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

**Full Paper**

**SACLA 2019**

Roshan Harneker[1] and Adrie Stander[1[0000-0003-2468-6820]]

[1] University of Cape Town, Rondebosch, 7701, South Africa
Roshan.harneker@uct.ac.za

**Abstract.** The young science of digital forensics has made great strides in the last decade, but so too has cybercrime. The growing complexity of cybercrime 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 research was to determine how academic teaching and research can support the needs of industry when investigating cybercrime. The research initially explores digital forensics and its challenges before describing past academic research conducted around digital forensics ontologies and taxonomies. Current digital forensics higher education curricula are discussed thereafter, along with limited information relating to forensics trends observed via social media sources. This is followed by a research analysis of academic research trends for this discipline for the period 2007 to 2017. It ends by highlighting research trends for which more research is required, and which could possibly contribute towards shaping future teaching and learning for digital forensics and also suggests future research to be conducted.

**Keywords:** Digital Forensics, Cybercrime, Curriculum, Research Trends.

## 1 Introduction

The proliferation and accessibility of the Internet have indelibly changed our lives in many positive ways. It 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. In contrast, the Internet's accessibility has also given rise to a cybercrime explosion, and it is estimated that South Africa loses more than R5.8 billion annually to cybercrime (Symantec, 2016).

Digital forensics, regarded as a relatively young science, 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].

As a new discipline, there is a need for the creation of a digital forensics taxonomy to guide the academic teaching that occurs to ensure that industry expectations and academic offerings are aligned. As technological change occurs at a rapid rate, it stands to reason that a digital forensics taxonomy should be updated on a regular basis to ensure that academia keeps up with industry's needs. There is also a requirement to support overburdened law enforcement that needs to keep up with ever-changing technological trends and the way these are used to commit cybercrime.

The paper initially discusses the research objectives and research limitations before moving to a definition of digital forensics, Higher Education Institutional curricula and challenges. This is followed by the methodology used, the trend analysis, results and a summary conclusion.

## 2 Research Objectives

The research aims to determine digital forensics trends covering the period 2007 to 2017 by investigating digital forensics (DF) trends published in academic resources. It also aims to highlight the 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 make recommendations on trends requiring future or ongoing research, the trend analysis will also assist with showing specific knowledge areas and differentiating them from general knowledge areas.

## 3 Limitations

There is always a chance that the data may not match the research questions or that it will contain gaps.

Another limitation likely to be experienced is that many articles conflate information security with digital forensics. Many articles, therefore, had to be scrutinized for digital forensics content before deciding whether or not it could form part of the research data set.

## 4 Digital Forensics

Reith, Carr & Gunsch [2] discern 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 document and present evidence in digital form to be able to reconstruct incidents deemed to be of a criminal nature.

## 5 Higher Education Institutional Curricula and Challenges

Lang, Bashir, Campbell, and DeStefano [3] conducted research that highlighted some of the obstacles encountered when attempting to formulate a curriculum for digital forensics. 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. The researchers also highlight that the lack of a globally accepted curricula model can also contribute to institutions not adopting a forensics programme due to uncertainty and impedance to curriculum development.

Gottschalk, Liu, Dathan, Fitzgerald & Stein [4] highlighted further difficulties pertaining to digital forensics training which is reliant on an instructor's personal experience. This can prove to be problematic due to a shortage of qualified digital forensics practitioners and the result highlights how difficult it can be to find qualified academics to provide training in an HEI setting.

Lang et al. [3] also highlight digital forensics, as a discipline, straddles the areas of computer science and law. Knowledge from both these fields is, therefore, a requirement, however; students studying digital forensics are highly unlikely to be studying both disciplines resulting in a difficulty in deciding which prerequisites from each field students should have to meet and which concepts from each field should be included in the curriculum.

Lastly, the research highlighted that no generally accepted model for a digital Forensics curriculum exists, although there are proposed curriculum standards. It 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.

## 6 Methodology

The descriptive review is meant to reveal patterns in existing literature being analyzed during research and produces quantifiable data such as publication time, the research methodology used and the research outcomes. This type of review method is mostly using searching, filtering, and classification. This means that the research starts off conducting a thorough and extensive literature review for several relevant papers that pertain to the research area and each study is then treated as a single data record. This is followed by the research noting trends and patterns. The result is often 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, and for that reason it was opted to use a descriptive literature review to determine what new topics emerged in the field and also to get an indication of the relative importance of focus areas.

