# Success Factors and Challenges in Digital Forensics for Law Enforcement in Sweden

Milagros D. Cervantes Mori [1], Joakim Kävrestad [1], and Marcus Nohlberg [1]

[1] *University of Skövde, Högskolevägen 1, 541 28, Skövde, Sweden*

**Abstract**

The widespread use of communication and digital technology has affected the number of devices requiring analysis in criminal investigations. Additionally, the increase in storage volume, the diversity of digital devices, and the use of cloud environments introduce more complexities to the digital forensic domain. This work aims to supply a taxonomy of the main challenges and success factors faced in the digital forensic domain in law enforcement. The chosen method for this research is a systematic literature review of studies with topics related to success factors and challenges in digital forensics for law enforcement. The candidate studies were 1,428 peer-reviewed scientific articles published between 2015 and 2021. A total of twenty-eight primary studies were analyzed by applying thematic coding. Furthermore, a survey of digital forensic practitioners from the Swedish Police was held to triangulate the results achieved with the systematic literature review.

**Keywords**

Digital forensics, computer forensics, success factors, opportunities, challenges, issues, law enforcement

## 1. Introduction

The digital forensics domain is new in comparison to traditional forensics. [1] defines digital forensics as: "the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict custody for the data". As the world becomes more digitalized, digital evidence in criminal investigations increases. Digital evidence is data of evidentiary value gathered from digital devices during forensic examinations. In modern criminal investigations, digital evidence plays an essential role in many types of crimes ranging from true cyber crimes such as computer intrusions to traditional crimes where the criminals benefit from opportunities provided by the digitalized society [2]. This includes, for instance, drug trade, fraud, and child exploitation, where digital platforms are used for marketing, communication, and payments [3], [4]. Furthermore, digital evidence is a critical part of the fight against organized crime, where recovery of communication between criminals or using geolocation to position digital devices can be crucial for investigators [5].

The act of securing digital evidence from digital devices is typically performed by forensic examiners employed by law enforcement agencies. Being a relatively new discipline, digital forensics has been overseen in an ad-hoc manner but has received more attention in recent years [6]. A forensic examiner is required to apply great care to ensure that the evidence produced holds up to high legal standards [7]. In essence, a forensic examiner is supposed to provide unbiased results using transparent and robust methods that allow for external assessment. Further, the forensic examiner is expected to provide an investigation with important data, often in a timely manner [2].

Digital forensics has experienced progress in formalizing, standardizing, and formulating digital forensic processes and approaches. For instance, ISO/IEC 27037:2012 supplies guidelines for handling

7th International Workshop on Socio-Technical Perspective in IS development, October11-12, 2021 (STPIS'21)
EMAIL: mcervantesmori@hotmail.com (A. 1); Joakim.kavrestad@his.se (A. 2); marcus.nohlberg@his.se (A. 3)

digital evidence during specific activities such as identification, collection, acquisition, and preservation [8]. On the other hand, the NIST provides practical guidance on how to perform computer and network forensic activities from an IT perspective [1]. Moreover, the National Criminal Justice Reference Service (NCJRS) shares guidelines and information about digital forensic procedures and processes specifically applied to law enforcement [9], and the National Police Chiefs' Council has identified three core challenges that digital forensic science faces, and that need to be addressed [10]. Given the significant role that digital evidence plays in modern crimes, the importance of effective forensic practices that adhere to strict legal principles cannot be understated. For one, even individual users now often hold several digital devices, each with an increasing room for data storage, making the amount of data in a typical forensic examination challenging [11]. Further, data is often stored in different geographical locations, making many forensic examinations subject to different jurisdictions with added legal overhead [7]. Third, the increasing use of cloud applications means that forensic examinations must interact not only with different legal systems but also with different cloud providers [7]. In that sense, NISTIR 8006 categorizes and discusses the forensics challenges faced when responding to incidents in cloud-computing environment [12]. To support future forensic practices, we argue that there is a need to further understand the emergent challenges facing modern-day forensics. While digital forensics can easily be perceived as a technical practice, it is highly dependent on the environment where it is performed. This study perceives digital forensics as socio-technical and argues that its success depends not only on the examiners' ability to perform technically sound examinations. Examiners or prosecutors request those examinations, and the forensic examiners need to understand what the examination is expected to produce. Further, the forensic examiners will ultimately report their findings back to the investigation and subsequently a court. The members of the investigation and courtroom must be able to interpret the findings and assess their value correctly. As such, interdisciplinary communication is central to digital forensics, making it technical and social in nature. In fact, the forensic process often includes repeated communication between the forensic expert and the investigator [2]. In summary, digital forensics originates a social-technical process that can only be fully understood by looking at both technical and social aspects [13], [14].

This study seeks to identify challenges and success factors for digital forensics within law enforcement. A systematic literature review (SLR) which includes recently published research in this domain was applied. A survey was distributed among forensic examiners within the Swedish Police to validate and extend the results of the SLR. This study highlights challenges and success factors within digital forensics and can, as such, guide future research as an outline for important research directions. It can also serve as a reference for decision-makers seeking to strengthen digital forensic practices.

## 2. Method

Qualitative research can include multiple data collection methods, such as document studies, surveys, interviews, and observations [15]. This study combines two different techniques to explore the research questions, an SLR, and a practitioners' survey. The purpose of using these two methods is to rely on data from diverse sources to triangulate the findings [16]. It also allows us to compare findings from the research community with opinions gathered from practitioners. Both methods, as well as the reasons for choosing them, are explained in the following subsections.

### 2.1. Systematic Literature Review

An SLR is the most appropriate method to address the research questions because it allows us to:

- Understand and explain the current situation of digital forensics in law enforcement.
- Acknowledge the success factors and challenges faced in digital forensics in law enforcement.
- Identify digital forensic challenges that deserve more attention.

The method followed in this SLR is based on the guidelines provided by [17] (3-phase method) and [18] (9 steps), which are represented in Figure 1.

