Developing a Digital Forensics Curriculum: Exploring Trends from 2007 to 2017

Roshan Harneker[1(✉)] and Adrie Stander[2]

[1] Department of Information Systems, University of Cape Town, Cape Town, South Africa
roshan.harneker@uct.ac.za
[2] Digital Forensics and E-Discovery Research Unit, Leiden University of Applied Sciences, Leiden, The Netherlands
stander.a@hsleiden.nl

Abstract. The young science of digital forensics has made great strides in the last decade, but so, too, has cyber crime. The growing complexity of cyber crime has necessitated that traditional forensics methods be updated to accommodate new technologies, and that further research is carried out to keep up with the rate of technological innovation. The main purpose of this paper is to determine how academic teaching and research can support the needs of the industry in investigating cyber crime. Current digital forensics curricula in higher education are discussed, followed by an analysis of academic research trends for this discipline for the years 2007 to 2017. We conclude by highlighting trends for which more research is required and which could possibly contribute towards shaping future teaching and learning of digital forensics in higher education.

Keywords: Digital forensics · Trends · Curriculum

1 Introduction

The proliferation and accessibility of the Internet have indelibly changed our lives in many positive ways. The Internet has, amongst others, improved cross-border collaboration, enabled almost instantaneous communication, and brought vast amounts of information to our fingertips at the click of a button. However, the Internet's accessibility has also lead to a cyber crime explosion, whereby it is estimated (for example) that South Africa alone loses several billions of Rand annually to cybercrime.

Digital forensics, regarded as a relatively young science [12], is an emerging area found under the broader umbrella of *computer security* that is mainly concerned with the discovery and preservation of evidence in a digital format for proof of criminal behaviour and ultimately prosecution of criminal activity [1].

For a new discipline there is a need for the creation of a digital forensics *taxonomy* to guide the academic teaching to ensure that industry expectations

B. Tait et al. (Eds.): SACLA 2019, CCIS 1136, pp. 64–76, 2020.
https://doi.org/10.1007/978-3-030-35629-3_5

and academic offerings are aligned. As technological change progresses at a rapid speed, such a digital forensics taxonomy should be updated regularly to ensure that academia keeps up with industry's needs. There is also a requirement to support overburdened law enforcement agencies that need to keep up with ever-changing technological trends and the ways these are used to commit cyber crime.

In this paper we outlines our research objectives and research limitations before moving to a definition of 'digital forensics', Higher Education Institutional (HEI) curricula, and current challenges. This is followed by a description of our methodology, a trend analysis, our results, and our summary and conclusions.

Our work aims to determine digital forensics trends covering the years 2007 to 2017 by investigating digital forensics (DF) trends published in academic resources. It also aims to highlight the current state of digital forensics research and, where possible, the needs of an industry that academic research should shift its focus to.

By highlighting certain trends, explaining their significance, and making recommendations on trends requiring more research, our analysis shall also assist with emphasising specific knowledge areas and with differentiating them from the more general knowledge areas.

There is always a possibility that the data may not match the research questions, or that it will contain particular gaps. Another limitation likely to be experienced is that *many papers conflate information security with digital forensics*. Many papers, therefore, had to be scrutinized for proper digital forensics contents before we were able to decide whether to include them into our research data set.

2 Related Work

2.1 Digital Forensics

Reith (et al.) distinguish between computer forensics and digital forensics by asserting that the former pertains specifically to methods used to find digital evidence on computers, while the latter uses scientifically verifiable methods to preserve, collect, validate, identify, analyze, interpret documents, and present evidence in digital form to be able to reconstruct incidents deemed to be of a criminal nature [13].

2.2 Higher Education Institutional Curricula and Challenges

Lang (et al.) highlighted some of the obstacles encountered when attempting to formulate an academic curriculum for digital forensics [9]. They found a lack of a standard curriculum and HEI-appropriate textbooks. Forensics training and education has a significant reliance on an instructor's or lecturer's personal experience. Moreover, the lack of a globally accepted curricular model can also contribute to institutions not adopting a forensics programme due to uncertainty

and impedance to curriculum development. Lang (et al.) also emphasise that digital forensics as a discipline straddles the areas of computer science and law [9]. Knowledge from both these fields is therefore a requirement—however: students studying digital forensics are highly unlikely to be studying both disciplines. This results in difficulties in deciding which prerequisites from each field students should have to meet, and which concepts from each field should be included in the curriculum.

