Journal of Forensic Toxicology & Pharmacology

Editorial A SCITECHNOL JOURNAL

Current Challenges and Future Research Areas for Digital Forensic Investigation

Victoria Samanidou *

Aristotle University of Thessaloniki, Department of Chemistry, Laboratory of Analytical Chemistry, Thessaloniki, Greece

***Corresponding author:** Victoria Samanidou, Aristotle University of Thessaloniki, Department of Chemistry, Laboratory of Analytical Chemistry, Thessaloniki, Greece, Tel: +30358995416; E-mail: Sctr64@gmail.com

Received date: 07 June, 2021; **Accepted date:** 20 July, 2021; **Published date:** 27 July, 2021

Editorial Note

In recent years, Information and Technology has rapidly advanced, bringing numerous benefits to the lives of the many individuals and organizations. Technologies like Internet of Things (loT) solutions, Cloud-Based Services (CBSs), Cyber-Physical Systems (CPSs) and mobile devices have brought many benefits to technologically-advanced societies. As a result, commercial transactions and governmental services have rapidly grown, revolutionizing the life sorts of many individuals living in these societies. While technological advancements undoubtedly present many advantages, at an equivalent time they pose new security threats. As a result, the amounts of cases that necessitate Digital Forensic Investigations (DFIs) are on the increase, culminating within the creation of a backlog of cases for enforcement agencies worldwide. Therefore, it's of paramount importance that new research approaches be adopted to affect these security threats. To the present end, this paper evaluates the prevailing set of circumstances surrounding the sector of Digital Forensics (DF). Our research study makes two important contributions to the sector of DF. First, it analyses the foremost difficult technical challenges that require to be considered by both LEAs and Digital Forensic Experts (DFEs). Second, it proposes important specific future research directions, the undertaking of which may assist both LEAs and DFEs in adopting a replacement approach to combating cyber-attacks.

From the past few years, technology has evolved at a way faster pace than expected. With the advancement in technology, there's an enormous increase within the number of frauds related to technology. Nowadays digital forensic investigators need to face complex challenges in digital forensic evidence collection. There are numerous digital forensic investigation techniques and tools available using which the forensic examiner can investigate cases during a better way and carve evidence. Still, various problems occur during the forensic investigation. Within the section given below a number of the frequently occurring challenges faced by the forensic investigators are thoroughly explained. So, let's begin by exploring all the problems in cybercrime investigation and study the right technique to eliminate them.

Sometimes, while investigating a case, the suspect replaces the hard disc before it's acquired by the forensic experts. In such scenarios, the info acquired from the pc system is of no evidentiary value. However, in some cases, the evidence of the replacement of the hard disc might not be apparent which again leads the investigation into darkness. There are cases during which suspects reset their mobile device in order that the investigator cannot find the specified evidence. So, in such cases, digital forensics investigator faces challenges at the time of carving evidence of communication from the mobile. In such a situation, investigators attempt to find backups in hope of fetching some evidence. In various laptops, the hard disc contains an inbuilt algorithm to self-erase data from the machine, if the drive is being removed. Under such instance, it becomes pretty difficult for the investigators to collect evidence from the hard disc without removing it. Moreover, in modern SSDs (Solid State Drives), recovery of deleted contents is another major challenge faced by the forensic investigators. During a few cases, the dimensions of a tough drive are large which suggests the investigator has got to become efficient enough while examining large volumes of electronic data. Forensic Examiners also got to be more selective about devices to be seized for examination. With the increased usage of mobile chat applications, now forensic investigators need to affect various challenges. One such complication includes the moment messages which get the auto–erased, once the message is delivered to the intended recipient.

Encryption within the devices also proves to be quite challenging while carving evidence from them. For instance, to collect evidence from a mobile messaging application like what's App, one has got to decrypt the What Sapp database. This comes bent be a challenging problem in cybercrime investigation. Nowadays, most of the businesses believe BYOD – Bring Your Own Device policy. The businesses allow employees to use their personal mobile devices to access the official communication. This has become another complex challenge faced by forensic investigators in gathering evidence during the investigation process. For instance, accessing an email from webmail employing a mobile device then downloading the attachments can cause data theft. Moreover, specific information on the device like the sort of data downloaded and therefore the file details might be difficult to trace within the current environment.

Criminals use technology for notorious tasks like data theft, identity breach etc. Whereas, development in technology is completed to supply benefits to mankind. Now, to affect such sorts of digital crimes, forensic investigators make use of various tricks and software to carve evidence and identify the criminal. Thanks to constantly developing technology alongside frequent advancing skills of criminals doggo evidence, an investigator has got to face variety of challenges during a cybercrime investigation.

Citation: *Victoria Samanidou (2021) Current Challenges and Future Research Areas for Digital Forensic Investigation. J Forensic Toxicol Pharmacol, 10:4*