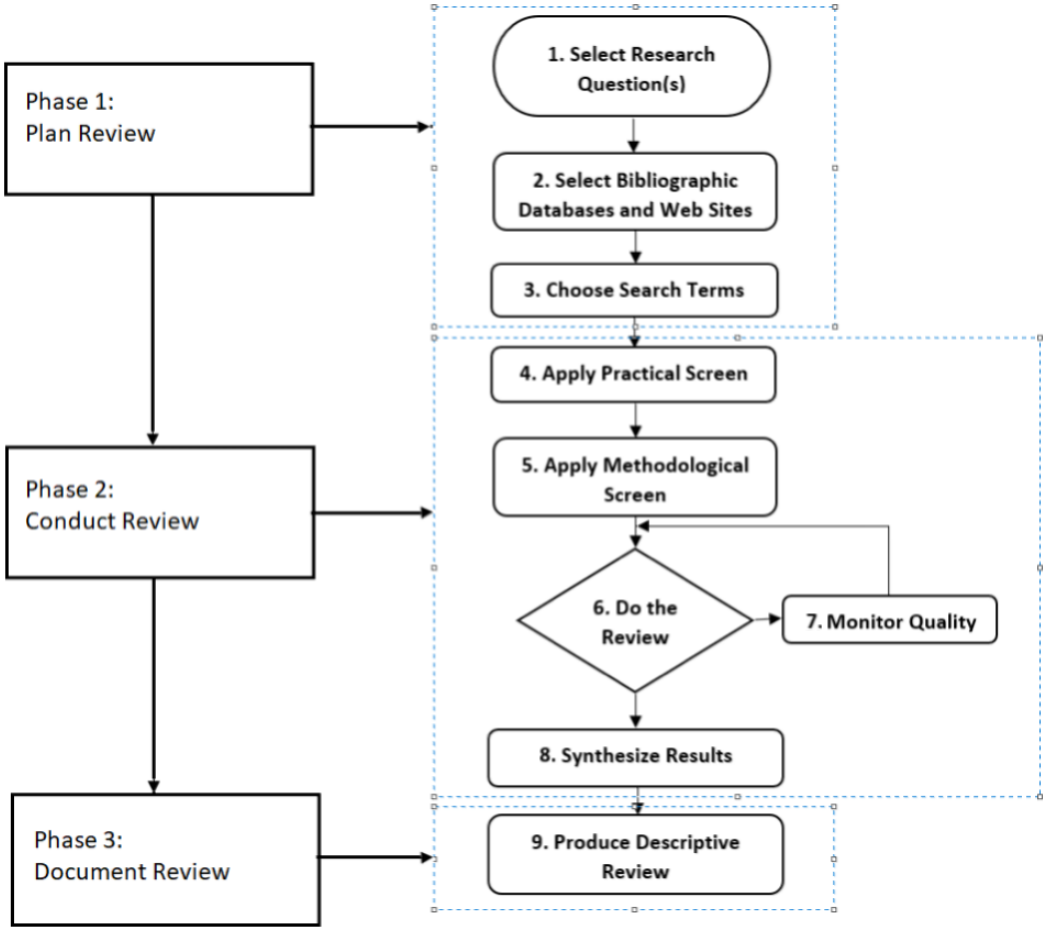


**Figure 1**: SLR Methodology Applied in this Study (based on [17] and [18])

The process is described in the following sections.

## 2.1.1. Bibliographic Database

The choice of the bibliographic databases was based on the recommendations from previous work like [19] who identify IEEE Xplore and Science Direct as relevant electronic sources, [17] recommend Scopus due to its extensive database of abstracts and citations, and [18] who states that Web of Science is a multidisciplinary database that indexes relevant journals across disciplines. Additionally, Taylor & Francis was also included as one of the bibliographic sources, because the authors found a high number of relevant publications related to digital forensics in law enforcement during an exploratory pilot search. The five bibliographic databases chosen as sources for this SLR are summarized in Table 1.

**Table 1**
Nominated Databases

| Source | URL |
|---|---|
| IEEE Xplore | https://www.ieeexplore.ieee.org |
| ScienceDirect | https://www.sciencedirect.com |
| Web of Science | https://www.webofknowledge.com |
| Scopus | https://www.scopus.com |
| Taylor & Francis | https://www.tandfonline.com |

To define the scope of this work and focus on recent studies, one inclusion criterion is to include studies published between the years 2015 to 2021. Other criteria are to include only peer-reviewed conference

papers and journal articles in published English. The risk of getting duplicate studies is also considered and addressed as part of the exclusion criteria. The inclusion and exclusion criteria defined for this work are summarized in Table 2.

**Table 2**
Inclusion and Exclusion Criteria

| Inclusion Criteria | Type |
|---|---|
| Studies that discuss success factors or challenges of digital forensics in law enforcement | Content |
| Published from 2015 to 2021 | Publication date |
| Conference papers and journal articles | Research design |
| Peer-reviewed | Content |
| English | Publication language |
| **Exclusion Criteria** | **Type** |
| Do not fulfill all the inclusion criteria | Content, publication, design |
| Duplicates (appear in more than one database) | Content |
| Cannot be accessed (require additional login) | Publication access |

### 2.1.2. Study Selection

A practical selection of studies based on the application of the inclusion and exclusion criteria and a methodological selection to identify the most relevant studies was made following five steps:

1. Apply the search query to each one of the chosen bibliographic databases
2. Store and organize the candidate studies using a reference management software
3. Apply a first scanning to exclude studies based on titles and keywords
4. Apply another scanning to exclude duplicate studies
5. Apply a third scanning to exclude studies based on their content

To complement the selection of primary studies, backward searching suggested by [20] was also used. The backward searching started with the compilation of references from the already selected primary studies. The previously defined inclusion and exclusion criteria were applied to the candidate studies from the backward searching. The final group of primary studies is composed of the studies found during the study selection process and the studies found from backward searching.

## 2.2. Thematic Analysis

The primary studies are analyzed using thematic coding. According to [21], this is a flexible method to evaluate qualitative data. The process starts with the repeated reading of the primary studies and continues with looking for patterns related to success factors and challenges in digital forensics. During this stage, it is necessary to take notes that can later be used for coding. Once a general knowledge about the content of the data is achieved, the next step is to assign initial codes that are going to aid in the definition of themes.

The coding themes are classified into two groups, one for success factors and the other for challenges. Depending on the preliminary results, subcategories can also be defined. Once the themes are defined, the extracts corresponding to the themes must be revised to verify coherence, and if required, redefine the themes and re-code as well. An assessment for each theme is conducted. To ease the understanding of the analysis, the content of the themes needs to be described, and themes with similarities can be grouped.

Once the analysis from the primary studies is completed, the findings are to be used in the survey design. The findings from the SLR and the survey are planned to be integrated to achieve confirmation and completeness. For confirmation purposes, the findings from the SLR are going to be counterbalanced with the ones from the survey. While for completeness purposes, the survey is going to add an in-depth understanding of the topic.

## 2.3. Qualitative Data Collection

In this case, a survey was used as qualitative data collection method and to extend the scope of the research [14]. The survey was formulated based on the findings from the SLR, and targeting the digital forensic practitioners belonging to the Swedish Police.

The survey allowed the authors to validate the outcome from the SLR by identifying challenges and success factors that were perceived as most important by the community of practitioners. The data collection was done by using a questionnaire with multiple-choice and open-ended questions. Some questions gathered basic information about the respondents (role and years of experience in the domain), while other questions were based on a predefined list of success factors constructed with the outcomes from the SLR. In the multiple-choice question, the respondents had to select the three most relevant success factors from a list. In the open-ended question, the respondents could point out other success factors that they considered relevant but were not specified in the list. A similar approach was followed with the questions that gathered information about the challenges in the domain.