Gottschalk (et al.) highlighted further difficulties pertaining to digital forensics training which is reliant on an instructor's personal experience [7]. This can turn out to be problematic due to a shortage of qualified digital forensics practitioners. Hence it can be difficult to find qualified academics to provide training in an HEI setting.

To date no generally accepted model for a digital forensics curriculum exists, although there are some curriculum standard *proposals*. In this context is interesting to note that the fast pace at which the discipline is growing, and the generally slow pace at which academic learning material is created and altered to keep up with current digital forensics trends, did not feature as a 'challenge' to the curriculum designers.

For further recent work on these (and similar) topics see also [2,10,14,15].

3 Method

Our descriptive review is meant to reveal patterns in the analyzed literature on the basis of quantifiable data such as publication time, the research methods underlying those papers, as well as their research results. Our method is *bibliometric*—i.e.: mostly using searching, filtering, and classification. We conducted a thorough and extensive literature review for relevant papers that pertain to the research area. Each paper is then treated as a single data record. This is followed by identifying trends and patterns. The result is claimed to be an accurate 'snapshot' of the current situation.

It is not practical to explore the totality of the field using interviews with academic or industry experts in the Digital Forensics field, or using questionnaires. Therefore we opted to use a descriptive literature review to determine what *new topics* emerged in the field and to get an indication of the relative importance of their *focus areas*.

Academic data was collected with help of Mendeley, a desktop- and web-based program that is used to manage and share research papers. Mendeley's use also encourages collaboration and the discovery of research data online. We opted for Mendeley's search function to avoid any bias which may arise from using specific databases such as ScienceDirect, EBSCOHost, IEEE Xplore, or the ACM DL. Search results were then further narrowed to the years from 2007 to 2017. Only the search term 'digital forensics' was entered. As the papers available via Mendeley are crowd-sourced and show the number of times an article has been read, we believe that Mendeley provides a reliable source of well-read peer-reviewed quality papers that have already been selected by a large pool of

independent researchers. We added a further delimiter to the retrieved papers by only choosing ones read by at least 5 readers.

Once enough peer-reviewed references were retrieved, the actual papers were downloaded via their hosting databases, websites or other sources. We collected 2200 articles and citations which were scanned manually for relevance by first reading abstracts and keywords. In cases where title, abstract and keywords did not provide enough information, the entire document was read to determine its relevance for our study.

During a second round of data analysis, we scanned abstracts (and read full texts if required) to exclude papers that did not have Digital Forensics as their central theme but merely mentioned it along with other interest areas. We also found papers which merely gave Digital Forensics a rather un-specific general coverage. Thus we filtered the papers that could not be placed into any relevant specific category. The papers which contained Digital-Forensics-related themes but could not be placed into a specific category were then placed into a 'general' category.

A third round of analysis involved reading all the remaining papers, and then applying *open coding* to ascertain and label variables in the form of categories, concepts and properties, as well as their interrelationships. The codes were generated from keywords as well as from analyzing the abstracts and the content of each paper.

4 Results

Our data analysis of 2200 papers, according to the method described above, revealed ≈ 50 trends. These are summarised in the following table—and further discussed thereafter—whereby the trend labeled *'General'* (Rank 6) consisted (as mentioned above) of a range of papers that either did not fit any of the specific categories, or where the topic of research was fairly broad. 'General' is thus not regarded as a trend in itself, though the papers listed under 'General' are still DF-related. Thus we consider our analysis as having revealed 49 *specific* trends, (not 50).

