computer forensics, and defines it as the use of scientific methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation helping to anticipate unauthorized actions exposed to be disrupting intended operations. Digital forensic investigation paradigm is laborious and requires significant expertise on the part of the investigator. Intelligence software agent is expected to offer more assistance in the investigation processes and better knowledge reuse and sharing in digital forensics explains (Ruibin and Gaertner, 2005).

Carrier and Spafford (2006) define digital evidence as a digital data that supports or refutes a hypothesis about digital events or the state of digital data. This definition includes evidence that may not be capable of being entered into a court of law, but may have investigative value. Carrier and Spafford (2006) describes digital forensic investigation as the process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred. One major problem in the field of digital forensic is the lack of intelligent tools to help forensic expert with the pre-analysis of data which results in collection of a large amount of data and resources contributing to waste in time to completing forensic examination. To advance the field of digital forensic investigations requires the development of intelligent tools that can be validated using scientific methods.

III. INTELLIGENT SOFTWARE AGENT

According to Williams (2005) an agent is anything that can perceive its environment through sensors and act upon that environment through effectors. The criterion that is used to evaluate and draws conclusion whether an agent is successful or not is performance measure and a critical successful factor is based on how an agent could perform a particular task. The intrinsic part of an agent is being autonomous, adaptive and cooperative in the environment which it operates. The most desirable attribute of an agent is autonomous meaning the agent should not be under the control of another agent. Wallace (1997) defined Intelligent Software Agent as software that uses Artificial Intelligence (AI) in the pursuit of the goals for its clients. AI is the limitation of human intelligence by mechanism means. In the terms of this research the word agent generally indicate intelligent software agent (ISA).

A typical agent should be autonomous; an agent should be able to do most of their tasks without any direct assistance from an outside source either human or other agents. Agents must be able to control their own actions and states. An agent should also be able to interact with other software agents as well as humans, they should be able to communicate and cooperate with other agents. According to Hermans (1997) agents was explained in weak and notion. In the weak notion of the concept of agent is autonomy: agent operates without the direct intervention of humans or other agents, social ability: agents interact with other agents and humans, proactively: agents do not simply act in response to their environment, reactivity: agents perceive their environment. The strong notion of the concept of agent mobility: this is the ability of the agent to move around an electronic network, agents do not have conflicting goals and an agent should be able to adjust itself to the habits, working methods and preferences of its user. However no particular agent possesses all these abilities but what researchers think is that these types of characteristics distinguish agents from ordinary programs.

Russell and Norvig (2010) describe an agent as anything that can perceive its environment through sensors and act upon that environment through actuators. For instance a human agent has eyes; ears for sensors and hands, legs, for actuators, a robotic agent might have cameras and infrared range finders for sensors and various motor for actuators. A typical example is Letizia, an intelligent agent used for reading documents off the worldwide web (WWW). Most of the time when the user is accessing the WWW, the computer is idle, waiting for instructions from the user to retrieve a new document. Letizia uses this otherwise idle time to look for other documents somehow related to the document being read, so that the user, after having read the document, will get suggestions for other documents that might be of interest. Letizia thus bases its searching on the contents of relatively recently read documents Lohani and Jeevan (2007). Wallace (1997) defined Intelligent Software Agent as software that uses Artificial Intelligence (AI) in the pursuit of the goals for its clients. AI is the limitation of human intelligence by mechanism means. In the terms of this research the word agent generally indicate intelligent agent (IA). The following features and properties are very important in defining intelligent agent:

A. Properties of Intelligent Agent

- *Autonomy:* The agent possesses the capacity to act independently from its user, both in chronological terms and in the sense of adding intelligence to the user's instructions, and exercising control over its own actions Williams (2004).

- *Reactivity:* The agent senses in and acts in its own surroundings. The agent also reacts to changes in the surroundings that are the result of its own actions Bradshaw (1997).

- *Proactivity:* This refers to the agent's ability to exhibit goal-directed behaviour and take initiatives by itself to get closer to the defined goal, out of an external instruction by its user Russell and Norvig (2010). It can predict, or at least make good guesses about the consequences of its own actions, and in this way use its reactivity to come closer to its goal. This should happen simultaneously, and on a periodical basis, which makes their use of enormous help in saving time.

- *Adaptability:* The agent's capacity to learn and change according to the experiences accumulated. This has to do with the feature of having memory, and learning. An agent learns from its user, from the external world and even from other agents, and progressively improves in performing its tasks, independently from external instructions Lohani and Jeevan (2007).

- *Continuity:* An agent doesn't necessarily work only when its owner is sitting by the computer, it can be active at all times. It is thus a temporally continuous process Lohani and Jeevan (2007).

- *Social ability:* An agent is social software, which interact to other agents to do its job. It can be talking to other similar agents to exchange information, or it can talk to other kinds of agents to request and offer services. Communication with the owner is also important. It is through this the agent is praised or punished for its work, and the owner can give further directions to the agent for how it can do its job better Herman (1997).

- *Flexibility:* The agent works proactively, that is directed by goals, but how it goes about to reach these goals may vary. As opposed to a script that performs the same sequence of commands each time it is run, an agent can do the same job in many different ways, depending on the situation and the surroundings Lohani and Jeevan (2007).

- *Cooperation:* The notion of cooperation with its user also seems to be fundamental in defining an agent, different from the one-way flow of information of ordinary software; intelligent agents are therefore true interactive tools William (2004).