To avoid potential problems concerning the reliability and validity of the responses, the recommendation from [27] to use local languages in written and verbal communication was followed, and the survey originality created in English was translated to Swedish. The questionnaire included brief instructions to answer the questions and a description of the purpose of the survey. The survey was delivered to the potential respondents in an electronic format via a Google Form link.

The aim of the survey was to gather information that could reinforce and improve the outcomes from the SLR by supplying new insights based on the opinions of the practitioners. However, the authors acknowledge the limited generalizability of the findings [14].

### 2.3.1. Target Group

The target group was composed of about two hundred digital forensic practitioners belonging to the Swedish Police. The participation in the survey was voluntary and anonymous, and at the time of this writing, sixteen respondents completed the questionary.

## 3. Results and Analysis

This section summarizes the results and analysis from both the SLR and the survey.

## 3.1. Systematic Literature Review

The SLR followed the steps and recommendations provided by [12] and [13]. The following subsections describe in detail the process and generated results.

### 3.1.1. Search Process

The search process was based on the application of a search query into electronic databases. This process was executed by applying an automated search to conferences proceedings and journal papers from 2015 to 2021. Since different electronic sources supply different functionalities, minor adjustments to the base search query are needed. When possible, advanced searches are used.

The base search query, including Boolean operators and wildcards, is as follows:
*(digital OR computer) AND forensic* AND law AND (success OR progress OR opportunit* OR improvement*) AND (challenge* OR problem* OR issue* OR failure*)*

### 3.1.2. Study Selection Process

The automated search query was applied to all the selected databases on February 23rd, 2021 and supplied a total of 1,428 candidate studies. After a first scanning based on titles and keywords, full copies of 71 remaining studies were obtained and organized. After a second scanning based on the inclusion and exclusion criteria, the number of selected candidate studies was narrowed to 60. After reading the content from the 60 studies, 22 studies were chosen as primary ones. The details corresponding to this part of the process are presented in Table 3.

**Table 3**
Selection of Studies using Automated Search

| Source | Candidate Studies | Selection Based on: | | |
|---|---|---|---|---|
| | | Title/Keywords | Incl./Excl. Criteria | Content |
| IEEE Xplore | 25 | 4 | 3 | 2 |
| ScienceDirect | 170 | 20 | 20 | 6 |
| Web of Science | 29 | 10 | 3 | 0 |
| Scopus | 44 | 10 | 7 | 4 |
| Taylor | 11,60 | 27 | 27 | 10 |
| **Total** | **1,428** | **71** | **60** | **22** |

The backward searching applied to the preliminary group of 22 primary studies supplied 1,137 more candidate studies. After a first scanning based on titles and keywords, 30 studies were considered relevant to the topic, and full copies were obtained. After a second scanning based on the inclusion and exclusion criteria, 18 studies were chosen for the next step. After reading the contents of those studies, six studies remained as primary ones. The results corresponding to steps 5 to 8 are summarized in Table 4.

**Table 4**
Selection of Studies using Backward Searching

| Source | Candidate Studies | Selection Based on: | | |
|---|---|---|---|---|
| | | Title/Keywords | Incl./Excl. Criteria | Content |
| Backward searching | 1,137 | 30 | 18 | 6 |

The primary studies were stored and organized using the reference management software Zotero. A unique identifier (from A1 to A28) was assigned to each primary study to ease the analysis and discussion of the results. The studies were organized in alphabetic order based on the authors' last names to distribute these identifications. The type of studies is represented by 'J' for journal article and 'C' for conference paper. The list of the twenty-eight primary studies is presented in Table 5.

**Table 5**
List of Primary Studies

| Id | Author(s) and Year | Title | Type |
|---|---|---|---|
| A1 | Amann, P., & James, J. I. (2015) | Designing robustness and resilience in digital investigation laboratories | J |
| A2 | Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018) | Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence | J |
| A3 | Casey, E. (2019) | The chequered past and risky future of digital forensics | J |
| A4 | Christou, G. (2018) | The challenges of cybercrime governance in the European Union | J |

| Id | Author(s) and Year | Title | Type |
|---|---|---|---|
| A5 | Dlamini, S., & Mbambo, C. (2019) | Understanding policing of cybe-rcrime [sic] in South Africa: The phenomena, challenges and effective responses | J |
| A6 | Du, X., Le-Khac, N.-A., & Scanlon, M. (2017) | Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service | C |
| A7 | Harichandran, V. S., Breitinger, F., Baggili, I., & Marrington, A. (2016) | A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later | J |
| A8 | Harkin, D., Whelan, C., & Chang, L. (2018) | The challenges facing specialist police cyber-crime units: An empirical analysis | J |
| A9 | Henseler, H., & van Loenhout, S. (2018) | Educating judges, prosecutors and lawyers in the use of digital forensic experts | J |
| A10 | Jordaan, J., & Bradshaw, K. (2015) | The current state of digital forensic practitioners in South Africa. | C |
| A11 | Kanta, A., Coisel, I., & Scanlon, M. (2020) | A survey exploring open source Intelligence for smarter password cracking | J |
| A12 | Karie, N. M., & Venter, H. S. (2015) | Taxonomy of Challenges for Digital Forensics | J |
| A13 | Kebande, V. R., & Ray, I. (2016) | A Generic Digital Forensic Investigation Framework for Internet of Things (IoT) | C |
| A14 | Kebande, V. R., & Venter, H. S. (2018) | On digital forensic readiness in the cloud using a distributed agent-based solution: Issues and challenges | J |
| A15 | Lanier, M. M., & Cooper, A. T. (2016) | From papyrus to cyber: How technology has directed law enforcement policy and practice | J |
| A16 | Lillis, D., Becker, B. A., O'Sullivan, T., & Scanlon, M. (2016) | CURRENT CHALLENGES AND FUTURE RESEARCH AREAS FOR DIGITAL FORENSIC INVESTIGATION | C |
| A17 | Luciano, L., Baggili, I., Topor, M., Casey, P., & Breitinger, F. (2018) | Digital Forensics in the Next Five Years | C |
| A18 | Montasari, R., & Hill, R. (2019) | Next-Generation Digital Forensics: Challenges and Future Paradigms | C |
| A19 | Morgan, R., & Benson, S. (2018) | Australasian Forensic Science Summit 2016: Future technology and research towards 2030 | J |
| A20 | Morgan, R. M., & Levin, E. A. (2019) | A crisis for the future of forensic science: Lessons from the UK of the importance of epistemology for funding research and development | J |
| A21 | Omeleze, S., & Venter, H. S. (2019) | Digital forensic application requirements specification process | J |
| A22 | Page, H., Horsman, G., Sarna, A., & Foster, J. (2019) | A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn? | J |
| A23 | Rappert, B., Wheat, H., & Wilson-Kovacs, D. (2021) | Rationing bytes: Managing demand for digital forensic examinations | J |
| A24 | Reedy, P. (2020) | Interpol review of digital evidence 2016—2019 | J |
| A25 | Sunde, N., & Dror, I. E. (2019) | Cognitive and human factors in digital forensics: Problems, challenges, and the way forward | J |
| A26 | van Beek, H. M. A., van den Bos, J., Boztas, A., van Eijk, E. J., Schramp, R., & Ugen, M. (2020) | Digital forensics as a service: Stepping up the game | J |
| A27 | Vincze, E. A. (2016) | Challenges in digital forensics | J |

| Id | Author(s) and Year | Title | Type |
|---|---|---|---|
| A28 | Waziri, I., & Sitarz, R. (2015) | Cyber forensics: The need for an official governing body | C |