Rank	Digital Forensics Trend 2007–2017	#Papers	%Percent
1	DF Process	173	8.33
2	Cloud Forensics	148	7.13
3	Image Forensics	141	6.79
4	DF Tools	128	6.16
5	Mobile Forensics	117	5.63
6	*General*	82	3.95
7	Digital Evidence	74	3.56

(contniued)

(contniued)

Rank	Digital Forensics Trend 2007–2017	#Papers	%Percent
8	Network Forensics	73	3.51
9	Legal	70	3.37
10	Digital Forensics Framework	66	3.18
11	Education	62	2.99
12	Cyber crime	61	2.94
13	Digital Forensics Challenges	53	2.55
14	Hardware Forensics	52	2.50
15	Operating Systems Forensics	51	2.46
16	Information Security	51	2.46
17	Memory Forensics	49	2.36
18	Multimedia Forensics	48	2.31
19	Digital Forensics Standards	39	1.88
20	Malware Forensics	38	1.83
21	Virtualization	33	1.59
22	Internet Forensics	31	1.49
23	Live Forensics	29	1.40
24	Anti-Forensics	28	1.35
25	Digital Forensics Readiness	28	1.35
26	Email Forensics	26	1.25
27	Steganography	26	1.25
28	OSINT Forensics	25	1.20
29	Cryptography	24	1.16
30	IoT Forensics	23	1.11
31	Software Forensics	21	1.01
32	Database Forensics	20	0.96
33	Digital Forensics Trends	20	0.96
34	Big Data	16	0.77
35	Biometrics	13	0.63
36	Digital Records Forensics	13	0.63
37	Console Forensics	12	0.58
38	Drone Forensics	11	0.53
39	GPS Forensics	11	0.53
40	Incident Response	11	0.53
41	Peer 2 Peer Forensics	11	0.53
42	Digital Forensics Research	10	0.48

(contniued)

(contniued)

Rank	Digital Forensics Trend 2007–2017	#Papers	%Percent
43	eDiscovery	10	0.48
44	Visualisation	10	0.48
45	Digital Forensics Analysis	8	0.39
46	SCADA	8	0.39
47	Bitcoin	7	0.34
48	Encryption	6	0.29
49	FaaS	5	0.24
50	Machine Learning	5	0.24
	Total	2077	100

4.1 The Most Important Trends

Trends, generally, demonstrate a pattern of change in output, state or process, or the generalized inclination of a series of data points and the directions in which they shift over a period. Looking for consequential, relevant and significant trends is an important and prevalent undertaking in scientific work, whereby the statistical noteworthiness of a linear trend plotted against a time series is regularly used to classify and quantify the 'usefulness' of a trend observed [3].

Trend 1: Digital Forensics (DF) Process. The *Digital Forensics Process* is recognised as a valid scientific and forensic method used to conduct Digital Forensics investigations. It is defined as the steps to be taken from the time an alert of an incident is received to the time of the formal reporting of the analytic findings. These processes are mostly conducted on computing devices, including mobile ones, and the steps mentioned above follow the route of acquiring an image, analysing the image, and providing a written report of the investigation's findings [4].[1] In our case, the trend encompassed a range of processes and/or procedures that were proposed for use for investigations that do not necessarily fit the mould of a traditional DF-related case. Notably, the year 2013 had a 'dent' in the number of papers about processes. No papers in the data sample showed process-related papers. This does of course not mean that no papers were written that year—only that none were found with Mendeley as auxiliary tool. The analysed papers discussed digital forensics case reconstruction, chains of custody processes, text string searching, how to conduct investigations, processes to use for embedded systems, hashing, data classification, insider threats, as well as processes pertaining to log gathering and analysis. Some of the more interesting papers discussed the use of digital forensics for medical cases and pattern matching by means of artificial intelligence. A variety of process methodologies and models were also described together with practical use cases.

[1] An internationally *standardized* definition of the term *'Digital Forensic Process'* can be found in **ISO 27043**.

Much research has gone into the development of processes to follow when conducting DF-related investigations. As technology changes, this topic will no doubt continue to attract much research interest. 173 peer-reviewed papers of this topic were analysed, i.e.: 8.33% of our entire data sample.