Academic data was collected using 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. The research opted for Mendeley's search function to avoid any bias which may arise from using specific databases such as ScienceDirect, EBSCOHost or ACM Portal to name but a few. Search results were then further narrowed to the last ten years only from 2007 to 2017. The single search term "digital forensics" was used. As the papers available via Mendeley are crowd-sourced and show the number of times an article has been read, the researchers believe that Mendeley provides a representative of well-read peer-reviewed quality papers that have already been selected by a large pool of independent researchers. The researchers added a further delimiter to the papers selected by only choosing ones read by at least five (5) readers.

Once enough peer-reviewed references were selected, the actual papers were then downloaded via the relevant databases, websites and other resources. The researchers collected two thousand two hundred (2200) articles and citations which were scanned manually for relevance by first reading the abstract and author keywords. In cases where the title, abstract and author keywords did not provide enough information, the full document text was read to determine its relevance to digital forensics.

During the second round of data analysis, the researchers scanned abstracts and read full texts if required, excluding papers that did not have Digital Forensics as a central theme but merely mention it along with other interest areas or give it general coverage. This allowed the exclusion of papers that could not be placed in a specific category. The papers which contained Digital Forensics related themes but could not be placed in a specific category were then placed in a "*general*" category.

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

## 7 Results

The researcher's data analysis of 2200 papers showed 49 distinct trends. The trends are summarised in a table below in the order of the number of papers analyzed.

**Table 1.** List of digital forensics trends 2007 – 2017.

| RANK | TREND | PAPERS | % |
|---|---|---|---|
| 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 |
| 8 | Network Forensics | 73 | 3.51 |
| 9 | Legal | 70 | 3.37 |
| 10 | Digital Forensics Framework | 66 | 3.18 |
| 11 | Education | 62 | 2.99 |
| 12 | Cybercrime | 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 |
| 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** | **100.00** |

The trend labeled "*General*" consisted of a range of papers that either did not fit any of the other categories or where the topic of the research paper being analyzed was fairly broad. "*General*" is thus not regarded as a trend in itself, but the papers listed under "*General*" are still DF-related. It is on this basis that the researchers consider the analysis to demonstrate forty-nine (49) trends, not fifty (50).

## 8 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 they shift in over a period. This is then represented graphically via a line or curve. Looking for consequential. relevant and significant trends is an important and prevalent undertaking in work of a scientific nature and the statistical noteworthiness of a linear trend plotted against a time series is regularly used to classify and quantify how useful an observed trend is [5].

### 8.1 Digital Forensics (DF) Process

The Digital Forensics process is recognised as a valid scientific and forensic method used to conduct Digital Forensics investigations and is defined as the steps taking from the time an alert of an incident is received right through to the formal reporting of final 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 [6].

This trend encompassed a range of processes and/or procedures that researchers have proposed for use for investigations that do not necessarily fit the mould of a traditional DF-related case. Notably, 2013 showed a peak in the number of papers being written about processes. The researchers found that 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 using Mendeley as a tool. The analysed papers discussed digital forensics case reconstruction, chain of custody processes, text string searching, how to conduct investigations, processes to use for embedded systems, hashing, data classification, insider threats and processes pertaining to log gathering and analysis. Some of the more interesting papers discussed the use of digital forensics for medical cases and artificial intelligence-based pattern matching. A variety of different process methodologies and models were also described and proposed with practical use cases.

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 a great deal of research interest. A total of 173 peer-reviewed papers were analysed, comprising 8.33% of the full data sample.

### 8.2 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 [7].

Zawoud and Hasan [8] explain that cloud forensics is often considered to be part of network forensics since cloud computing services require substantial network access and network forensics investigations are conducted on private and public networks and IP space. Cloud forensics though also includes the investigation of operating system processes, file systems, registry entries, and cache. Different forensics steps would be followed depending on which implementation model of cloud computing is involved. As an 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 the virtual machine image directly from customers making use of the cloud service, allowing a forensics practitioner to examine and analyse the images forensically.

Although cloud forensics is commonly thought of as a subset of network forensics, the research was significant enough to be considered a trend on its own. Cloud forensics came in second with 148 peer-reviewed research papers comprising 7.1% of the data sample. With the move away from physical infrastructure towards cost-saving cloud solutions, this topic will continue to garner interest and research but interestingly, research seems to wane after 2016 according to the data sample. The researcher believes this could be due to Digital Forensics being lumped more and more into information security spheres of research.

Since many cloud solutions are cross-jurisdictional there are also legal implications that affect where organisations and individuals store their data. Cloud is also a move away from traditional computing upon which traditional Digital Forensics methods are based. Cloud has become a ubiquitous part of life given that cloud features are built into most current smartphone and tablet mobile devices, showing that it is 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 since the hard drive isn’t physically present on the computing device used to access the cloud service and is often accessed via a web client. The existence and use of cloud computing and its associated services such as IaaS, SaaS, PaaS meant that new, forensically-sound methods needed to be developed to acquire and analyse cloud-based data especially bearing in mind the different ways in which the cloud offering will affect the ability of a forensic practitioner to obtain the data required, in a forensically sound manner.

