What do incident response practitioners need to know? A skillmap for the years ahead

Radek Hranický[a,*], Frank Breitinger[b,**], Ondřej Ryšavý[a], John Sheppard[c], Florin Schaedler[b], Holger Morgenstern[d], Simon Malik[d]

[a] *Faculty of Information Technology, Brno University of Technology, Brno, Czech Republic*
[b] *Hilti Chair for Data and Application Security, Institute of Information Systems, University of Liechtenstein, Liechtenstein*
[c] *Waterford Institute of Technology, Waterford, Ireland*
[d] *Albstadt-Sigmaringen University, Sigmaringen, Germany*

Abstract

Digital forensics incident response (DFIR) specialists are expected to possess multidisciplinary skills including expert knowledge of computer-related principles and technology. On the other hand, recent studies suggest that existing training and study programs may not fully address the needs of future DFIR professionals. To reveal possible gaps in practitioners education and identify the most needed skills, we built a skillmap for DFIR where we followed a threefold approach: (1) an online survey among DFIR experts; (2) a review of training programs; and (3) an analysis of job listings on LinkedIn. Each source was first analyzed on its own and the findings were merged into a DFIR skillmap which is the main contribution of this article. The results show that network forensics and incident handling are the most demanded domains of skills. While these are covered by existing courses the newly desired skills, in particular, cloud forensics and encrypted data, need to get more space in training and education. We hope that this article provides educators with information on ways to improve in the years ahead.

Keywords: Digital Forensics, Incident Response, Skills, Skillmap, Survey, DFIR

1. Introduction

Cybersecurity incidents such as breaches are omnipresent, and they will likely continue to be in the future as it will be hard, or impossible, to avoid them completely. Dealing with the occurrence of an incident requires a "systematic approach taken by an organization to prepare for, detect, contain, and recover from a suspected cybersecurity breach" (CrowdStrike (2019); definition of *incident response*). The ability to react to cyberattacks led to the development of numerous Computer Security Incident Response Teams (CSIRT) worldwide. These groups operate on an organizational, national, or international level to minimize damage from security incidents and provide an adequate response and recovery (Ruefle et al., 2014).

Both law enforcement and the corporate sector continue to report a growing need for cybersecurity experts, particularly digital forensic professionals. Multiple surveys revealed that the lack of adequate knowledge and skills are the most significant issues (Stambaugh, 2000; Henry et al., 2013; Ruefle et al., 2014; Vincze, 2016; Harichandran et al., 2016) (more details in Related work). Other studies from the European Union Agency for Cybersecurity (ENISA) also confirm these concerns and summarize reasons for the worldwide cybersecurity skills shortage (Vishik & Heisel, 2015; Zan & di Franco, 2020): One of the principal issues identified is the limited offering of cybersecurity courses in computing curricula, poor alignment between these offerings and labor market needs, and insufficient focus on practical exercises.

While these studies did not particularly focus on Digital Forensics Incident Response (DFIR) and the skills required in this domain, we argue that the situation is similar, if not worse. DFIR requires immense multidisciplinary knowledge and intensive hands-on training, which is not adequately addressed in all the current academic curricula. Generally speaking, skills expected from DFIR professionals include expert knowledge of computer-related principles and technology, thoroughness, understanding of the law and criminal investigation, and communication skills. Among them, technology-focused skills may be the most volatile given the fast pace of development. Taking into account the breadth of possible topics, this paper addresses the following questions:

Q1 Which skills are essential (required) for DFIR specialists?
Q2 Are all skills equally important or can they be ranked?

Furthermore, this paper looks into education aspects. In detail, we also address the following two questions:

Q3 How do experts gain their experience/knowledge (educate themselves)?
Q4 Does the job market require certain degrees / training / certifications?

*Corresponding author.
**New affiliation: School of Criminal Justice, University of Lausanne
Email addresses: ihranicky@fit.vutbr.cz (Radek Hranický), frank.breitinger@unil.ch (Frank Breitinger), rysavy@fit.vut.cz (Ondřej Ryšavý), jsheppard@wit.ie (John Sheppard), florin.schaedler@uni.li (Florin Schaedler), morgenstern@hs-albsig.de (Holger Morgenstern), maliks@hs-albsig.de (Simon Malik)
URL: https://www.FBreitinger.de (Frank Breitinger)

To answer these questions, we follow a threefold approach: First, a survey among selected DFIR experts was conducted with a total of 15 questions where most were open-ended to not limit answers; second, training programs, such as those offered by SANS, were reviewed to grasp the focus of existing programs; and third, an analysis of job listings on LinkedIn to identify current market needs was completed. Using these three sources and following a systematic approach, this paper contributes (1) answers to the previously raised questions Q1-Q4 and (2) a *skillmap* for DFIR. This skillmap provides a baseline for creating and improving training courses to educate digital forensic practitioners.

Note, while doubtless soft skills are highly relevant for DFIR personnel, this study primarily focuses on technical skills as soft skills are relevant for almost all (technical) domains and could result in its own study and go beyond the constraints of this article.

Definition of skill. For this work, we define a skill as the ability to solve a specific task. Gaining skills requires specialized training, experience, and/or education. Skills can be of different complexity (e.g., performing carving vs. Windows forensics). Note that the focus of this article is on technical skills, where skill is the capability to perform practical tasks in digital forensic and incident response based on an individual's knowledge, capacity, and competence (we are not saying that technical skills are more important than soft skills). We recognize that technical skills are often expressed as expected knowledge of specific technical areas at different depths of expertise. This work presents skills in a tree-like structure to reflect the relationship between general skills and specialized ones.

Structure of the paper. The paper is organized as follows: The next section summarizes related work. Sec. 3 to 5 present the approach and results of skills gathering from a survey among practitioners, course analysis, and job listing review, respectively. The skillmap is highlighted in Sec. 6. The last two sections outline the Limitations of this study followed by a Discussion and conclusion.

2. Related work

In the following, we briefly discuss other surveys stressing the importance of Training and education, Standards and guidelines and lastly Forensics needs and skills.