## 3.2. Thematic Coding

The primary studies were subjected to a thematic analysis following the procedure presented by [21]. The studies were read several times, and information relevant to the aim of the study was found and extracted. Those extracts were later classified based on the answers provided to the research questions. Qualitative codes were assigned, and similar codes were grouped to form themes. This process was followed to identify both the success factors and the challenges in separate stages.

Once the preliminary list of success factors was ready, the next step was to evaluate which codes should be kept and which could be merged or regrouped. It is important to mention that the list of success factors is not intended to be an exhaustive list, but a reflection of the success factors considered by the authors of the primary studies. Moreover, since the list of success factors did not happen to be as extensive as the one for challenges, it was not needed to consider categories to classify the success factors.

About the challenges, the content of the selected primary studies shows that the challenges in digital forensics are a major concern in the research community, which is reflected not only in the greater number of studies focused on challenges, but the extension of the discussion dedicated to them. Twenty studies out of twenty-eight focused on challenges as their main topic and included a limited discussion about success factors. Six studies out of twenty-eight discussed challenges alone, and two studies only presented success factors.

Moreover, the extensive list of challenges compiled from the analysis required a classification into categories. Only five studies (A11, A12, A14, A18, and A27) out of the twenty-six that focused on challenges supplied some type of categorization. Those categorizations were used as a baseline to formulate seven categories that are used to present the analysis of the challenges. These seven categories are not intended to be exhaustive and could be extended or updated. Besides, due to the nature of certain challenges, it can be possible to classify some of them into more than one category. In that case, and to avoid duplication of information, such a challenge is placed only into one category that suits it better. Additionally, some challenges that turned out not to be straightforward to categorize were located into the category 'other challenges'.

The themes mapped into success factors and challenges in digital forensics for law enforcement are presented in the following sections.

### 3.2.1. Finding 1: Success Factors in Digital Forensics for Law Enforcement

From the analysis of the primary studies, twelve success factors were identified. Some of the primary studies discuss more than one success factor. The twelve success factors and some references to specific studies are as follows:

1. 'Cooperation and knowledge exchange' is acknowledged as a success factor, particularly in the form of active national workshops to "reassess the community's accomplishment towards improving state of the art in the field" (A17, pp. 12). Another example was the educational experience of university students from Norway and the USA who co-created and analyzed digital forensic data (A24).
   However, several studies also agree that more needs to be done in terms of cooperation.
2. 'Digital Forensic as a Service (DFaaS) supporting investigations' is considered beneficial due to the possibility of saving costs and freeing up forensic and law enforcement personal to focus on their caseload (A6).
3. 'Cloud systems dealing with a large volume of evidence' through distributed parallelization represent a success factor in the field (A6, pp. 7).
4. 'Best practices applied to domain' is a key factor. Some examples to highlight are the Best Practice Manual (BPM) prepared by the European Network of Forensic Science Institutes (ENFSI) in 2015

and the active role of both the Scientific Working Group on Digital Evidence (SWGDE) and the NIST (A9).

5. 'Novel solutions supporting the domain in storing, exchanging, and facilitating access to information and tools are already assisting law enforcement agencies' (A11).
6. 'Digital information used as digital evidence' supports investigators in tracking transactions, messages, and diverse digital media (A2).
7. 'Triage process saving time for practitioners' is also considered beneficial for the specialists who attend crime scenes (A24).
8. 'Training opportunities for law enforcement officers' are supported by organizations like the National White Collar Crime Center (NW3C) offering training at no cost, and the Consortium of Digital Forensic Specialists dedicated to improving digital forensics as a profession (A27).
9. 'Professional satisfaction working in the domain' is highlighted from the results of research applied in a case study in Australia (A8).
10. 'Criteria of competence for digital forensic practitioners' have been developed in both international standard bodies and digital forensics standards bodies (A10).
11. 'IoT-connected devices as digital evidence' supply many benefits to digital forensics, however, privacy challenges are acknowledged (A18).
12. 'Government initiatives to support the domain', like the one promoted by the United Kingdom's Minister for Policing and Fire services appealing for a collaborative review of the quality and sustainability of forensic science service provision (A24).

The success factors and the primary studies that cover them are summarized in Table 6. Minor adjustments to the description of some success factors have been made to improve the visual presentation of the results.

**Table 6**

Success Factors by Studies

| | Topic | Studies |
|---|---|---|
| 1 | Cooperation and knowledge exchange | A1, A3, A4, A9, A17, A19, A24, A25, A26 |
| 2 | DFaaS supporting investigations | A2, A6, A16, A18, A23, A26 |
| 3 | Cloud systems dealing with large volume of evidence | A6, A11, A12, A14 |
| 4 | Best practices applied to the domain | A1, A6, A9, A16 |
| 5 | Novel solutions supporting the domain | A2, A6, A11, A15 |
| 6 | Digital information used as digital evidence | A2, A15 |
| 7 | Triage process saving time from specialists | A23, A24 |
| 8 | Training opportunities for law enforcement officers | A24, A27 |
| 9 | Professional satisfaction working in the domain | A8 |
| 10 | Criteria of competence for practitioners | A10 |
| 11 | IoT devices as digital evidence | A18 |
| 12 | Government initiatives to support the domain | A24 |
| | **Total number of studies** | **22** |

Figure 2 illustrates the success factors and the corresponding primary studies in a linear dendrogram. The size of the spheres standing for each success factor is proportional to the number of studies dedicated to it.

