Editorial
Volume 7:2, 2022

Journal of Forensic Medicine

ISSN: 2472-1026 Open Access

Editorial on Computational Forensics

Samyukta Srinivasan*

Department of Forensic Medicine, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India

Editorial

Crimes perpetrated in electronic or digital environments, especially in cyberspace, have grown increasingly widespread. Criminals are increasingly employing technology to accomplish their crimes, posing new obstacles for law enforcement officers, attorneys, judges, military personnel, and security personnel. Digital forensics has emerged as a critical tool for detecting and investigating computer-based and computer-assisted crime. This paper gives a basic overview of digital forensics.

The term "digital forensics" is often used to describe the detection and prevention of cybercrime. It's linked to digital security because both are concerned with digital occurrences. Digital forensics focuses on reactive measures, whereas digital security focuses on preventative measures. Computer forensics, network forensics, mobile device forensics, memory forensics, and email forensics are the five branches of digital forensics. Criminals are targeting peer-to-peer file sharing as a soft target. Mobile device forensics is a subfield of digital forensics that deals with recovering digital evidence from a mobile device. Email hacking has increasingly moved to the digital realm.

DF began as a synonym for computer forensics, but its scope has since broadened to encompass all digital forensics. The preservation of evidence, analysis, and presentation/reporting are the three stages of a digital forensic inquiry. Open computer systems, communication systems, and embedded computer systems all have digital evidence. It is difficult to erase digital evidence since it may be precisely replicated. Hard drives, flash drives, phones, mobile devices, routers, tablets, and equipment such as GPS all include it. Evidence must be both relevant and reliable to be acceptable in a court of law. There have been very few legal challenges against digital evidence so far. The jigsaw pieces that solve the computer crime are identified through forensic investigation.

It necessitates the use of effective tools. There are currently a variety of software tools available for skilled forensic investigators to employ. Analysts use a variety of methodologies to perform investigations while adhering to forensic science principles. Preparing a report to present the findings to all stakeholders, including the judge, jury, accused, lawyers, and prosecutors, is part of the evidence presentation process. The report must be written in a way that it can be submitted in a court of law.

Digital forensics is a multi-disciplinary and inter-disciplinary field that includes criminology, law, ethics, computer engineering, Information and Communication Technology (ICT), computer science, and forensic science, among other fields. A typical manner of depicting these connected fields. It is the process of locating and analyzing electronic data in order to preserve any evidence in its most natural state. Despite the fact that the subject of digital forensics is still in its infancy, rising awareness of DF has drew many people to it. It is undergoing a transformation from a relatively obscure tradecraft to a scientific area that must be held to higher standards on a continual basis. A number of next-generation forensic analysis technologies are in the works.

Around the world, colleges and institutions have begun to include DF courses in their information security curricula at the undergraduate and graduate levels. The Digital Forensic Research Workshop (DFRWS) has contributed more to digital forensics research and development than any other institution. Since 2001, it has hosted yearly open workshops in digital forensics. DFRWS is a non-profit organization that supports an online peer-reviewed International Journal of Digital Evidence [1-5].

Conflict of Interest

None.

References

1. Ya-Ting, Fang, Qiong Lan, and Tong Xie. “New opportunities and challenges for forensic medicine in the era of artificial intelligence technology.” *J Forensic Med* 36 (2020): 77.

2. Khanagar, Sanjeev B, Vishwanathaiah Satish, Naik Sachin, and Al-Kheraif A. Abdulaziz, et al. “Application and performance of artificial intelligence technology in forensic odontology: A systematic review.” *Leg Med* 48 (2021): 101826.

3. Pathak, Manoj, and Narang Himanshi. “Application of artificial intelligence in the field of forensic medicine.” *Indian J Forensic Med Toxicol* 15 (2021).

4. Cossellu, Gianguido, De Luca Stefano, Biagi Roberto, and Farronato Giampietro, et al. “Reliability of frontal sinus by cone beam-computed tomography (cbct) for individual identification.” *Radiol Med* 120 (2015): 1130-1136.

5. Der Mauer, Markus Auf, Well Eilin Jopp-Van, Herrmann Jochen, and Groth Michael, et al. “Automated age estimation of young individuals based on 3D knee MRI using deep learning.” *Int J Leg Med* 135 (2020): 649-663.

How to cite this article: Srinivasan, Samyukta. “Editorial on Computational Forensics.” J Forensic Med 7(2022): 165.

***Address for correspondence:** Samyukta Srinivasan, Department of Forensic Medicine, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India, E-mail: srinivasan_s@gmail.com*

Received 12 March, 2022, Manuscript No. JFM-22-58808; **Editor assigned:** 14 March, 2022, PreQC No. P-58808; **Reviewed:** 19 March, 2022, QC No. Q-58808; **Revised:** 24 March, 2022, Manuscript No. R-58808; **Published:** 29 March, 2022, DOI: 10.37421/jfm.2022.7.165