Training and education. Several surveys and studies have been published over the past two decades with respect to stressing the importance of education, training, and certifications. One of the first was conducted in 1998 when the US National Institute of Justice (NIJ) funded a systematic 1-year study to map state and local law enforcement agencies' needs for fighting cybercrime. The top 10 identified requisites included uniform training and certification courses, cooperation with the high-tech industry, and the possession and knowledge of up-to-date investigative and forensic tools (Stambaugh, 2000). A few years later, Rogers & Seigfried (2004) conducted an online single-question survey asking "the respondents to list what they considered to be the top five issues related to computer forensics". They gathered a total of 60 responses from researchers and practitioners in both the private and public sectors. Rogers & Seigfried grouped the answers into ten high order categories. The number one identified issue was the lack of education, training, or certification. Other frequently reported obstacles were technology, encryption, difficulties with data acquisition, and deficient tools. These older studies coincide with more recent studies, e.g., from 2015 (Forensic Focus, 2016) and 2018 (Forensic Focus, 2018), where the lack of training or standards was identified. Vincze (2016) adds that with the rapid change in forensic practices, ongoing education and training are necessary. Vincze also points out the growing demand for digital forensics and incident response experts. For instance, the US government reported a 74% jump in cybersecurity job postings from 2007 to 2013. This has also previously been stressed by Garfinkel (2010) who said that "training is a serious problem facing organizations that deliver forensic services. As a result, many organizations report that it typically takes between one and two years of on-the-job training before a newly minted forensics examiner is proficient enough to lead an investigation." While training and education seem problematic, a study on threat hunting from SANS (Lee & Lee, 2018) concludes that trained staff is the key.

Standards and guidelines. The early years of digital forensics were mainly about the investigator's intuition and the "trial and error" method. There were no globally accepted standards describing the procedures or provide an idea of the expert's level of competency (Garfinkel, 2010; Vincze, 2016). The absence of formal processes and training led institutions around the world to take steps towards standardization. In the US, the Scientific Working Group on Digital Evidence (SWGDE) started to publish various guidelines and best practices for computer forensics[1]. In 2005, ISO published the General Requirements for the Competence of Testing and Calibration Laboratories ISO/IEC 17025. This international standard unifies the commonly-used terms and describes technical and management requirements for laboratories (STN, 2005). Vincze (2016) agrees with the need to establish universally accepted standards.

Forensics needs and skills. A first article addressing skills was published by Werlinger et al. (2010). However, they are kept very general, e.g., tacit knowledge, pattern recognition, collaboration, and simulation. In a survey from Harichandran et al. (2016) with 99 participants, mostly from North America and Europe, 31% called for improvements in education and training. As the top three skills needed for the future, the respondents identified investigative skills, proficient use of forensic tools, and reverse engineering. Based on the answers, mobile and cloud forensics could have better tools and technology available. As the most crucial challenges needing research, the participants identified encryption, malware, and trail

[1] https://www.swgde.org/documents/published (last accessed 2021-02-22).

obfuscation. The importance of challenging encryption and cloud systems strongly correlates with the challenges identified by the participants of the surveys from Forensic Focus (2016, 2018). To identify the direction of digital forensics in the next five years, Luciano et al. (2018) analyzed qualitative and quantitative data from twenty-four cyber forensics expert panel members at the 2017's National Workshop of Redefining Cyber Forensics (NWRCF). The methodology used a pre-workshop survey, data collection during the workshop, and a post-workshop survey. The biggest anticipated challenges were encryption, keeping up with technological change, and lack of standards for best practices. As the most important areas of further research, the participants identified IoT, cloud infrastructure, and distributed storage. Based on their opinions, the most important job-ready relevant skills are communication skills, thinking out of the box, and understanding legal and ethical issues.

Summary. While many organizations and researchers have stressed the importance of education and training for years, there still seems to be a level of disparity between industry needs and education possibilities/offerings. Although there is consensus that standards and guidelines are needed, a unified skillmap for DFIR skills has not yet been discussed/presented by the community. However, some more recent studies such as Luciano et al. (2018) have started to look more closely at skills and concluded that technical as well as soft skills are essential for digital forensics and its subdomains.

3. Survey of DFIR practitioners

To develop the skillmap, a major focus was getting expert opinions which were gathered through an online survey.

3.1. Methodology

The survey consisted of fifteen questions (SQ1-SQ15) sent to a group of 40 practitioners. The survey asked for some demographics about the participants and then allowed respondents to provide their own opinion/thoughts. In detail, the following questions were included (OE=open ended, MC=multiple choice).

1. How many years of experience do you have in DFIR? [MC]
2. What is your role/job title? [OE]
3. What is the size of your team? [MC]
4. How large is your organization (employee number)? [MC]
5. What is your organization's primary sector? [MC]
6. Do you find it difficult to retain the members of your team? [MC]
7. How did you get your experience/knowledge (e.g., which study programs, certificate programs, training, events) and how do you stay up to date (e.g., blog, video channel, forums, best practice documents, external consultancy, training such as SANS)? [OE]
8. Which 5 skills are the most essential on a daily basis from (1) a technical perspective and (2) a knowledge perspective? [OE]
9. Which skills are you looking to acquire in the future? (Please rank if possible) [OE]
10. What tools and technologies do you primarily use? [OE]
11. Can you name the most useful tool you have? [OE]
12. If you had to design a DFIR course (e.g., 1-2 weeks) with 5 modules, what would you name these 5 modules? [OE]
13. What are the primary challenges you face? [MC]
14. What is the scope of your DFIR team? [MC]
15. Do you have a formal DFIR procedure and is it part of a company security policy? [Y/N]

3.2. Findings

In total, we received 32 answers. This first paragraph briefly summarizes the demographics [SQ1-5]. The survey was answered by candidates across a wide range of industries, with varying sizes of organizations. In detail, the interviewees had differing levels of experience with 6% having less than two years of experience, 28% between two and five, 38% had six to ten years, and 28% with over ten years of experience. The industries with the highest representation were Government at 25%, while forensics/security consulting and High-Tech accounted for 16% of responses. Other industries included Engineering/Construction, Financial, Health Care, Law Enforcement, Logistics, Manufacturing, and Retail. With respect to organization size, 72% employ more than 500 people and a further 19% between 100 and 500 employees. The size of the teams was broadly distributed across the organizations, with 28% being on a team of 1-5, 31% on a team of 6-10, 9% on a team of 11-15, and 31% on a team of more than 15.