IV. RELATED WORK

A number of different approaches have been proposed to deal with reduction in the amount of evidences to be examined during digital examination during digital investigation and measuring the reliability of digital evidence.

A research work that was done by Ruibin and Gaertner, (2005) proposes the application of a case-relevance indicator to the evidences. In their research, case-relevance is a piece of information used to measure its ability to answer questions such as who, what, where, when, why and how in crime investigation. Their work defined the level of relevance from absolutely irrelevant to probably case-relevant.

Sommer (2009) carried out research for Information Assurance Advisory Council (IAAC). The author explores the necessity for digital evidence and explained that the importance and need for digital evidence cannot be over emphasized. A huge amount of transactions are done through digital forms. People often leave their digital footprints of their activities behind from which their action or reason of action can be inferred. In as much as digital evidence is highly volatile and easily compromised by poor handling, the demand for digital evidence cannot be undermined. Gonzalez and Javier (2009) developed a procedure to enable forensic police to extract metric data from crime scenes using just a single photograph, and this is an improvement in documenting, analyzing and visualizing crime scenes.

Another research was carried out by Roussev and Richard III (2004) which proposes the case for distributed digital forensic and presents some examples where the forensic work can't perform anymore on a single workstation, and they proposed a distributed framework that shows the advantages of distributed approach. The authors design a prototype based on distributed processing and open protocol where they presented a prototype where searches can be performed 18-89 times faster using 8 machines.

V. CONCLUSION/FUTURE WORK

This work is used to show findings of the relevance and usefulness of intelligent software agent applied to digital forensic examination. Digital forensic is a very young and maturing field. Digital evidence are presented, examined, and challenged by the jury and the judges in the courtroom. There is need for more forensically sound solutions. Our future research will focus on intelligent software agent that will be based on agent technology and will benefit from the distributed nature of a multi-agent system and provide a better performance advantage and reduce the time required to perform digital forensic examination and security issues will also be analyzed.

REFERENCES

[1] Ademu, I. Imafidon, C. Preston, D. (2011) A new approach of digital forensic model for digital forensic investigation, in press.

[2] Bradshaw, J. (1997) Software Agent pg. 347 MIT Press – London

[3] Carrier, B. (2006), Categories of digital investigation analysis techniques based on the computer history model. Available (Online): http:// dfrws.org/2006/ proceedings/16-carrier.pdf Accessed on the 12th August 2011.

[4] Gonzalez, A. Javier, G. (2009). Crime scene measurements can be taken from a single image. Available (online) : http:// www. sciencedaily. com/ releases /2009/ 12/ 091201102338.htm Accessed on the 13th September 2011.

[5] Hermans, B. (1997). Intelligent software agents on the internet: An inventory of currently offered functionality in the information society and a prediction of (near) future developed. Available online: http://www. firstmonday.dk/issues /issues2_3/ch_123/ Accessed on 01 August 2011.

[6] Lohani, M, Jeevan, V. (2006) Intelligent software agents for library application Vol. 28 (3) Available (Online): www. emeraldinsight.com /0143-5124.htm Accessed on 18th October 2011.

[7] Nikkel, B. (2006) The role of digital forensic with a corporate organisation. Available (online): www.digitalforensics.ch/nikkel/06a.pdf Accessed on 25th August 2011

[8] Palmer, G. (2001). A road map for digital forensic research. Available (online): http://www.dfrws.org/2001/dfrws-rm-final.pdf Accessed on 25th February 2011.

[9] Reith, M. Carr. C. Gunsch, G. (2002), An examination of digital forensic model. Department of Electrical and Computer Engineering Air force institute of technology. Wright-Patterson. Available (Online): http://www.utica.edu/academic/institudes/ecii/ijde/articles.cfm?action Accessed on the 7th September 2011.

[10] Roussev, V. Richard III, G (2004) Breaking the performance wall: The case of distributed digital forensics Available (online): http://www. dfrws.org/2004/day2/Golden-Perfromance Accessed on 25th September 2011.

[11] Ruibin, G. Garrtner, M. (2005) Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework. Vol. 4(1) Available (Online): http://www.utica.edu/academic/ institutes/ ecii/publications/ articles/ B4A6A102- A93D-85B1-95C575D5E35F3764.pdf Accessed 24th October 2011.

[12] Russell, S. Norvig, P. (2010) Artificial Intelligence: A modern approach. 3rd Edition. Pg. 34 Prentice Hall – New Jersey.

[13] Sommer, P. (2009) Directors' and corporate advisors' guide to digital investigations and evidence: Information Assurance Advisory Council 2nd edition. Available (online): www.iaac.org.uk/Portals/0/DigitalInvestigations Guide.pdf Accessed on 3rd September 2011.

[14] Wallace, D. (1997). Intelligent software agents: Definitions and applications. Available online: http://alumnus.caltech.edu/~croft/research/agent/ definition/ Accessed on 25th August 2011.

[15] Williams, G. (2005) Software agent: A tool for digital investigation on wireless communication networks, Proceedings of AICE, IEEE, and International Conference on Advances in Information and Communication Engineering, La Palm Royal Beach Hotel, Ghana.

[16] Williams, G. (2004) Synchronizing E-Security Kluwer Academic Publishers. Pp 34-35.