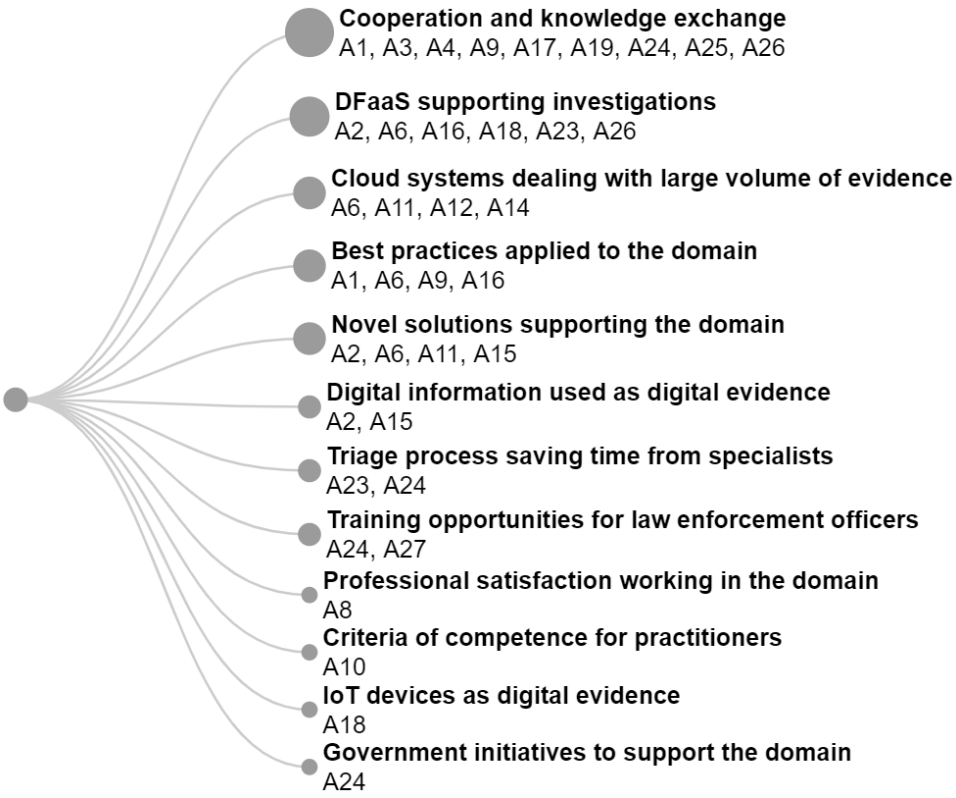


**Figure 2**: Representation of the Success Factors (authors' own)

## 3.2.2. Finding 2: Success Factors in Digital Forensics for Law Enforcement

From the analysis of the primary studies, seven categories of challenges were identified as follows:

A. Resource-related challenges: This category considers the assets the organizations require for their normal operations, including the personnel as a key asset.
B. Technical challenges: This includes the challenges caused by new devices, software, tools, protocols, or any technological solution. Technical challenges have a broad coverage due to the growing number of seized devices, increasing data storage, and the complexity of environments like cloud systems (A11, A14).
C. Organizational challenges: Those challenges are related to institutions, their internal structure, their management, and their interaction with others.
D. Legal challenges: Related to issues that are originated in the legal system, court of law, prosecutions, and the admissibility of digital evidence (A11).
E. Operational challenges: Challenges faced by the organizations while executing their duties, especially in incident detection, response, and prevention (A12, A27).
F. Human-related challenges: Challenges specifically targeting the human factor. They include issues related to unintentional outcomes like errors or biases introduced into the digital forensic process due to human iteration (A22, A25).
G. Other challenges: This category holds challenges not included in previous categories.

The challenges classified into the seven categories and the primary studies that cover them are presented in Table 7. Some primary studies discuss more than one challenge. Minor adjustments to the description of some challenges have been made to improve the visual presentation of the results.

**Table 7**
Challenges by Studies

| | Topic | Studies |
|---|---|---|
| **A** | **Resource-related challenges** | |

| | Topic | Studies |
|---|---|---|
| 1 | Lack of formal training/continuous education | A1, A7, A10, A11, A12, A17, A19, A22, A23, A24, A25, A27 |
| 2 | Insufficient qualified staff | A1, A4, A7, A8, A10, A11, A12, A23, 27 |
| 3 | Lack of funding | A1, A7, A8, A15, A17, A20, A27 |
| 4 | Inefficient knowledge management | A1, A2, A3, A12, A19, A24 |
| 5 | Absence of accreditation/regulation of the profession | A10, A17, A22, A27, A28 |
| 6 | Limited access to latest technology | A11, A12, A15, A23 |
| 7 | Limited information sharing | A4, A17 |
| 8 | Unavailability of datasets for testing | A17, A24 |
| 9 | Talent drain | A1 |
| **B** | **Technical challenges** | |
| 1 | Complexity of cloud computing | A2, A6, A7, A11, A12, A14, A16, A17, A18, A24, A27 |
| 2 | Heterogeneity of tools, methods, and data sources | A2, A7, A10, A12, A16, A17, A18, A23, A24, A27 |
| 3 | Use of encryption | A2, A7, A11, A12, A14, A17, A18, A27 |
| 4 | Elevated use of IoT devices | A2, A6, A11, A13, A16, A17, A18, A24 |
| 5 | Complexity in volume and distribution of evidence | A3, A6, A12, A16, A17, A18, A23, A27 |
| 6 | Availability of anti-forensic techniques | A2, A12, A16, A18, A24 |
| 7 | Lack of validation of tools | A17, A20, A21 |
| 8 | Need for improvement of open-source tools | A7, A27 |
| 9 | Unrestrained use of drones | A15, A24 |
| 10 | Use of cryptocurrency | A24 |
| **C** | **Organizational challenges** | |
| 1 | Lack of standardization/best practices | A1, A2, A12, A13, A14 |
| 2 | Insufficient quality management | A3, A10, A22, A23, A24 |
| 3 | Inconsistent cooperation | A4, A5 |
| 4 | Lack of awareness in cyber-crimes | A5, A15 |
| 5 | Lack of collaboration | A17, A18 |
| 6 | Incongruences between organizations and policies | A17 |
| **D** | **Legal challenges** | |
| 1 | Different jurisdictions | A1, A3, A4, A11, A12, A14, A16, A18, A24 |
| 2 | Difficulties in attribution of crimes | A1, A3, A4, A14, A18, A24, A27 |
| 3 | Invasion of privacy | A2, A3, A7, A17, A27, A28 |
| 4 | Complexity of legal processes and systems | A2, A12, A24, A28 |
| 5 | Inadmissibility of digital evidence | A11, A12 |
| **E** | **Operational challenges** | |
| 1 | Demanding workload/backlog | A8, A18, A23, A27 |
| 2 | Inappropriate evidence management | A1, A4, A12 |
| 3 | Unsuitable chain of custody | A1, A18, A23 |
| 4 | Difficulties in data acquisition | A12, A16, A27 |
| 5 | Lack of scientific validation | A2, A24 |
| 6 | Insufficient timeframes for analysis | A19, A24 |
| 7 | Issues in seizure of digital evidence | A23, A27 |
| 8 | Irreproducibility of examinations | A21, A24 |
| 9 | Use of different terminology | A24 |
| **F** | **Human-related challenges** | |
| 1 | Human errors and biases | A3, A22, A24, A25, A28 |
| 2 | Interpretative errors | A3, A24 |

| | Topic | Studies |
|---|---|---|
| 3 | Deficiencies in explicability | A3 |
| 4 | Issues understanding digital examinations | A23 |
| **G** | **Other challenges** | |
| 1 | Renewed trends in crime | A1, A12, A15, A16, A23, |
| 2 | Lack of trust in the digital forensic process | A2 |
| 1 | Renewed trends in crime | A1, A12, A15, A16, A23 |
| | **Total number of studies** | **26** |

The challenges and their classification into categories are illustrated in a linear dendrogram in Figure 3. Following each challenge, there is a number in parenthesis that corresponds to the number of primary studies dedicated to that challenge. The size of the spheres representing the challenges is proportional to the number of studies.