Education. An important aspect of this survey was to understand how experts gained their experience/knowledge [SQ7]. Figure 1 presents a count of the number of respondents using each education source. Half of the survey population commented on their academic qualifications. In some instances, participants listed more than one, but only the highest level attained was included in our results. For instances where an individual held more than one qualification at a particular level, such as an MSc qualification, those qualifications were only counted as one instance. Based on this, half of the respondents held an academic qualification specific to cybersecurity or digital forensics, 16% at the undergraduate level, 25% at the MSc level, and 9% at the Ph.D. level. Vendor-neutral training programs such as summer schools or those offered by groups such as SANS were utilized by 53% of respondents, while 19% used vendor-specific training. A further 19% made use of discussions with their colleagues and in-house training. Interestingly, the *most important form of education was self-learning at 63%* conducted through formally peer-reviewed sources such as conference and journal publications and informal sources such as blogs, videos, and personal research. Learning on the job was useful to 22%. Capture the flag exercises and community interaction were both highlighted to be useful by 16% of participants.

In terms of the structure of a course on incident response modules [SQ12], the responders listed: Basics 44%, Network Forensics 28%, Disk Forensics 25%, Operating System (OS) Forensics 25%, Memory Forensics 25% and Incident Investigation Case study/exercises 22% as the most important topics to be covered. Less popular modules included monitoring

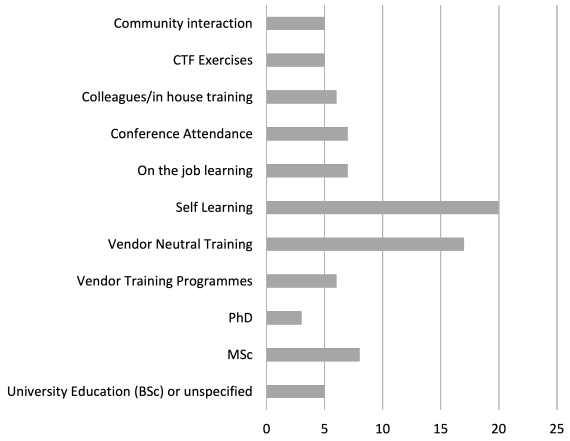

Figure 1: Sources of Education and Training.

and detection, incident response tools and processes, and legal, all at 19%, while malware was suggested by 16% of participants. Modules on evidence acquisition, timelines, mobile devices, and containment, eradication, and restoration were lower in priority at 6%. Modules titled internet forensics, user activity, penetration testing, cryptocurrency, and open-source intelligence were highlighted in just 3% of answers.

Skills. The most important non-technical skills [SQ8] identified were communication skills (written/oral/verbal) 31%, critical thinking 13%, and attention to detail 13%. The essential technical skills were knowledge of software and scripting, along with OS and Applications (Knowledge of and Analysis), both requested by 44% of respondents. Networks skills were identified as important by 40%, while knowledge of, and the ability to use general forensics tools was deemed important to 21%. Knowledge of Attacks and Security issues was important to 19%.

When asked about skills they consider acquiring in the future [SQ9], the areas of Cloud, Artificial Intelligence (AI)/Machine Learning, Penetration Testing, and Offensive Security were most frequently mentioned with 9% each. The next most desired skills participants wished to improve related to Software and Scripting, OS and Applications (Knowledge of and Analysis), Networks, IoT, Knowledge of Attacks and Security issues, and Cryptography. The growth in areas such as cloud and AI has been accepted and documented in the literature. Acquisition and analysis of cloud data pose many ongoing and changing challenges to investigators (Lillis et al., 2016), while AI technologies provide investigators with many opportunities in different areas of digital forensics (Du et al., 2020). In terms of soft skills, management skills in the area of teams and risk were identified by 9% of participants. Communication skills were also highlighted by one respondent. The need for management skills is consistent with the changing role of incident responders as they progress through their careers. There is a wide range of tools [SQ10] in use throughout the community. The most popular of these are highlighted in Figure 2 which presents a count of the number of respondents using each tool. In total, 99 different tools were identified, with Autopsy the most common tool used by 19% of participants, while EnCase, Linux, and self-built tools being the second most popular with 16% of users. Another question looked at the most useful tool [SQ11] that people have where both Splunk and Wireshark were named by 9% of respondents in each instance.

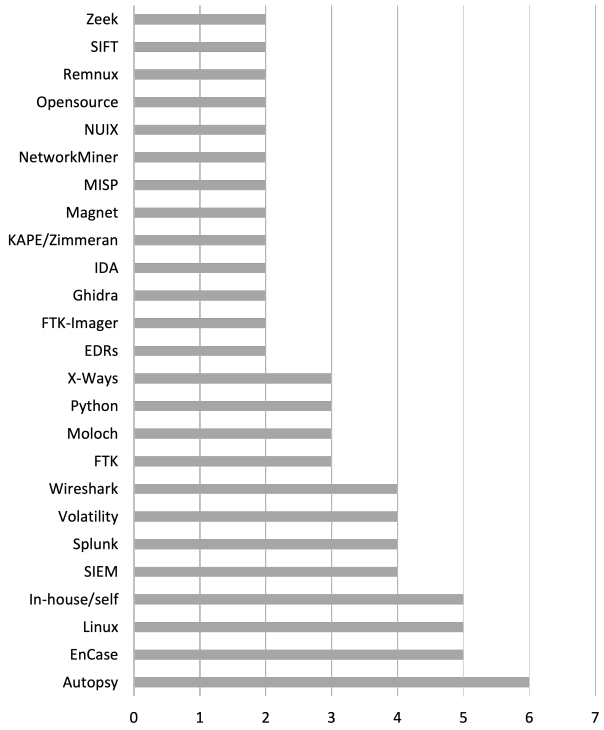

Figure 2: Most Commonly Identified Tools.