Trend 2: Cloud Forensics. Cloud computing delivers services via shared pools of configurable computing system resources and is an ever-present transformative technology that is well known for its flexibility, scalability, elasticity, and consistency of service. It has changed the way in which data is created, stored, managed, used, shared and secured [1].

Zawoud and Hasan explain that cloud forensics is often considered as part of network forensics since cloud computing services require substantial network access, and network forensics investigations are conducted on private and public networks and the IP space [16]. Cloud forensics also includes the investigation of operating system processes, file systems, registry entries, and caches of the participating machines. Different forensics steps must be followed depending on which implementation model of cloud computing is involved. For example, collecting evidence for SaaS relies solely on the cloud service provider to obtain and send application logs, whereas with IaaS the data owner can obtain a virtual machine image directly from customers using the cloud service. This allows a forensics practitioner to examine and analyse the images.

Although cloud forensics is commonly thought of as a subset of network forensics, the research on this topic was significant enough to be considered a trend on its own. Cloud forensics came to rank 2 in our table with 148 peer-reviewed research papers, i.e.: 7.1% of the entire data sample. With the move away from private physical infrastructure towards cost-saving cloud solutions, this topic will continue to garner interest and research. Interestingly, however, research seems to wane after 2016 according to our data sample. We believe that this could be due to Digital Forensics being lumped more and more into information security research.

Since many cloud solutions are cross-jurisdictional there are also legal implications that affect where organisations and individuals store their data. Clouding is also a move away from traditional computing upon which traditional Digital Forensics methods are based. Clouding has become a ubiquitous part of life given that cloud features are built into most current smartphone and tablet mobile devices—making it both a consumer and enterprise product. Cloud investigations can stymy those who are used to the concept of taking custody of a hard drive to forensically image and analyse it, as the hard drive is not physically present on the computing device used to access the cloud service which is often accessed via a web client. The existence and use of cloud computing and its associated services such as IaaS, SaaS, and PaaS meant that new, forensically sound methods needed to be developed to acquire and analyse cloud-based data. Here we must bear in mind the different ways in which the cloud will affect the ability of a forensic practitioner to obtain the data required in a forensically sound manner.

Trend 3: Image Forensics. Image forensics refers to the processes followed to analyse and investigate digital photographic images. This should not be confused with forensic photography which refers to pictures taken at and of crime scenes for a court of law. Kim (et al.) explain 5 classification types of image forensics techniques [8]: pixel-based, format-based, camera-based, physically-based, and geometry-based. Farid describes these techniques in more detail [6]. Pixel-based techniques identify statistical deviations introduced at the pixel level and can analyse interconnections that occur because of image tampering. Format-based techniques analyse statistical associations that arise from a specific lossy compression scheme. Camera-based techniques highlight artefacts introduced by the camera's lens, sensor or onboard processing chip. Physically-based techniques model and highlight irregularities in the interaction between the camera, physical objects, and light. Lastly, geometry-based techniques measure objects being photographed and their position in relation to the camera photographing them.

The technology of today caters for almost imperceptible changes to be made to digital media that would not have been possible as recently as 20 years ago. The plethora of papers noted for image forensics—141 in total—made this trend the third most important one in our data sample assessed, (6.79% of all papers analysed). Most of those papers focused on forgery and image manipulation. Several papers described methodologies and algorithms to detect anomalies and variances from original images. The number of papers per year that contributed to this trend reached a maximum in the year 2009 and a minimum in 2017.

Trend 4: Digital Forensics Tools. This trend refers to the array of tools available for imaging, indexing and analysing digital forensics images and data artefacts. These tools are commonly used for cases that may be tried in a court of law. They must thus withstand legal scrutiny and satisfy legal requirements. 21 out of the 128 analyzed articles delved into the use of open source tools and their associated merits. Interest in this topic peaked in 2013; the 2017 yielded no such papers with our method of search. Related topics included the use of tools for automation of manual tasks, challenges associated with the use of DF tools, and using tools for investigation standardisation (amongst others).