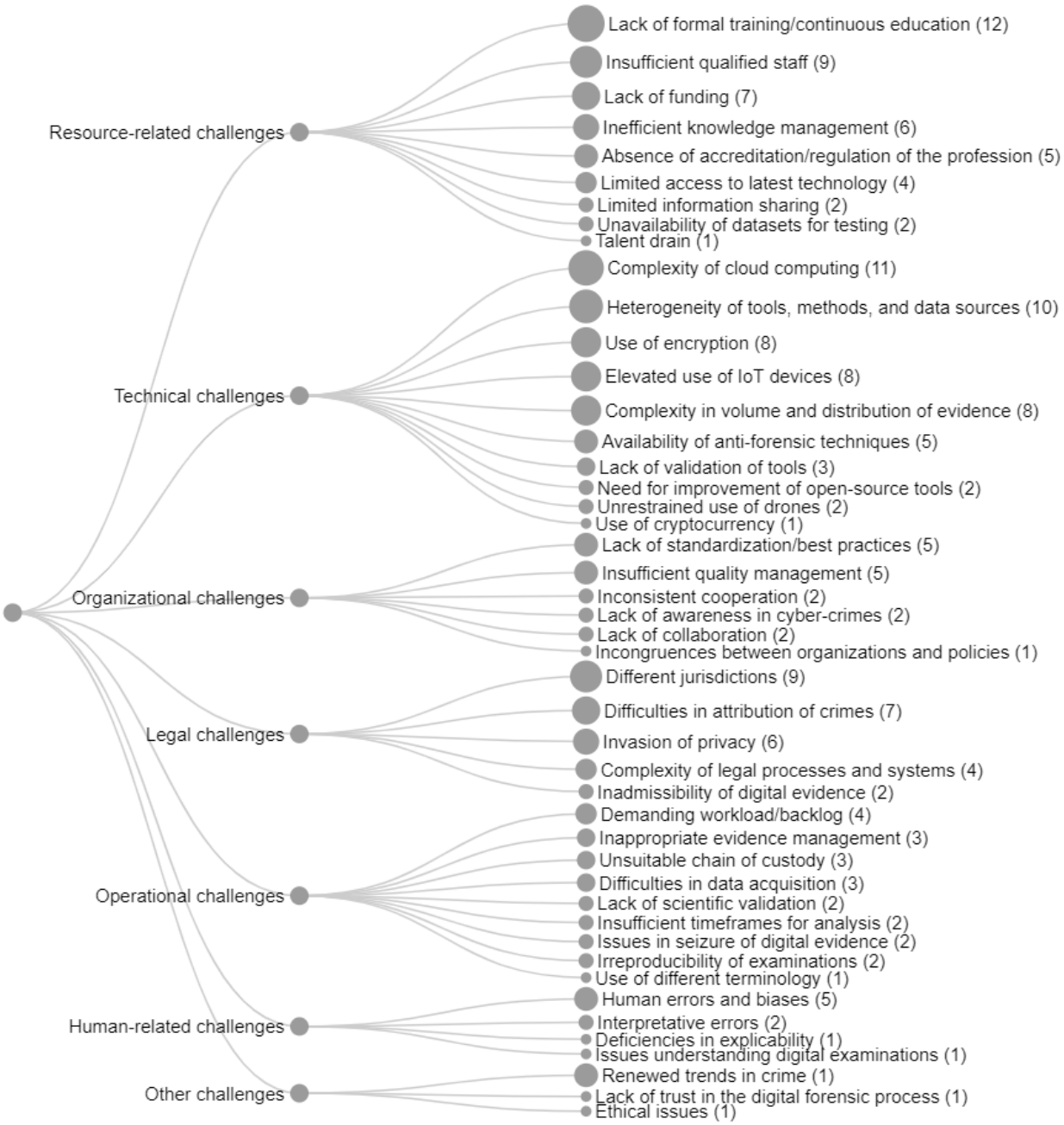


**Figure 3**: Representation of the Challenges (authors' own)

## 3.3. Survey

The survey was designed based on the findings from the SLR. The questions used in the survey were translated to Swedish and distributed to the population of digital forensic practitioners from the Swedish Police (about two hundred potential respondents) via a Google Form link on May 17th 2021. Their participation in the survey was voluntary and anonymous. Besides, there were no questions that could be used to find out the identity of the respondents. Only sixteen respondents completed the survey. The number of respondents was not representative, and the results from the survey cannot be generalized to the digital forensic practitioners from the Swedish Police. However, these results are considered to be useful and provide some insights from the respondents.

To report the results from the open questions, a pseudonym was assigned to the respondents based on the order they completed the survey, from Respondent 1 to Respondent 16. The analysis of the results is as follows:

i. Concerning success factors in digital forensics for law enforcement, a list of success factors identified during the SLR was provided to the respondents. They were asked to choose the three most relevant. The success factors chosen by the respondents are as follows:
   - 'Novel solutions supporting the domain' → chosen by 11 respondents
   - 'Cooperation and knowledge exchange' → chosen by 9 respondents.
   - 'Professional satisfaction working in the domain' → chosen by 9 respondents.

   Each of the remaining success factors was chosen by one to seven respondents, which means that the respondents neglected none of the success factors listed in the survey.

   Moreover, some respondents supplied some success factors that they considered were not included in the list, for example:
   - Respondent 5: *"Good dialog with investigators and prosecutors. Legal support to access the cloud*."
   - Respondent 12: *"Humility between digital forensic practitioners should be encouraged. One should be able to ask any question."*
   - Respondent 16: *"Legislation in Sweden and international cooperation."*

ii. Concerning challenges in digital forensics for law enforcement, a list of challenges found during the SLR was provided to the respondents. They were asked to choose the three most relevant. The challenges chosen by the respondents are as follows:
   - 'Legal barriers imposed on criminal investigations' → chosen by 11 respondents.
   - 'Limited access to the latest technology (software and hardware)' → chosen by eight respondents.
   - 'Demanding workload/backload (too much to do)' → chosen by seven respondents.

   Four challenges that were not considered relevant for any of the respondents were: 'heterogeneity of tools,' 'lack of standardization/best practices,' 'ethical issues,' and 'renewed trends in crime.'