Miscellaneous. The duties associated with incident response (IR) teams [SQ14] allowed respondents to choose between the categories: detection of incidents, immediate incident response, incident analysis, collecting evidence for further investigation, analysis after breaches, recovering deleted data, security awareness training, improving security measures and vulnerability advisory internally in the organization. The main duties of most teams are incident detection, response, evidence collection and analysis. Many teams are also involved in other tasks such as internal vulnerability advisory, security awareness and improving security measures. The lowest occurring role was the recovery of deleted data by just 28% of participants. Almost two-thirds of respondents confirmed the existence of a formal IR procedure [SQ15] within their organization, while 25% confirmed that no official procedure existed.

Survey participants were asked about the primary challenges they face in an investigation [SQ13] where the following difficulties were listed: big data problem, [2], encrypted data, cloud computing, lack of adequate tools, insufficient resources, legislation, and others.

The three biggest issues identified were encrypted data at 29%, insufficient resourcing at 22%, and cloud computing at

[2]Big data is frequently used in digital forensics describing the problem of large amounts of data, e.g., by Zawoad & Hasan (2015).

21%. The big data problem was ranked fourth by 12% of respondents. Other challenges included legislation issues at 10% and a lack of adequate tools at 5%. The challenge of retaining team members [SQ6] was found to be a problem for 22% while somewhat difficult for 50% of participants.

4. Analysis of selected DFIR courses

Compared to other disciplines, digital forensics in higher education has only been around for approximately two decades. While in the beginning, literature used the term computer forensics (Kessler & Schirling, 2006; Kessler, 2007), nowadays, the domain comprises several sub-disciplines. To get an overview of existing DFIR education possibilities and their contents, we analyzed a selection of academic and commercial offers. Note, for simplicity in the following, we use the term courses instead of education possibilities where a course may be a part of a class[3], a single class offered as part of a degree program as well as fully featured courses and study programs. Courses are usually developed over a longer time period, and changes are slow, especially in academic programs. Therefore, this analysis provides insights into a more stable set of DFIR skills. The descriptions of courses are provided in a wide range of granularity, from no description to long lists of content. Furthermore, the descriptions of skills differ significantly. The challenge was to match this on a common denominator.

4.1. Methodology

We examined a mixed set of courses from both academia and the private sector, where the main focus was on Europe. The courses from the private sector were offered from institutions such as SANS, Udemy, and IACIS. Academic courses came from various universities and countries across Europe, including Czech, Germany, Ireland, Norway, and the UK. Our selection was built as follows:

Collection: Existing DFIR courses were identified through online searches and collected in a preliminary list. Searches focused on keywords such as `DFIR`, `Digital Forensics`, `Incident Response`, `Course`, `Training`, `Education` and combinations thereof. The list includes 42 elements. Note, we do not claim that this list is complete (listing all offerings), but it is sufficient for this article

Initial assessment: Next, we checked that the results were legitimate and provided sufficient detail on the corresponding website (we did not contact any provider for additional details). This reduced the list to 37 (17 academic; 20 private sector) elements.

Manual analysis: Lastly, all course descriptions were reviewed and mapped against the tree-structured skill matrix (see DFIR Skillmap) to identify the most frequently taught skills. Given the differences and detail throughout the descriptions, this was done manually.

[3] E.g., Incident response is covered during an 'Introduction to Digital Forensics' course in one session, but it is not the focus of the class.

4.2. Findings

A key finding was that there were only a few courses that explicitly advertise themselves as Incident Response courses. For instance, we found 'Advanced Incident Response, Threat Hunting, and Digital Forensics' (SANS; 6 days) or 'Certified Incident Handler' (ECIH; self-studied, or 2-day seminar). The majority of the identified courses were part of broader education programs labeled with 'Digital Forensics' and 'Incident Handling' being only a (small) part of the program. Consequently, the presented results are not limited to dedicated DFIR courses. Furthermore, we note that some programs use strongly related terms such as cybercrime, forensic computing, or investigations in their title. Lastly, we only found one self-learning and free opportunity named 'Intro to DFIR: The Divide and Conquer Process (3 hours)'[4].

Education. In general, we differentiate between academic programs, which are usually longer and cover a broader range of topics, and non-academic. With respect to academic programs, we found more master programs focusing on digital forensics than bachelor programs. A reason may be that digital forensics often requires computer science skills that can be gained through different degrees. Interestingly, we saw that academic programs (BSc and MSc) most often do not have a dedicated class on IR but incorporate it into other classes, e.g., Incident Response and Malware Analysis. In addition to dedicated programs, we also found that many universities at least offer 1-2 courses in the area of digital forensics, often as part of their cybersecurity or computer science degree. These introductory courses also often listed IR as part of the course, which by nature will not have thorough coverage.

On the other hand, the analysis showed that the majority of courses from the private sector require fundamentals from the computer science and security domains (prerequisite). These skills must be acquired beforehand, e.g., through academic programs, work experience, or other sources. The duration of these training programs varied from two to six days with one exception of 2 weeks. As mentioned earlier, there were only a few offers directly targeting IR; the majority of courses included the topic, e.g., as a module on one day.

Skills. From matching the description of each course with the developed skill matrix, we found that the focuses currently are 'investigation techniques' (73%), 'network forensics' (65%), 'system forensics', and 'data acquisition' (both 57%). While those were leading, the majority of topics from the matrix were covered by courses, given that many had very detailed descriptions. A possible reason that investigation techniques were found so frequently may be its general nature. It is also a common topic for less technical programs as they might occur in criminal justice programs.

Having a deeper look into investigation techniques (sub-skills) showed that many programs especially focus on 'digital

[4] `https://dfir-training.basistech.com/courses/intro-to-divide-and-conquer` (last accessed 2021-02-22).

forensics software tools' (49%), the 'digital forensic process' (49%), and 'investigation methodology' (41%). With respect to network forensics, it was eye-catching that rarely additional information was provided on what this entails (i.e., with respect to the skill matrix, this means no lower levels were defined). The most frequently mentioned topics were 'network traffic capturing' (16%), 'common network protocols' (14%), and 'network device analysis' (14%). In terms of system forensics, we found that nowadays, many programs focus on mobile devices (41%) and thus outperform traditional operating systems such as Windows (35%), Linux (19%), or Mac OS (19%). Another noticeable aspect was that newer topics such as IoT forensics (5%) or Cloud forensics (3%) were rarely included in programs. Lastly, we observed that topics such as legal issues (22%), ethical aspects (19%), and standards (3%) were often not part of the programs which we feel are important aspects of digital forensics and require attention.