Trend 5: Mobile Forensics. This trend covers digital forensics conducted on mobile devices including cell phones and tablets. According to [11], the influx of smartphone devices on the consumer market resulted in a burgeoning demand for digital forensics that could not be met by traditional forensics investigative techniques. There were 117 papers (5.63%) covering this trend which reached its peak in the year 2013 when smartphone usage became more ubiquitous. The papers assessed discussed operating systems forensics for Android, iOS, and Windows smartphones, legal issues pertaining to the use of cell phone data, the development of frameworks specifically for mobile device forensics, application and software forensics for mobile devices, and data recovery. Marturana (et al.) further observe that law enforcement officials are more than likely to encounter criminals with at least a smartphone in their possession than a larger computing device such as a laptop or desktop [11]. This trend in the 'top 5' also relates to the evolution of investigations from 'live forensics' which consists of examining

mobile content via the screen in a decidedly non-forensic manner. It, therefore, became important to create and streamline image acquisition, indexing, and analysis techniques that could be conducted with forensics in mind, and therefore also withstand legal scrutiny in a court of law.

Quasi-'Trend' 6: General. This quasi-'trend' is actually only a label to list all assessed papers which remained uncategorized either due to the broadness of their topics or due to too few other papers with similar content. These papers consisted of a wide range of topics covering the detection of hoaxes, fraud, and deception based on online writing style, how forensics is being shaped, and many others. In total, 86 papers fell into this category.

Trend 7: Digital Evidence. Casey defines 'digital evidence' as data in a binary form that is transmitted via or stored on a computing device that either supports or refutes a hypothesis held about how an offense has taken place or that speaks to certain aspects of the offense such as intention or alibi [4]. Data comprising digital evidence consists of either text, images, audio or video or a combination of these elements. Digital evidence has, in the past, been submitted to courts of law in the form of emails, word processor documents, GPS coordinates, digital photographs, computer printouts, backups, and computer memory to name a few. This topic consisted of 75 papers (3.56% of the total data sample). 74 of those were peer-reviewed; 1 came from a popular media sources. They discussed automated production of digital evidence, a network-based architecture proposal for the storage of digital evidence, guidelines for seizing, imaging and analysing digital evidence, the need for standardising digital evidence, how to manage digital evidence, challenges facing digital evidence, court judges' awareness of digital evidence, how to assess whether digital evidence is forensically sound, and digital evidence for mobile devices. There was an almost consistent interest in this theme between 2009 and 2015, with far fewer papers published from 2016 onwards.

Trend 8: Network Forensics. Network forensics, according to [1], forms part of network security which addresses the requirement for dedicated investigative competencies to be able to investigate the origin and traversing of malicious network traffic—which constitutes security attacks—by dealing with the acquisition, recording, and analysis of network-related events for law enforcement purposes. 73 papers were analysed for this trend with discussions of intrusion investigations, analysis of VoIP traffic, proposals of network forensics frameworks, IP traceback models, analysis of wireless network traffic, connection chain analysis, network security, locational wireless and social media surveillance, wireless security vulnerabilities, evidential discovery of networked smart devices, organisational network forensics readiness, network analysis of the ToR network, network forensics education, network forensics challenges, and analysis of honeypot traffic, to name a few. Most of those papers were written in 2010 and then again in 2014. Fewer papers in this category appeared from 2016 onwards—perhaps due to the tie-in between this topic and network security which is a subset of

information and cyber security. This topic constituted 3.51% of the total number of papers analysed.

Trend 9: Legal Matters. This trend refers to the legal aspects of digital forensics. As the 9th trend in our list it consists of 73 papers, 70 of which are peer-reviewed; (2 were duplicates and 1 came from a popular media source). This trend comprised 3.37% of our total data sample. These papers discussed legal issues affecting digital forensics tools, forensics and the legal system, the validation of digital evidence for legal argument, bridging differences in digital forensics for law enforcement and national security, forensic analysis of a false digital alibi, investigating and prosecuting cyber crime, digital forensics and legal systems across different countries, legal and technical issues affecting digital forensics, and digital forensics testimony in courts of law. Interest in this research topic peaked in 2008 and then again in 2011, but declined from 2016 onwards. This is decline of interest is peculiar, as digital forensics is a process that exists primarily for courts of law.