   When asked about challenges that were not necessarily in the list but were considered relevant, the respondents' opinions were as follows:
   - Respondent 2: *"Political barriers, politicians get involved in things they do not understand."*
   - Respondent 3: *"Psychological distress due to the exposure to sensitive material."*

   The opinion from Respondent 3 is supported by [24] in their research about techniques to reduce the exposure of digital forensic investigators to child sexual abuse material.
   - Respondent 5: *"A big challenge is that there is not enough staff. Many investigations are affected because of that."*

   This argument corresponds to the challenge identified as 'insufficient qualified staff,' considered in the category resource-related challenges, and supported by nine primary studies: A1, A4, A7, A8, A10, A11, A12, A23, and A27 (see Table 7).
   - Respondent 16: *"Financial resources to be able to employ the right qualified staff."*

   In general terms, the challenge identified by Respondent 16 is already considered in the challenge' lack of funding', included in the category resource-related challenges; and discussed in seven primary studies: A1, A7, A8, A15, A17, A20, and A27 (see Table 7).

iii. Concerning other comments about success factors and challenges, two respondents showed concern about training and education as follows:

- Respondent 5: *"Training in legislation for digital forensic practitioners is missing. It would be faster and better to investigate if we have a better knowledge about legislation..."*
  The opinion from Respondent 5 is reflected in the challenge identified as 'lack of formal training/continuous education' included in the category resource-related challenges, and supported by twelve primary studies (Table 7); especially A17 that emphasizes the lack of multidisciplinary approaches in educational programs.
- Respondent 12: *"The approach on how to get knowledge must be extended. There is so much free [training] available that is not considered due to a conservative perspective…"*
  The opinion from Responder 12 is reinforced by the studies A24 and A27, which consider as success factor the 'training opportunities for law enforcement officers' (Table 6).

## 4. Discussion

The rapid progress in technology has changed how people interact, communicate, work, and deal with data; crime is not exempt from taking advantage of technological innovations. Criminals are early adopters of technology and have managed to integrate it into their illegal activities. Additionally, criminals have redesigned crime into cyber-aided and cybercrimes. On the other hand, digital sources' diversity, quantity, and complexity make it difficult for digital forensic practitioners to find digital evidence relevant to criminal investigations. Digital forensics is facing a wide variety of challenges. Researchers tend to focus their attention on challenges tackled by specific digital forensic disciplines like IoT forensics, cloud forensics, and multimedia forensics. Apart from the attention those disciplines deserve, a taxonomy of challenges in the field can facilitate addressing solutions where it is more required and suitable and orient future work aiming to improve the digital forensic domain.

This work aimed to identify success factors and challenges in digital forensic for law enforcement based on available and published scientific literature. One criterion for the selection of primary studies was to include publications from the last seven years. This timeframe is appropriate, considering the dynamic technological environment that surrounds the field. The initial plan for this study was to do an SLR and interviews with digital forensic practitioners from the Swedish Police. Interviews with practitioners could certainly supply an in-depth perspective on the topic. However, due to time constraints and certain limitations caused by the social distancing required to combat the pandemic, the interviews were replaced by a survey distributed via the Internet.

Concerning the validity of the research methods, the SLR was done following guidelines and recommendations from recognized academics, which are scientifically verified and widely applied by the research community. The steps followed during the execution of the SLR have been explained and documented with enough details to facilitate the reproducibility of the process. To minimize the potential impact of search bias, a combination of search terms based on keywords from the research questions was arranged and the search for primary studies was also complemented with a backward search. Additionally, to avoid database bias, an extensive number of candidate studies was gathered from six different electronic databases. On the other hand, the survey targeting the digital forensic practitioners from the Swedish Police was used as a qualitative data collection method. Even though the number of respondents to the survey was limited, the information gathered from the answers is a qualitative dataset that adds value to the research by providing some insights from the point of view of the respondents who are experts in digital forensics applied to law enforcement. Finally, there are no ethical issues that arise from conflicts of interest.

## 5. Conclusions

The thematic analysis applied to the primary studies has provided valuable information to identify the success factors and challenges of digital forensics in law enforcement. Practitioners and researchers acknowledge the success factors in the field. However, the main focus of the research community is oriented to deal with the challenges in the domain with less emphasis on success factors or opportunities, which is evident in both the number of studies and the extension of the discussion dedicated to challenges in comparison to success factors.

About the aim of this work, and to the best of our knowledge, no similar studies are dedicated to identifying success factors of digital forensics for law enforcement. However, some efforts to supply

classifications of challenges in digital forensics have been made by [25], [26], and [27]. These studies are valuable and were used as a baseline to elaborate the taxonomy of challenges in digital forensics for law enforcement presented in this work. Moreover, the contribution of this work is to have addressed both topics' success factors and challenges.

Regarding the results, the research community tends to focus mostly on two categories of challenges: technical and resource-related, with less recurrence in legal, operational, organizational, and human-related challenges (in that order). This situation puts in evidence the need for more research in organizational and human-related challenges. Additionally, researchers and practitioners agree that laws and legal procedures to combat crime do not evolve fast enough, and there is room for more research in this area as well. Two technical areas that seem to capture recurrent attention from researchers are the cloud environment and the IoT devices and the specific challenges that these technologies represent for the digital forensic domain.

Moreover, the results of this work also reveal that challenges identified almost twenty years ago by [28] and related to education/training and certification, data acquisition, tools, the legal justice system, and lack of funding are still prevalent in the digital forensic domain.

On the other hand, the opinions of the sixteen digital forensic practitioners from the Swedish Police who answered the survey are considered valuable because they are based on their work experience in the domain. Besides, the outcomes of the survey confirm the findings from the SLR and put in evidence gaps between what the research community considers relevant to investigate and the needs perceived by digital forensic practitioners. Moreover, both researchers and practitioners also agree on the need for improvements in communication, collaboration, and best practices in the domain, among other issues.

**Ethical, Societal, and Scientific Impacts**

Concerning the SLR, this work does not cause any negative ethical impact in terms of privacy and confidentiality because the analysis is based on publicly available studies that can be accessed by whoever is interested in the topic of digital forensics in law enforcement. Moreover, no personal, sensitive, neither confidential information about the authors of the primary studies is exposed. On the other hand, the survey to digital forensic practitioners grants anonymity to the responders; and does not disclose any critical or sensitive information that could be misused.

This work is expected to contribute with a positive societal impact in terms of providing reliable knowledge about the state of the art of digital forensics for law enforcement, specifically related to the success factor and challenges. Besides, within the framework of the agreement between the University of Skövde and the Forensic Department of the Swedish Police from Västra Götaland to do research applied to the forensic methodology, the results of this work are planned to be shared with representatives from the Swedish Police, extending the target readers outside of the academic community.

This work relies on the scientific evidence from the primary studies that answered the research questions proposed in this research. The review process was performed following a scientific method that ensures transparency and reproducibility of the results. On the other hand, even though the sample reached with the survey is not statistically representative, the answers reflect the point of view of sixteen digital forensic practitioners. Finally, the scientific impact of this work relies on the possibility to guide future research by pointing out the challenging areas that are more relevant for the practitioners (respondents to the survey).

