Short Communication

International Journal of Forensic Research

Digital Forensics: Where Are We?

Shimaa M Motawei

Associate Professors of Forensic Medicine & Clinical Toxicology, Faculty of Medicine, Mansoura University, Egypt.

***Corresponding author**
Shimaa M Motawei, Associate Professors of Forensic Medicine & Clinical Toxicology, Faculty of Medicine, Mansoura University, El-Gomhoria street-Mansoura City, Egypt: sh-mm@mans.edu.eg

Submitted: 09 Nov 2020; **Accepted**: 16 Nov 2020; **Published**: 23 Nov 2020

Abstract

Digital Foensics is a branch of Forensic Sciences that involves the recovery of materials in digital devices, e.g. computers, mobile phones and storage devices. Fast and continuous advances in digital techniques and devices are happening. On the other hand, the forensic tools to track these technologies are short lagged. This mini-review discusses the issue and its consequences and recommendations for covering the gap between the two.

Keywords: Digital Forensics- Technology- Evidence- Gap.

Abbreviations

SMS: Short Message Service
MMS: Multimedia Message
GB: Gigabytes
GANs: Generative Adversarial Networks
UFED: Universal Forensic Extraction Device

Introduction

Digital Forensics is a branch of Forensic Sciences that involves the recovery of materials in digital devices, e.g. computers, mobile phones and storage devices. Computer Forensics is a branch of digital Forensics that pertains to retrieve the evidence from computing devices in a way to be presented in a court of law. Digital Forensics is a rapidly changing and a competitive field [1].

Digital Forensics also includes Mobile device Forensics; which is related to the recovery of data from a mobile device under forensically sound conditions. Several types of information can be retrieved from mobile devices such as contacts, photos, videos, images, calendars, notes, SMS and MMS messages [2].

Tower Dumps is a procedure that the police use to collect cell phone data without a warrant. Most cell phones activities are connected to a tower in a way that police can collect, for example, making phone calls, texting, chatting in social media and Facebook activities [3].

Forensic Toolkit (FTK) is a computer software that scans a hard drive for various information. It can locate deleted e-mails and scan a disk for text strings to use them as a password dictionary to crack encryption [3].

Cellebrite's Mobile Forensics introduced mobile Forensics products in 2007 under the family brand name 'Universal Forensic Extraction Device' (UFED), with the ability to extract both physical and logical data from mobile devices such as cell phones, tablets and other hand-held computing devices [4].

Cellebrite is a company fully owned by Sun Corporation, a publicly traded company based in Nagoya, Japan. It was reported that a data breach had happened to Cellebrite in January 2017 where 900 GB of confidential data were hacked [4].

A very rapid and startling advances in machine learning had happened over the past few years, and it has been easier to create and spread fake news that endanger communities' safety. Not only can these automatic tools be used to create compelling fakes, but they can also be turned against the Forensic known forensic techniques to bypass forensic detection; what is known of 'Generative Adversarial Networks' (GANs). This mandates the forensic tools to be upgraded continuously to face this flood of digital tools update [5].

However, the application of Digital Forensics is very deficient in the court yards and has failed obviously to reliably authenticate digital contents [6].

Hany Farid outlined five calls to the scientific community, so Digital Forensics can be more effectively used in the court. These are funding, scaling, balancing, responsibility and legislations [7].

Hany Farid stated that the field of Digital Forensics is relatively new and small, therefore it needs to grow, and this requires resources and fund-raising. He also recommended sharing of the newly-developed datasets amongst the scientific community so can better ensure that the techniques recently developed can be deployed, and be effective, at internet-scale [7].

Professor Hany Farid advised that the scientific community should have to contemplate how best to balance the contradictory goals of scientific openness with that of fueling adversaries and treating failures like the GANs. Also, enduring a responsibility on social media giants on published news will limit the proliferation of fake news that sometimes carries horrible consequences (for example the devastating violence that happened in Myanmar and Sri Lanka in the near 2018, and it has been fueled by fake news and calls to violence on Facebook). This will be supported by issuing and acting legislations that punish, fine or detain any person or company who create, spread or help in spread of fake news. This will rein the abuse and lying on social media platforms [7].

The scientific community as well as the public need to raise their awareness of the technical issues surrounding both the creation and the detection of fake contents; Hany Farid believed [7].

The past few years have given us a lesson of the consequences that happened when the digital issues were ignored as a factor affecting the incidence of crimes and shifting the public opinions to certain directions. So, it becomes a pressing need to advance our Forensic tools of unraveling digital evidence and verifying it as a tool in the court. Failure to follow the very fast advancement in technology in relation to Forensic use falls on us as a scientific community and on funding bodies, social media giants and legislatives agencies [8].

Acknowledgements: Not applicable.

Conflicts of Interests: None.

References

1. Bulbul HI, Yavuzcan HG, Ozel M (2013) Digital forensics: an analytical crime scene procedure model (ACSPM). Forensic Sci Int 233: 244-256.
2. Trcek D, Abie H, Skomedal A, Starc I (2010) Advanced framework for digital forensic technologies and procedures. J Forensic Sci 55: 1471-1480.
3. Horsman G (2018) "I couldn't find it your honour, it mustn't be there!" - Tool errors, tool limitations and user error in digital forensics. Sci Justice 58: 433-440.
4. Trček D, Abie H, Skomedal A, Starc I (2010) Advanced framework for digital forensic technologies and procedures. J Forensic Sci 55: 1471-1480.
5. Houck MM, McAndrew WP, Porter M, Davies B (2015) A Review of Forensic Science Management Literature. Forensic Sci Rev 27: 53-68.
6. Ludwig A, Fraser J (2014) Effective use of forensic science in volume crime investigations: identifying recurring themes in the literature. Sci Justice 54: 81-88.
7. Farid H (2018) Digital forensics in a post-truth age. Forensic Sci Int 289: 268-269.
8. Collie J (2018) Digital forensic evidence-Flaws in the criminal justice system. Forensic Sci Int 289: 154-155.