## 8.3 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 photographs taken at and of crime scenes, for a court of law. Kim, Ling, Kim and Jung [9] explain that five (5) classification types of image forensics techniques exist. The five types are pixel-based, format-based, camera-based, physically-based and geometry-based. Farid [10] describes the techniques in more detail. Pixel-based techniques identify statistical deviations introduced at the pixel level and can analyse interconnections at the pixel level 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 lens, camera 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 that 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 2 decades ago. The plethora of papers that the researcher noted for image forensics, 141 in total, caused this trend to be the third most research trend in the data sample assessed. This constituted 6.79% of the total number of papers analysed. Most papers focused on forgery and image manipulation with several papers offering methodologies and algorithms to use to detect anomalies and variances from original images. The graph above shows the number of papers per year that contributed to the overall total with 2009 showing the greatest number of research papers and 2017 showing the least.

## 8.4 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 end up in a court of law and must thus bear up to legal scrutiny and satisfy legal requirements. It is noteworthy that 21 out of the 128 articles delved into the use of open source tools and their associated merits. Interest in this topic peaked in 2013, with 2017 yielding no papers. As mentioned previously, this does not mean that papers were not produced about DF tools in that year, just that they did not feature in the researcher’s sample. Other 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.

### 8.5 Mobile Forensics

This trend covered digital forensics conducted on mobile devices which included cell phones and tablets. According to Marturana, Me, Berte and Tacconi [11], the influx of smartphone devices on the consumer market resulted in a burgeoning demand for digital forensics that was not able to be met by traditional forensics investigative techniques. There were 117 papers making up 5.63% of the total data sample covering this trend which reached its peak in 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, Me, Berte and Tacconi [11] 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. This makes the case for this being in the top 5 researched digital forensics trends and the evolution of investigations from “live forensics” which consisted 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 bear up to legal scrutiny in a court of law.

### 8.6 General

This trend is the catch-all label used by the researchers to list all papers which remain uncategorized either due to the broadness of the topic discussed in the paper or due to too few other papers which contained similar content. The 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 constituted being general in nature.

### 8.7 Digital Evidence

Casey [6] 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. 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, and backups, and computer memory to name a few. This topic consisted of 75 papers of which 74 were peer-reviewed making up 3.56% of the total data sample with 1 paper was from popular media sources. The papers analysed for this trend 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 near consistent interest in this trend between 2009 to 2015, with far fewer papers being published from 2016 onwards.

### 8.8 Network Forensics

Network forensics, according to Almulhem [7], 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 constituting security attacks by dealing with the acquisition, recording, and analysis of network-related events for law enforcement purposes. A total of 73 papers were analysed for this trend with discussions including 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 papers were written in 2010, then in 2014. Fewer papers came out from 2016 onwards, perhaps due to the tie-in between this topic and network security which is a subset of information and cybersecurity. This topic, with seventy-three (73) papers, constituted 3.51% of the total number of papers analysed.

### 8.9 Legal

This trend refers to the legal aspects of digital forensics and as the 9th trend in the list, consists of 73 papers, 70 of which are peer-reviewed, 2 were duplicate articles and 1 was from a popular media source. This trend contributed 3.37% of the total data sample. The 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 cybercrime, digital forensics and legal systems across different countries, legal and technical issues affecting digital forensics and digital forensics testimony in courts of law. The graph above shows that interest in this research topic appears to peak in 2008 and then again in 2011 but declines from 2016 onwards. This is concerning especially since digital forensics is a process that exists primarily for a court of law.

### 8.10 Digital Forensics Frameworks

This very important topic 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 and since digital evidence can be found on literally almost any computing device, it follows that several frameworks exist to cater for the different technologies, hardware, and software. What remains a constant is that the methods used to extract and analyse data for a digital forensics' investigation must stand up under legal scrutiny. This trend accounts for 68 papers of which 66 were peer-reviewed, 1 was a duplicate and 1 was from a popular media source. The 66 papers constituted 3.18% of all peer-reviewed papers making up the total data sample. 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.

### 8.11 Education

This trend comprised 62 papers or 2.99% of the total data sample with 2010 being the year when most papers were produced. Discussion in the papers focussed on various education programmes and curricula in use in countries around the world, incorporating digital forensics understanding into law school programmes, creation of practical lab exercises for students studying forensics, case studies in teaching forensics, defining of an agenda for forensics education, assessment strategies for forensics training and education and teaching forensics in different operating system environments.