5. Skills identification based on job listing review

The last pillar for this study was job listings collected and analyzed to confirm our previously identified findings. A supporting argument for job listings is that they reflect the current market situation, reveal the most needed expertise, and provide condensed summaries. In comparison, training programs may be updated less frequently and often have longer descriptions.

Job listings platforms. When looking into job listing platforms, we saw two challenges: (i) there are a plethora of employment websites for job listings; and (ii) to the best of our knowledge, we are not aware of any software that allows an automatic parsing of several platforms doing a keyword-based analysis. Hence, we decided to use a single website and perform a manual analysis of all listings. We opted for LinkedIn as it one of the biggest platforms, primarily in English and available worldwide. Moreover, LinkedIn has a standard job listing structure and allows scrolling through all available listings, making it easier to analyze manually and stay consistent. While we considered opting for more data sources, we decided to stick with LinkedIn for the sake of consistency and ease of use.

5.1. Methodology

As this study serves as an input for a DFIR course development for Europe, we aimed for higher weight on listings within Europe. Therefore, we divided our search into several regions/countries across Europe plus a small sample from the USA. The analyzed regions include Germany, Austria, Switzerland, Czech Republic, Netherlands, Sweden, Italy, Poland, and the USA. The searches were performed on LinkedIn.com, and the incognito browser mode was used. The only two parameters that were set in the search are the keywords presented in the following section and a country. To identify relevant listings, the following procedure was used:

Search: For each region, we utilized the following key terms: `Digital, Forensics, Incident, Response, DFIR` and combinations thereof.

Selection: Since these searches revealed large numbers of results, we carefully selected listings based on different locations, number of employees, and description, to obtain broad coverage. We also ensured that the listing included sufficient detail (i.e., education, skills) about the position where sufficient is a subjective classification.

Collection: All selected listings were aggregated in an Excel sheet focusing on the following aspects (columns): Job ID, date, company name, location, description, required skills, required qualification, and industry.

Manual analysis: Findings were mapped against the tree-structured skill matrix to identify most frequent skills.

5.2. Findings

The searches were conducted from January 25^{th} to 31^{st} in 2021 and the initial searches revealed a total of 200 to 22'000 jobs worldwide on LinkedIn alone, depending on the keywords used, which confirms the immense need for DFIR experts. For our analysis, we downloaded several listings per region and deleted non-English ones. Next, we removed listings that were too general (without the possibility to extract skills) or not related to the field of cybersecurity, such as incident response for nuclear threats or non-technical consulting. The filtering resulted in 66 listings used for the calculation of our skillmap. Most jobs were in major cities, but some offered remote work. Many listings were from well-known tech organizations such as Facebook, CrowdStrike, or Amazon. Still, DFIR experts are also wanted in other industries by less known companies like OTTO (German mail company) or Aposto Personal GmbH (placement of health care professionals).

Required education. The analysis showed a high overlap of education requirements between the listings from our sample. 48% asked for at least a bachelor's degree in computer science, cybersecurity, information systems, or related fields. Including listings that ask for a master's degree, the proportion of listings that ask for higher education rises to 53%. A Ph.D. is asked by 3% of the analyzed listings. Many state that equivalent practical experience is equally valued. 44% did not mention specific requirements for educational levels. Especially bigger corporations do not explicitly require a particular education. 15% of listings request applicants to possess or wanting to pursue certificate programs (i.e., GIAC, CISSP, etc.).

Required hard skills. From matching the required skills sourced from job listing with the preliminary skill matrix, we found tendencies for particularly valued and demanded skills. The top 5 skills named are 'incident handling' (79% of all job listings mentioning the keyword), 'data analysis' (42%), 'security event and incident logging' (39%), 'network forensics' (38%) as well as 'Linux forensics', 'windows forensics' and 'data acquisition' (18%), respectively. Additionally, a majority of the listings asked potential applicants to be proficient in one or more general-purpose scripting languages, such as Python, PowerShell, Ruby, Perl or Bash.

Required soft skills. Although soft skills were not the focus of our research, they are generally important as well. Besides technical skills and knowledge, almost all job listings asked their applicants for various soft skills, which were mostly overlapping throughout the job listings and included: analytic and logical thinking, an organized way of working, being a team player, flexibility, discretion, interpersonal skills and a strong interest in DFIR. Furthermore, even in countries where English is not the official language, the job listings asked their potential applicants for good proficiency in English, both written and spoken.

Offers for unexperienced graduates. When looking at the initial set of job listings, an eye-catching aspect was that most asked for experience. Thus, as a follow-up, we wanted to see how the market is for job starters. Since the number of entry-level positions on LinkedIn was rather small, we also looked on indeed.com (both offer options to filter based on job levels such as entry-level, mid-level, senior-level, etc.). Interestingly, most of the DFIR job offerings labeled as entry-level listings still ask for experience in DFIR or related fields, highlighting the importance of internships (or at least hands-on experiences during the study). We also performed a trivial search with respect to internships, which showed that offers for internships are generally very low. On both platforms, listings for internships worldwide were below 150.

6. DFIR Skillmap

In the following we combine the results of the survey, courses and job listings to build the DFIR skillmap. The subsections outline the methodology and present the results.

6.1. Methodology

The goal of the skillmap is to identify the most crucial skills for DFIR. Therefore, in our conception, the skillmap is a list of skills and their rankings. For its development, we used a hierarchical classification and a matrix-based ranking methodology. The creation of the skillmap consists of three steps:

Classification of skills: First, we generated a tree-based classification consisting of four levels (L1 to L4) of technical skills related to DFIR. The highest level (L1, root) is *DFIR*. L2 has 14 skills, mostly inspired by the ACM CCS[5]. L3 and L4 skills were gathered from various sources, mainly digital forensic papers, existing courses and teaching programs, websites, and blogs. In total, the tree consists of 134 skills; the lower in the tree, the narrower the skill is. The hierarchy was built manually to reflect relations between individual skills and avoid duplicates.

