International Journal of Digital Crime and Forensics
Volume 10 • Issue 2 • April-June 2018

Advances in Digital Forensics Frameworks and Tools:
A Comparative Insight and Ranking

Muhammad Abulaish, Department of Computer Science, South Asian University, New Delhi, India

Nur Al Hasan Haldar, Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia

ABSTRACT

Digital forensics science is a well-known initiative to unearth computer-assisted crimes. The thriving criminal activities using digital media have changed the typical definition of a traditional crime. Meanwhile, the means and targets of criminal activities have been transformed in a broader context due to the diverse nature of offenses associated with the multiple crime categories, affecting the way of investigations as well. In order to withstand the difficulties caused due to the crime complexity, forensics investigation frameworks are being tuned to adjust with the nature and earnestness of the felonies being committed. This article presents an in-depth comparative survey of fourteen popular and most cited digital forensics process models and various forensics tools associated with different phases of these models. The relationships among these forensics process models and their evolutions are analyzed and a graph-theoretic approach is presented to rank the existing process models to facilitate investigators in selecting an appropriate model for their investigation tasks.

KEYWORDS

Digital Forensics Framework, Digital Forensics Tools, Digital Forensics, Digital Investigation, Process Models

1. INTRODUCTION

Digital forensics (also known as computer forensics) is a systematic process of uncovering a crime through investigating the media components found in associated digital devices. The investigation practice follows a list of scientifically derived and justified mechanism towards gathering and illustrating the evidences of a crime scene. A forensic science integrates the scientific knowledge and methodology to a legal problem and criminal investigation. Over the last few years, digital forensics has been given much importance where electronic devices are used for executing an offense. Though the initial focus of digital forensics investigations was based on the crimes perpetrated using computers only, the field nowadays has been extended to incorporate different other digital devices like camera, smart phones, etc. Any digital information stored in such devices can be inspected and identified for various types of criminal activities (Kohn, Eloff & Eloff, 2013).

Forensics is a very different business when it comes to technology. Compared with traditional forensic science, digital forensics differs significantly and also poses some substantial challenges. The traditional forensics analysis involves the investigation using tangible, physical items found around the crime scene, whereas the digital forensics encompasses with various operations like extraction, storage and analysis of digital data using scientifically derived and proven methods. A traditional

DOI: 10.4018/IJDCF.2018040106

forensic analysis can logically progress step-by-step, with a common intention with widely accepted forensic practices. It is generally dependent upon the laboratory setting and on-field activities. However, in general, it comes with the widely accepted physical forensics practices. In comparison, a computer forensic science is almost technology and market driven, independent of laboratory environment and settings (Noblett, Pollitt, & Presley, 2000). The digital examinations and analysis present a unique variation in different investigations. In case of sample accumulation for investigation, traditional forensics attempts to gather as much information as possible from an evidence sample, whereas digital forensics attempts to discover only the relevant information from a large volume of heterogeneous digital data.

In digital forensic research workshop, Palmer (2001) defined digital forensics 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 is frequently cited and also accepted to be an all-inclusive definition (Kohn, Eloff, & Eloff, 2013). Willassen et al. (2005) defined digital forensics in a broader way as "…the practice of scientifically derived and proven technical methods and tools towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of after-the-fact digital information derived from digital sources for the purpose of facilitating or furthering the reconstruction of events as forensic evidence…" The main change in this definition in comparison to the Palmer's definition is that Willassen et al. have removed the criminal events and unauthorized actions. As a result, this definition extends the scope of application to include digital forensics in various types of investigation, such as commercial investigation (Kohn, Eloff, & Eloff, 2013).

However, with the arrival of new technologies, some notable changes along with challenges have been observed in the digital investigation processes. Since a contemporary crime may be introduced due to the current age digital technologies, an investigation process model should be particularly flexible and intelligent enough to deal with such unfamiliar incidents. Technology has impacted the way evidences are gathered, analyzed, and presented in courts. A large number of digital forensics investigation process models, tools and equipments have been developed for facing challenges that are raised due to technology advancements. It is important for every country or organization to develop its own digital forensics investigation mechanism based on its specified laws, rules, and policies. In general, digital forensics investigation follows a number of processes like identification, preparation, preservation, analysis, and presentation to exhaust a proper investigation. Depending on the type and intensity of a crime such processes can be divided into various phases. The identification phase recognizes the incident type and tasks to be accomplished throughout the investigation. The preparation phase is involved in analyzing the organizational infrastructure, requirements and tools to be used to carry out the investigation. The preservation phase is followed by preparation phase, where digital data are extracted from device and preserved for future analysis. One of the usages of data preservation is to cross check and validate the identified evidences. In analysis phase, data are examined to identify evidence patterns and findings from crime scene. Finally, the presentation phase generates the reports and findings and produces them in front of jury or respective management units.

The main focus of digital forensics is to exhibit digital evidences and relate them to the crime scene. The criminal evidences may be hidden within massive amount of digital data stored in various digital storage devices. The digital investigation process follows some systematic steps to extract evidences from such vast amount of digital data in such a way that they should be admissible, as well as authentic by the court of law (Richter, Kuntze, & Rudolph, 2010). One of the main objectives of digital forensics is to preserve any evidence in its most original form. In order to reconstruct past events, digital forensics targets to perform an analytical investigation by identifying, collecting and justifying the digital information. In a broader scenario, digital forensics incorporates the field of computer science with legal practices while investigating a crime. After recovering and analyzing