**Future Work**

More work needs to be done in the identification of success factors and opportunities in the domain. About the challenges, the outcomes from the survey reflect the need to consider the practitioners' opinions when addressing research in the area.

An area that deserves more attention and investigation is human-related challenges. For instance, the psychological distress digital forensics can experience after continuous exposure to illicit content (like child sexual abuse) is a topic that has not captured enough attention from the researchers. This topic is particularly important because it can be addressed from different perspectives, which may require multidisciplinary approaches.

## 6. Acknowledgments

The authors want to thank the regional cybercrime center in the police region west of the Swedish Police for their cooperation with valuable discussions and assistance in forwarding the survey.

## 7. References

[1] National Institute of Standards and Technology (2006). *Guide to integrating forensic techniques into incident response* (NIST SP 800-86; 0 ed., p. NIST SP 800-86). https://doi.org/10.6028/NIST.SP.800-86.

[2] Kävrestad, J., Fundamentals of Digital Forensics: Theory, methods, and real-life applications, 2nd ed., Springer International Publishing, 2020. DOI:10.1007/978-3-030-38954-3.

[3] Duxbury, S. W., & Haynie, D. L., Building them up, breaking them down: Topology, vendor selection patterns, and a digital drug market's robustness to disruption, Social Networks, 52 (2018), pp. 238-250. DOI:10.1016/j.socnet.2017.09.002.

[4] Seigfried-Spellar, K. C., Assessing the psychological well-being and coping mechanisms of law enforcement investigators vs. digital forensic examiners of child pornography investigations, Journal of Police and Criminal Psychology, 33(3) (2018), pp. 215-226. DOI:10.1007/s11896-017-9248-7.

[5] Murray, D., Trouble on line for criminals using encrypted phones, Australasian Policing, 13(1) (2021), pp. 10-11. ISSN: 1837-7009.

[6] Sunde, N., & Dror, I. E., Cognitive and human factors in digital forensics: Problems, challenges, and the way forward, Digital investigation, 29 (2019), pp. 101-108. DOI:10.1016/j.diin.2019.03.011.

[7] Losavio, M. M., Pastukov, P., Polyakova, S., Zhang, X., Chow, K. P., Koltay, A., James, J., & Ortiz, M. E., The juridical spheres for digital forensics and electronic evidence in the insecure electronic world, Wiley Interdisciplinary Reviews Forensic Science, (2019), e1337. DOI:10.1002/wfs2.1337.

[8] International Organization for Standardization (2012). *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence* (ISO/IEC Standard No. 27037:2012). Retrieved January 6, 2021 from https://www.iso.org/standard/44381.html.

[9] National Criminal Justice Reference Service (NCJRS) (2021). *About NCJRS*. [Online]. Retrieved June 5, 2021 from https://www.ojp.gov/ncjrs.

[10] National Police Chiefs' Council (2020). *Digital Forensic Science Strategy*. Retrieved September 26, 2021 from https://www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf.

[11] Caviglione, L., Wendzel, S., & Mazurczyk, W., The future of digital forensics: Challenges and the road ahead, IEEE Security & Privacy, 15(6) (2017), pp. 12-17. DOI:10.1109/MSP.2017.4251117.

[12] National Institute of Standards and Technology (2020). *NISTIR 8006 NIST Cloud Computing Forensic Science Challenges*. Retrieved September 26, 2021 from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf.

[13] Leitch, S., & Warren, M. J., ETHICS: The past, present and future of socio-technical systems design, in: Proceedings of the IFIP International Conference on the History of Computing, Brisbane, Australia, September 2010, pp. 189-197. Springer, Berlin, Heidelberg.

[14] Nouh, M., Nurse, J. R., Webb, H., & Goldsmith, M., Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement, in: Proceedings of the Workshop on Usable Security (USEC), San Diego, CA, 24 February 2019, pp. 1-11. DOI:10.14722/usec.2019.23032.

[15] Creswell, J., & Poth, C., Qualitative inquiry and research design: choosing among five approaches, 4th ed., Sage Publications, 2018. ISBN 978-1-5063-3020-4.

[16] Arksey, H. & Knight, P., Interviewing for social scientists, an introductory resource with examples, Sage Publications, 1999. ISBN 0 76 1 9 5869.

[17] Kitchenham, B., & Charters, S., Guidelines for performing systematic literature reviews in software engineering, EBSE Technical Report EBSE-2007-01 (2007). http://cdn.elsevier.com/promis_misc/525444systematicreviewsguide.pdf.

[18] Fink, A., Conducting research literature reviews, from the Internet to paper, 5th ed., Sage Publications, 2019. ISBN 978-1-4833-0103-7.

[19] Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M., Lessons from applying the systematic literature review process within the software engineering domain, Journal of Systems and Software, 80(4) (2007), pp. 571-583. DOI:10.1016/j.jss.2006.07.009.

[20] Wohlin, C., Guidelines for snowballing in systematic literature studies and a replication in software engineering, in: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering - EASE '14, London, 13-14 May 2014, pp. 1-10. DOI:10.1145/2601248.2601268.
[21] Braun, V. & Clarke, V., Using thematic analysis in psychology, Qualitative Research in Psychology, 3:2 (2006), pp. 77-101. DOI:10.1191/1478088706qp063oa.
[22] Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A., Experimentation in software engineering. Springer, 2012. ISBN 978-3-642-29044-2.
[23] Bujra J., Lost in Translation? The Use of Interpreters in the Fieldwork, in: Desai, V., & Potter, R. B. (Eds.), Doing development research, Sage Publications, 2006. ISBN10 1 4129 02843.
[24] Sanchez, L., Grajeda, C., Baggili, I., & Hall, C., A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM), Digital Investigation, 29 (2019), pp. 124-142. DOI:10.1016/j.diin.2019.04.005.
[25] Kanta, A., Coisel, I., & Scanlon, M., A survey exploring open source Intelligence for smarter password cracking, Forensic Science International: Digital Investigation, 35 (2020), pp. 1-11. DOI:10.1016/j.fsidi.2020.301075.
[26] Karie, N. M., & Venter, H. S., Taxonomy of Challenges for Digital Forensics, Journal of Forensic Sciences, 60(4) (2015), pp. 885-893. DOI:10.1111/1556-4029.12809.
[27] Reedy, P., Interpol review of digital evidence 2016-2019, Forensic Science International: Synergy, 2 (2020), pp. 489-520. DOI:10.1016/j.fsisyn.2020.01.015.
[28] Rogers, M. K., & Seigfried, K., The future of computer forensics: A needs analysis survey, Computers & Security, 23(1) (2004), pp. 12-16. DOI:10.1016/j.cose.2004.01.003.