Creation of the skill matrix: With the existing classification, we created a matrix of skills to map to our data as depicted in Table 1. Each row represents one skill. Each column stands for one data record (R_1, R_2, ...). The matrix was manually populated with data from our three sets: 32 survey answers, 37 courses, and 66 job listings. Specifically, we searched for keywords *related* to the skills and marked the corresponding cell with an *X*. Note, each match of skill also triggers a match for the upper-level skill.

Skills	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	...
DFIR	X	X	X	X	X	X	X	X	...
– L2 skill	X		X	X	X		X	X	...
—- L3 skill			X	X			X		...
—- L3 skill	X		X	X	X			X	...
—— L4 skill					X			X	...
—— L4 skill	X		X	X					...
– L2 skill	X	X	X		X	X		X	...
—- L3 skill			X			X			...
—- L3 skill					X			X	...
...	...	...	...	...	...	...	...	...	...

Table 1: An example skill matrix.

Assessment: For each skill, we calculated the number of matches (*X*) between survey answers, courses, and job listings. The calculation is not weighted as we did not want to prioritize any particular skill or data source over the others. Next, we normalized each result as percentages of matching records for each skill in each dataset. To estimate its overall importance, we calculated the average (avg) percentage across all three datasets. The resulting values indicate what skills are the most important.

6.2. Results

Table 2 shows a simplified version of the resulting map of skills followed by the percentage of matches with survey answers, courses and job listings. The complete skillmap is available from the project web pages[6]. The last column shows the average of the previous three. Since the complete skillmap is too large to display, the table only shows L2 skill categories and part of the most frequent L3 skills. In network forensics, as the most significant category, the map goes down to L4 with 'application protocol analysis'. Note, the table does not display skills whose average percentage is below 1%.

6.2.1. L2 skills

Figure 3 provides a complete overview of L2 skills and their match ratio over all datasets. The top 3 skills are 'network forensics', followed by 'incident handling' and 'system forensics'. All three frequently appeared among the survey answers, existing courses, and job listings. Skills like 'investigation techniques' or 'data acquisition', mostly covering general principles, appeared primarily in courses. An interesting case is 'cloud forensics' that our respondents frequently mentioned in the survey, but the courses almost never cover this area. The finding correlates with multiple surveys from related work where participants often referred to cloud forensics as a challenge for future research (Harichandran et al., 2016; Forensic Focus, 2016; Luciano et al., 2018). We suggest this could be a critical-to-include topic in future courses.

[5] https://dl.acm.org/ccs (last accessed 2021-02-22).

[6] https://sites.google.com/vutbr.cz/dfir-alliance

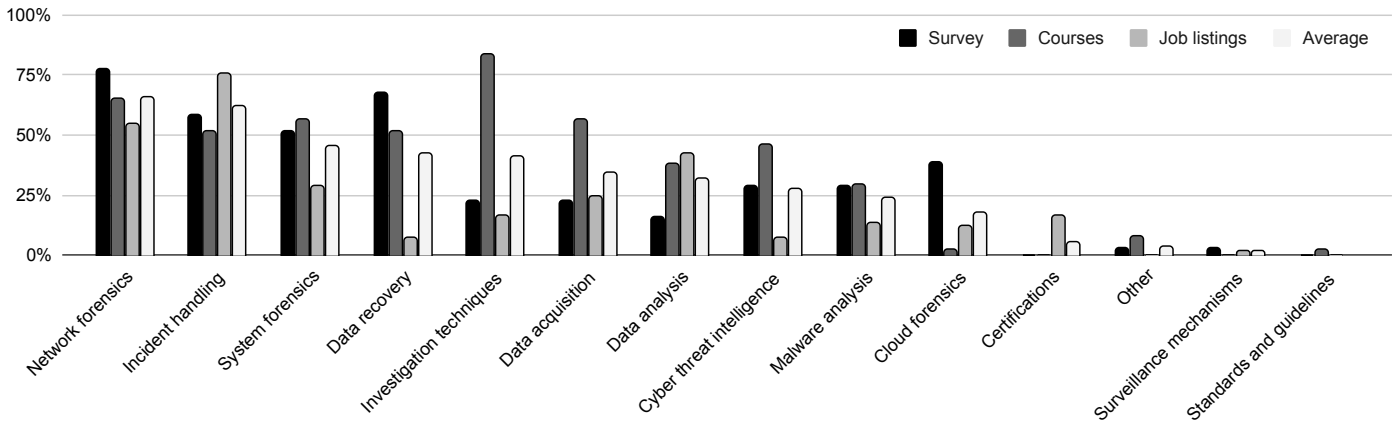

Figure 3: L2 skill categories and their and their occurrence in survey answers, courses, and job listings

6.2.2. *L3 skills*

To provide a deeper insight into the three most significant L2 skills, we summarize the L3 sub-skills:

Network forensics. In the area of network forensics, illustrated in Figure 4, the most significant L3 skill is 'encrypted traffic analysis'. Similar to cloud forensics, survey participants frequently refer to the topic, but existing training courses rarely cover it. We believe this confirms the findings from multiple related surveys where the respondents identified encryption as the biggest current challenge in digital forensics (Harichandran et al., 2016; Forensic Focus, 2018; Luciano et al., 2018). Another domain for possible improvement in training courses is 'security event and incident logging', frequently requested in job listings. The remaining top-ranked L3 skills in network forensics are mostly general proficiencies (i.e., basic skills) like understanding network protocols, architecture, analyzing and capturing the traffic.

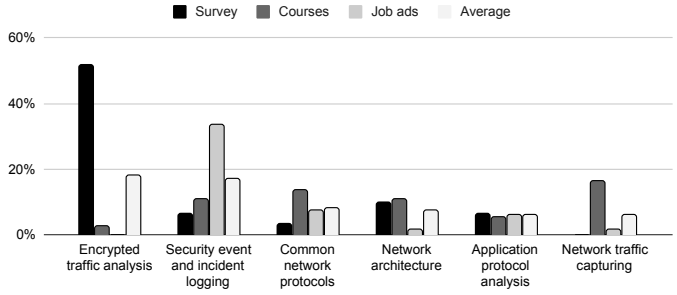

Figure 4: Network forensics: the top L3 skills

Incident handling. Figure 5 shows the top-ranked L3 skills from the incident handling category. The courses' descriptions frequently refer to the incident handling process and often mention detailed skills like understanding endpoints, domains, physical attacks, or covering tracks. Interestingly, while most survey answers and job listings cover the need for incident handling proficiency, they provide very little information about what particular skills from this domain are needed the most. On the other hand, the survey respondents, course descriptions, and job listings often provided concrete information on the usage of tools for security monitoring, network traffic processing, and penetration testing. Possibly, they considered the individual incident handling processes too apparent to be described in detail for a DFIR survey. Therefore, existing courses seem to be the only valuable source of information in this case.