Trend 10: Digital Forensics Frameworks. This very important field of research addresses frameworks for digital forensics, of which many have been proposed since this science first emerged. At present, there is no de-facto framework that acts as a one-size-fits-all. Since digital evidence can be found on almost any computing device, several frameworks exist to cater for the different hardware and software technologies. What remains constant is that the methods used to extract and analyse data for a digital forensics investigation must withstand legal scrutiny. This trend accounts for 68 papers (3.18% of the entire sample) of which 66 were peer-reviewed, (1 was a duplicate and 1 was from a popular media source). The papers discussed digital forensics investigative frameworks, forensics frameworks for web-related services, triage frameworks for digital forensics, open source frameworks for digital forensics, frameworks for analysing internet-related traffic, frameworks aimed at enhancing timeline analysis during a forensic investigation, disk monitoring and analysis frameworks, frameworks for hybrid evidence investigation, and a case-based reasoning framework aimed at improving the trustworthiness of forensic investigations.

Trend 11: Education. This trend comprised 62 papers (2.99% percent of the total data sample) with 2010 as the year in which most of its papers were published. The discussion in these papers focussed on various education programmes and curricula in use in countries around the world, on incorporating digital forensics understanding into law school programmes, creation of practical lab exercises for students studying forensics, case studies in teaching forensics, defining agendas for forensics education, assessment strategies for forensics training, as well as teaching forensics in different operating system environments.

Year	Most-Researched Trend
2007	Digital forensic process
2008	Digital forensic process
2009	Image forensics
2010	Image forensics
2011	Image forensics
2012	Cloud forensics
2013	Digital forensic process
2014	Cloud forensics
2015	Cloud forensics
2016	Cloud forensics
2017	Cloud forensics

4.2 Data Analysis of Papers by Years

From a starting point in 2007 with 120 papers, the field showed consistent growth until 2016 with 279 papers, at which point it began to taper off. This may be attributed to the increase in academic research focused on information and cyber security. Facets of forensics have been absorbed into information security, such as incident response and general forensic and cyber security readiness, which follow similar methods to achieve their respective aims. However, it is recommended that future research be conducted to fully explore and compare the number of papers submitted relating to digital forensics and information security respectively. Another possible cause could be the stagnation of developments in the field at that stage. This is likely to change with many recent developments that incorporate machine learning and artificial intelligence.

By year, the following most researched topics trends were observed; The small table of above shows that the top 3 trends for this period are digital forensic processes, image forensics, and cloud forensics.

5 Conclusions and Outlook to Future Work

We suggest that still more research is required to determine the digital forensics trends that are important for curriculum development for HEI. For this purpose we analysed a significant sample of publications that dealt with digital forensics trends. Practitioners' and academic interest in digital forensics continues, following the trends in cyber crime. While we cannot claim this paper to be exhaustive, it provides insights into digital forensics trends previously researched. This overview could be valuable to researchers and/or experts who are looking for further direction w.r.t. where to focus their teaching, learning, and publication efforts. This paper shall, in particular, contribute towards the design of curricula, as it points out areas of interest that might otherwise be overlooked, such as cloud forensics, digital image forensics, and investigation frameworks.

We pointed to a range of topics that have seen significant research already and are thus important for inclusion into forthcoming digital forensics-related HEI curricula. Based on our findings we can emphasise cloud forensics, mobile forensics, digital forensics processes, image forensics, and digital forensics tools for this purpose. Cloud and mobile forensics, as discussed above, tend to move away from traditional forensics techniques, processes, and methodologies. They are complemented by forensics processes and forensics tools which have had to evolve to accommodate this move away from traditional forensics methods. Image forensics remains relevant due to several factors: cameras being incorporated into mobile and smartphone devices, the rise of social media, the use of photography, and the increase in the use of technology to commit cyber crime by altering digital images.

