OPEN ACCESS Freely available online

ISSN: 2090-2697
Journal of
Forensic Biomechanics

Commentary

Digital Forensics: A Key to Electronic Data

Zhu Yang*

Department of Forensic Science, The George Washington University, Washington, USA

ABOUT THE STUDY

A subfield of forensic science called "digital forensics" deals with recovering, looking into, looking at, and analyzing data discovered on digital devices, frequently in connection with mobile devices and computer crime. Originally used as shorthand for computer forensics, the term "digital forensics" has come to refer to the investigation of all devices that can store digital data. The discipline, which had its origins in the personal computing revolution of the late 1970s and early 1980s, developed in a disorganized way during the 1990s, and it wasn't until the dawn of the twenty-first century that national policies started to take shape. There are many uses for digital forensics investigations. The most typical is to prove or disprove a theory in civil or criminal court. Criminal cases centre on alleged infractions of state-sanctioned offences like murder, theft, and assault against the person that are governed by legislation, policed, and prosecuted by the state. Contrarily, civil cases focus on defending people's rights and property while also potentially involving commercial contract disputes that may involve a type of digital forensics known as electronic discovery. In the private sector, forensics may also be used, for example, in internal corporate investigations or intrusion investigations. Depending on the type of digital devices involved, the technical aspect of an investigation is further broken down into several sub-branches, including computer forensics, network forensics, forensic data analysis, and mobile device forensics. The standard forensic procedure involves the seizure, forensic imaging, and analysis of digital media, as well as the creation of a report on the gathered evidence. Digital forensics can be used to locate direct evidence of a crime as well as to assign evidence to particular suspects, verify alibis or statements, ascertain intent, identify sources, or authenticate documents. Investigations typically involve complex timelines or hypotheses and have a much wider scope than other types of forensic analysis. Acquisition or imaging of exhibits, analysis, and reporting are the three stages of a digital forensic investigation. The ideal acquisition process entails taking a snapshot of the computer's volatile memory and producing an exact sector-level duplicate of the media, frequently with the aid of a write blocking device to prevent the original from being changed. The increasing size of storage media and innovations such as cloud computing have increased the use of "live" acquisitions, which involve acquiring a "logical" copy of the data rather than a complete image of the physical storage device. To confirm the copy is accurate, the hashed values of the original media and data and the acquired image are compared. An alternative strategy combines discovery procedures with digital forensics. This method has been implemented in a for-profit tool called ISEEK, which was presented at a conference in 2017 along with test results.

CONCLUSION

Using a variety of techniques and tools, an investigator gathers evidence during the analysis phase. In 2006, forensics researcher Brian Carrier described an "intuitive procedure" in which "exhaustive searches are conducted to start filling in the gaps" after identifying the obvious evidence. While the actual analysis process can differ depending on the investigation, common methodologies include keyword searches across digital media, file recovery from deletions, and registry information extraction. In order to reconstruct events or actions and draw conclusions, the recovered evidence are analyzed, work that is frequently capable of being done by less specialized staff. When an investigation is finished, the data is presented, typically in the form of an easy-to-understand written report.

Correspondence to: Zhu Yang, Department of Forensic Science, The George Washington University, Washington, USA, E-mail: Zhuyang@gmail.com

Received: 04-Nov-2022, Manuscript No. JFB-22-19156; **Editor assigned:** 7-Nov-2022, PreQC No. JFB-22-19156 (PQ); **Reviewed**: 21-Nov-2022, QC No. JFB-22-19156; **Revised:** 29-Nov-2022, Manuscript No. JFB-22-19156 (R); **Published:** 07-Dec-2022, DOI: 10.35248/2090-2697.22.13.414

Citation: Yang Z (2022) Digital Forensics: A Key to Electronic Data. J Forensic Biomech.13:414.