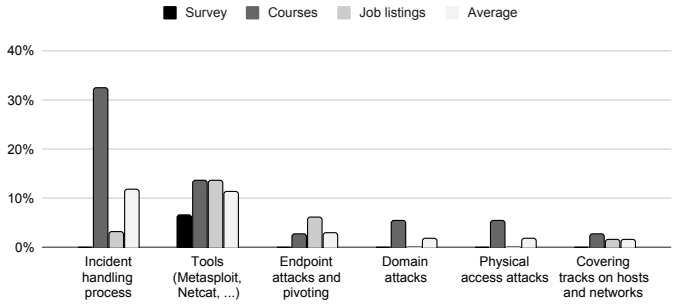

Figure 5: Incident handling: the top L3 skills

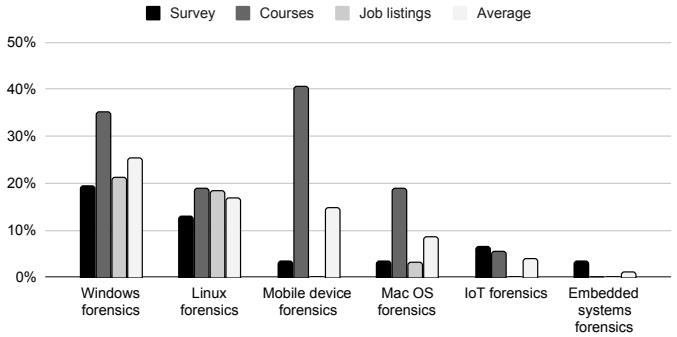

Figure 6: System forensics: the top L3 skills

System forensics. Ranked third was the L2 category system forensics which, summarized in Figure 6. The most frequent topics are Windows and Linux forensics. Both are frequently referred to in all three input datasets. An interesting observation is mobile device forensics' regular appearance in courses, although this skill is requested by no listing and only rarely mentioned in the survey answers.

Skill	Survey	Courses	Job list.	Avg
DFIR (L1)	100 %			
Network forensics (L2)	77 %	65 %	55 %	66 %
Encrypted traffic analysis (L3)	52 %	3 %	0 %	18 %
Security event and incident logging	6 %	11 %	33 %	17 %
Common network Protocols	3 %	14 %	8 %	8 %
Network architecture	10 %	11 %	2 %	7 %
Application protocol analysis	6 %	5 %	6 %	6 %
Web forensics (L4)	6 %	8 %	5 %	6 %
E-mail forensics	0 %	8 %	0 %	3 %
File transfer protocols	0 %	3 %	2 %	1 %
VoIP analysis	0 %	3 %	0 %	1 %
Network traffic capturing	0 %	16 %	2 %	6 %
Network device analysis	0 %	14 %	3 %	6 %
Network protocol reverse engineering	3 %	0 %	5 %	3 %
NetFlow analysis and attack visual.	0 %	5 %	0 %	2 %
Wireless network analysis	0 %	5 %	0 %	2 %
Open-source network security proxies	0 %	3 %	0 %	1 %
Incident handling	58 %	51 %	76 %	62 %
Incident handling process	0 %	32 %	3 %	12 %
Tools (Metasploit, Netcat,...)	6 %	14 %	14 %	11 %
Endpoint attacks and pivoting	0 %	3 %	6 %	3 %
Domain attacks	0 %	5 %	0 %	2 %
Physical access attacks	0 %	5 %	0 %	2 %
Covering tracks on hosts and net.	0 %	3 %	2 %	1 %
Password attacks	0 %	3 %	0 %	1 %
Reconnaissance and open-source int.	0 %	3 %	0 %	1 %
Scanning and mapping	0 %	0 %	2 %	1 %
System forensics	52 %	57 %	29 %	46 %
Windows forensics	19 %	35 %	21 %	25 %
Linux forensics	13 %	19 %	18 %	17 %
Mobile device forensics	3 %	41 %	0 %	15 %
Mac OS forensics	3 %	19 %	3 %	8 %
IoT forensics	6 %	5 %	0 %	4 %
Embedded systems forensics	3 %	0 %	0 %	1 %
Data recovery	68 %	51 %	8 %	42 %
Memory forensics	32 %	14 %	5 %	17 %
Recovery of encrypted content	48 %	0 %	0 %	16 %
Disks and storages	13 %	16 %	2 %	10 %
Carving	3 %	16 %	0 %	6 %
Recovery of multimedia files	3 %	11 %	0 %	5 %
Data hiding	3 %	0 %	0 %	1 %
Artifact recovery	0 %	3 %	0 %	1 %

