OPEN ACCESS Freely available online

ISSN: 2090-2697
Journal of
Forensic Biomechanics

Commentary

Complexity of Law Enforcement in Forensic Cloud Environment

Kenny Devrim*

Department of Criminology, University of Portsmouth, Hampshire, United Kingdom

ABOUT THE STUDY

The proliferation of electronic devices in modern society has led to cybercrime as criminals resort to hacking and illegally using these devices. This is mainly due to the higher rewards and lower chances of getting arrested. The rise of cybercrime poses a major challenge for forensic investigators due to the need to process vast amounts of data from various sources in a limited amount of time. As a result, investigators take longer to process cases and in some cases lose links when working with data from different sources. The increasing amount of digital evidence collected and its complexity impacts the overall processing time of digital forensics. Therefore, investigations are now concerned with big data or big data forensics. Big data forensics is the specialty of digital forensics, such as identification, collection, verification, analysis, interpretation, and representation, in which processes are performed on large data sets from various sources of evidence to identify the facts of a crime.

The biggest challenge investigators face when working with volumes stems from today's state-of-the-art forensic tools, such as the Access Data Forensic Toolkit. Forensic examiners examine a variety of sources of evidence, including well-known sources such as computers, hard drives, USB devices, the Internet of Things, devices, network data, email, and social media. Most of the time, investigators rely on manual analysis to establish correlations between evidence, which is very difficult, especially when dealing with many big data cases. To make matters worse, forensic collections are heterogeneous, and in fact, 95% of collections are unstructured. However, existing forensic tool designs are based on relational databases.

Our computer forensics lab experts forensically analyze all types of data stored on computer hard drives, USB memory sticks, cloud storage, social media, cameras, and mobile phones to find relevant digital evidence. For example, by analyzing the location of a mobile phone, we can track where the owner of the mobile phone has been. Cyber security focuses on crime prevention. In the event of a security breach, cyber forensics (also known as computer forensics) experts lead the criminal justice response. The high adoption of digital technology means that digital evidence is being generated mainly from various sources on an ongoing basis.

Digital forensics begins with gathering information in a way that preserves its integrity. Investigators then analyze the data or system to determine if it was changed, how it was changed, and by whom. The use of computer forensics is not always associated with criminal activity. Forensic processes are also used as part of data recovery processes to collect data from crashed servers, failed drives, and reformatted operating systems or any other situation where the system stops working unexpectedly. In civil and criminal justice, computer forensics helps ensure the integrity of digital evidence presented in court. With the widespread use of computers and other data-gathering devices in all fields, digital evidence (and the forensic process of collecting, storing, and investigating digital evidence) has become an integral part of solving crimes and other legal problems have become more and more important. Digital evidence doesn't just help to solve crimes in the digital world such as data theft, network breaches, and illegal online transactions but is also used to solve physical world crimes such as robberies, assaults, hit-and-runs, and murders.

The role of big data presents new encounters and opportunities for digital forensics investigators. To ensure case isolation, FCE stores each case separately in HDFS and HBase. That is, each case has its folder for storing case-related files and HBase tables prefixed with the case number. Some of the security requirements are addressed by case separation. This is because authentication measures are used against unauthorized actions to ensure that only authorized investigators can run their applications on the platform. Also, an audit trail is generated for each action taken on the evidence.

Correspondence to: Kenny Devrim, Department of Criminology, University of Portsmouth, Hampshire, United Kingdom, E-mail: kendev@edu.uk

Received: 29-Aug-2022, Manuscript No. JFB-22-18539; **Editor assigned:** 01-Sep-2022, PreQC No. JFB-22-18539 (PQ); **Reviewed:** 15-Sep-2022, QC No. JFB-22-18539; **Revised:** 22-Sep-2022, Manuscript No. JFB-22-18539 (R); **Published:** 29-Sep-2022, DOI: 10.35248/2090-2697.22.13.409

Citation: Devrim K (2022) Complexity of Law Enforcement in Forensic Cloud Environment. J Forensic Biomech.13:409.