## 9 Data Analysis of Papers by Years

From a starting point in 2007 with 120 papers, the research 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 cybersecurity. Facets of forensics have been absorbed into information security such as incident response and general forensic and cybersecurity readiness, both of which follow similar methodologies to achieve their respective aims. However, it is recommended that future research is conducted to fully explore and compare the number of papers submitted relating to digital forensics and information security respectively.

Another possible cause can be the stagnation of developments in the field at that stage. This is likely to change with many recent developments incorporating machine learning and artificial intelligence.

By year, the following trends were observed with reference to the most researched topics:

**Table 2.** List of most researched trends by year.

| YEAR | 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 |

The research thus indicates that the top 3 trends for this period are digital forensic processes, image forensics, and cloud forensics.

## 10 Conclusion

It is proposed that more research is required to determine the digital forensics trends that are of importance. The researchers analysed a significant sample of published papers that dealt with digital forensics trends, taxonomy and ontology to examine past research already done and the importance ascribed to the specific focus areas previously identified as important.

Practitioner and academic interest in digital forensics remain relevant, following the trends in Cybercrime. While this paper cannot claim to be exhaustive, it provides insights into digital forensics trends previously researched. This research could prove to be quite valuable to researchers and/or digital forensics practitioners who are looking for more direction with reference to where to focus their teaching, learning, and knowledge sharing efforts. It can also contribute towards the design of curricula as it points out areas of interest that might often be overlooked such as cloud forensics, digital image forensics, and investigation frameworks.

The research pointed to a range of topics that have seen significant research conducted already and are still important for inclusion into existing digital forensics-related curricula. Based on the findings of this paper, the research highlights cloud forensics, mobile forensics, digital forensics processes, image forensics and digital forensics tools for future research. Cloud and mobile forensics, as discussed earlier, show a move away from traditional forensics techniques, processes, and methodologies and 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 a few factors; cameras being incorporated into mobile and smartphone devices, the rise of social media and the use of photography and the increase in the use of technology to commit cybercrime by altering digital images.

Using the data sample, it was not possible to fully determine the scope of digital forensics curricula in HEIs to provide a complete answer. Instead, the data sample was able to comprehensively determine where academia had concentrated its digital forensics research efforts. Fourty-nine (49) distinct trends were identified after which each paper was categorized according to one of the 49 trends.

Future research should address the trends highlighted via popular media as the corporate world does tend to advance and adopt technology at a faster rate than HEIs do.

There is also a requirement to determine why the academic interest in terms of research outputs of papers relating to digital forensics is on the decline despite the ever-growing urgency for organizations to be able to conduct digital forensic investigations caused by the sharp increase in cybercrime. There would be value in determining whether other disciplines e.g. information and cybersecurity, are incorporating aspects of digital forensics into its research agenda.

Lastly, another area of forensics that is in dire need of active research is that of standardisation, not only in terms of investigative methodologies, but also curricula, as this fledgling discipline continues to grow and evolve in complexity as a result of the fast rate of technological change and the sharp rise in cybercrime at a global level.

## References

1. Endicott-Popovsky, B., & Frincke, D. (2006). Embedding forensic capabilities into networks: addressing inefficiencies in digital forensics investigations. Workshop on Information Assurance: Computer Forensics. West Point, NY: United States: IEEE.
2. Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1-12.
3. Lang, A., Bashir, M., Campbell, R., & DeStefano, L. (2014). Developing a new digital forensics curriculum. Digital Investigation, 11, S76-S84
4. Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., & Stein, M. (2005). Computer forensics programs in higher education: a preliminary study. ACM SIGCSE Bulletin, 37(1), 147-151.
5. Bryhn, A. C., & Dimberg, P. H. (2011). An operational definition of a statistically meaningful trend. PLoS One, 6(4). Retrieved from http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0019241#, October 2018.
6. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press.
7. Almulhem, A. (2009, December). Network forensics: Notions and challenges. Signal Processing and Information Technology (ISSPIT), 2009 IEEE International Symposium on (pp. 463-466). IEEE.
8. Zawoad, S., & Hasan, R. (2013). Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. Retrieved from http://arxiv.org/abs/1302.6312, October 2018.
9. Kim, H. J., Lim, S., Kim, B., & Jung, E. S. (2010, October). A new approach to photography forensics using 3d analysis for correcting perception errors: a case study. Proceedings of the 2010 ACM workshop on surreal media and virtual cloning (pp. 27-30). ACM.
10. Farid, H. (2009). Image Forgery Detection. IEEE Signal Processing Magazine, 26(2), 16-25
11. Marturana, F., Me, G., Berte, R., & Tacconi, S. (2011, November). A quantitative approach to triaging in mobile forensics. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on (pp. 582-588). IEEE