With our data sample it was not yet possible to fully determine the scope of forthcoming digital forensics curricula in HEIs. However, our data sample was able to comprehensively determine where academia had concentrated its digital forensics research efforts. 49 distinct trends were identified. Future research should also address the trends highlighted via popular media, as the corporate world tends to advance and adopt technology at a faster rate than HEIs do.

There is also a need to determine why the number of papers published on digital forensics seems to be declining despite the ever-growing urgency for organizations to be able to conduct digital forensic investigations caused by the sharp increase in cyber crime. There would be value in determining whether other disciplines, e.g. information and cyber security, are incorporating aspects of digital forensics into their research agendas. Lastly, another area of forensics in need of active research is that of standardisation, not only w.r.t. investigative methodologies (see ISO 27043), but also and especially HEI curricula, as this fledgling discipline continues to grow and evolve in complexity as a result of the fast rate of technological change and the globally sharp rise in cyber crime.

References

1. Almulhem, A.: Network forensics: notions and challenges. In: Proceedings of IEEE ISSPIT International Symposium on Signal Processing and Information Technology, pp. 463–466 (2009)
2. Bagby, J.W.: The cyber forensic war room: an immersion into IT aspects of public policy. In: Carroll, J.M. (ed.) Innovative Practices in Teaching Information Sciences and Technology: Experience Reports and Reflections, pp. 117–132. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-03656-4_11
3. Bryhn, A.C., Dimberg, P.H.: An operational definition of a statistically meaningful trend. PLoS ONE **6**(4), e19241 (2011)
4. Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, Orlando (2011)
5. Endicott-Popovsky, B., Frinke, D.: Embedding forensic capabilities into networks: addressing inefficiencies in digital forensics investigations. In: Proceedings of IEEE Workshop on Information Assurance, pp. 133–139 (2006)
6. Farid, H.: Image forgery detection. IEEE Sign. Proc. Mag. **26**(2), 16–25 (2009)

7. Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., Stein, M.: Computer forensics programs in higher education: a preliminary study. ACM SIGCSE Bull. **37**(1), 147–151 (2005)
8. Kim, H.J., Lim, S., Kim, B., Jung, E.S.: A new approach to photography forensics using 3D analysis for correcting perception errors: a case study. In: Proceedings of ACM Workshop on Surreal Media and Virtual Cloning, pp. 27–30 (2010)
9. Lang, A., Bashir, M., Campbell, R., de Stefano, L.: Developing a new digital forensics curriculum. Digit. Investig. **11**, s76–s84 (2014)
10. Leung, W.S.: Cheap latex, high-end thrills: a fantasy exercise in search and seizure. In: Liebenberg, J., Gruner, S. (eds.) SACLA 2017. CCIS, vol. 730, pp. 265–277. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-69670-6_19
11. Marturana, F., Me, G., Berte, R., Tacconi, S.: A quantitative approach to triaging in mobile forensics. In: Proceedings of the IEEE TrustCom 10th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 582–588 (2011)
12. Olivier, M., Gruner, S.: On the scientific maturity of digital forensics research. In: Peterson, G., Shenoi, S. (eds.) DigitalForensics 2013. IAICT, vol. 410, pp. 33–49. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41148-9_3
13. Reith, M., Carr, C., Gunsch, G.: An examination of digital forensic models. Int. J. Digit. Evid. **1**(3), 1–12 (2002)
14. Stenvert, M., Brown, I.: Qualifications and skill levels of digital forensics practitioners in South Africa: an exploratory study. In: Kabanda, S., Suleman, H., Gruner, S. (eds.) SACLA 2018. CCIS, vol. 963, pp. 345–361. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-05813-5_23
15. Wu, D., Fulmer, J., Johnson, S.: Teaching information security with virtual laboratories. In: Carroll, J.M. (ed.) Innovative Practices in Teaching Information Sciences and Technology: Experience Reports and Reflections, pp. 179–192. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-03656-4_16
16. Zawoad, S., Hasan, R.: Cloud forensics: a meta-study of challenges, approaches, and open problems. Technical report, arXiv:1302.6312 (2013)