Skill	Survey	Courses	Job list.	Avg
Investigation techniques	23 %	84 %	17 %	41 %
Digital forensics process	6 %	49 %	12 %	22 %
Digital forensics software tools	0 %	49 %	8 %	16 %
Computer for. and inv. methodology	0 %	41 %	0 %	14 %
Reporting and presenting evidence	6 %	27 %	3 %	12 %
Data acquisition	23 %	57 %	24 %	35 %
Data acquisition process	0 %	38 %	8 %	15 %
Evidence handling	6 %	16 %	3 %	9 %
Host based live acquisition	3 %	16 %	2 %	7 %
Acquisition preparation	0 %	19 %	0 %	6 %
Filesystem fundamentals	0 %	19 %	0 %	6 %
Dead box acquisition	3 %	8 %	0 %	4 %
Manual triage	0 %	3 %	5 %	2 %
Remote acquisition	0 %	5 %	2 %	2 %
Storage technologies	0 %	5 %	2 %	2 %
Data formats	0 %	3 %	0 %	1 %
Manually finding data	0 %	3 %	0 %	1 %
Data analysis	16 %	38 %	42 %	32 %
File system timeline analysis	3 %	16 %	0 %	6 %
Id. of normal system and user act.	3 %	3 %	0 %	2 %
Data analytics in-depth	0 %	3 %	2 %	1 %
Cyber threat intelligence	29 %	46 %	8 %	28 %
Intelligence fundamentals	0 %	32 %	0 %	11 %
Kill chain, diamond, action matrix	13 %	8 %	3 %	8 %
Intelligence application	3 %	11 %	0 %	5 %
Campaigns and attribution	0 %	11 %	0 %	4 %
Analysis of intelligence	0 %	8 %	0 %	3 %
Malware as a collection Source	3 %	0 %	0 %	1 %
Sharing intelligence	0 %	3 %	0,%	1 %
Malware analysis	29 %	30 %	14 %	24 %
Code and behavioral analysis	0 %	5 %	3 %	3 %
Analysis of malicious documents	0 %	5 %	0 %	2 %
Analysis of malicious executables	0 %	5 %	0 %	2 %
Analysis of web-based malware	0 %	3 %	0 %	1 %
Windows malware characteristics	0 %	3 %	0 %	1 %
Malware analysis in memory	0 %	3 %	0 %	1 %
Cloud forensics	39 %	3 %	12 %	18 %
Certifications	0 %	0 %	17 %	6 %
Other	3 %	8 %	0 %	4 %
Surveillance mechanisms	3 %	0 %	2 %	2 %
Standards and guidelines	0 %	3 %	0 %	1 %

Table 2: A simplified version of the DFIR skillmap. L1 and L2 topics are complete. L3 and L4 are limited to selected top-ranked entries. The listing only contains entries with one or more appearances; one L1, L2, L3 and L4 have been marked.

Though this may be viewed as an anachronism in the design of courses, the explanation is that the participants of the survey were DFIR practitioners rather than employees of law enforcement agencies. Nevertheless, it indicates that traditional mobile forensics plays a less important role in the DFIR domain, and this should be considered for future updates of training and teaching curricula. Similarly, forensic analysis of macOS exhibits the significant gap between course offerings and requests. This can be explained by the fact that courses involving operating system analysis systematically focus on all major types, while the practice reflects the difference in the use of these systems in the target environments. Microsoft Windows is the common desktop operating system installed on more than 70% of machines[7]. While macOS is the second, the demand for the Linux OS investigation skills in our survey is because of its use as the major operating system of servers.

Summary. With the spread of attacks from the Internet, network forensics and incident handling are the most demanded domains. System forensics and data recovery are the most common in the courses, and their supply/demand is balanced. Some traditional topics like investigation techniques, data acquisition, and analysis, frequently covered in courses, were not stressed in DFIR demands. It may be attributed to the fact that these topics are fundamental and thus often considered evident by survey participants, deducing from some answers.

Surprisingly, skills related to cyber threat intelligence topics are less demanded among practitioners than generally considered and offered in courses. The role of DFIR practitioners can explain it. The vast majority of them are consumers of intelligence systems, not participating in their development. Finally, the survey revealed a significant difference in supply/demand for cloud forensics. While more than a third of participants denoted this area as important or a challenge for their daily work, only a fraction of courses offers adequate training.

Recall that the applied methodology employed the review of research papers as the source of topics for the classification system. However, the practitioners and job listing analysis survey barely provided information in the L4 level of detail. The analysis of digital forensic courses gave us more detailed information but did not cover all topics in the classification tree. However, the developed classification was supposed to unify the name system of DFIR topics rather than exhaustively cover all.

[7] https://gs.statcounter.com/os-market-share/desktop (last accessed 2021-02-22).

7. Limitations

Due to the nature of the collected data, we analyzed data from the three sources manually. The number of gathered items is therefore limited mainly by the time, language (only materials in German, Czech, and English are considered), and labor resources available. We argue that our results provide sufficient guidance and paint the picture of the state of the domain. Using open-ended *survey* questions provided an interesting view on the current practice but complicated the evaluation of the results as participants used different terminology. Also, some questions could not be unambiguously answered by all participants due to the domain's sensitive nature. For example, 25% of participants could not declare whether their team has a formal DFIR procedure. The *job listings* search was limited to one platform. In the listings themselves, employers' skills were stated in an abstract manner rather than being specific. As common practice for job listings suggests, the demanded skills describe a perfect candidate who most of the time does not translate to real-world applicants. The original *skillmap* consisted of four levels with 134 nodes total. However, mapping the data to the skills revealed that many of the nodes at the deepest level are not explicitly referenced. We argue that this fine granularity is still important but may be too specific to be explicitly named. Furthermore, using more higher-level terms (L2) provides more flexibility, i.e., no need to change descriptions, and may be sufficient (specific skills may be acquired as needed).

8. Discussion and conclusion

The paper aimed to identify the essential Incident Response Practitioners' technical skills collected through surveying professionals, analyzing existing courses and job listings. Finally, we briefly answer the questions from the introduction.

Q1. Which skills are essential (required) for DFIR specialists? Major findings of each part have been summarized in the corresponding paragraphs. All collected data were projected to the DFIR skillmap enabling us to cluster skills according to their current relevance. An eye-catching aspect was that often only L2 / L3 terms are used and required, which could be for several reasons: (1) one may want to keep everything more general to have more flexibility (e.g., during the hiring or developing training materials); (2) it may be better to have broad knowledge on general topics instead of being an expert in several L4 skills; or (3) the domain is too complex to cover everything, and thus we stick to a higher level of detail. The most desired future skills are Cloud Forensics, AI/Machine Learning, Pentesting, and Offensive Security. They, together with encrypted data analysis, were often denoted as challenges. While not be part of this analysis, soft skills were also frequently mentioned and are equally important.

Q2. Are all skills equally important or can they be ranked? Our matrix shows that it is possible to rank skills to a certain degree where network forensics, incident handling and system forensics are the top three. An interesting finding from the survey was basic skills such as programming are in high need. This is an indicator that despite all the tools on the market, it is still necessary to develop one's own scripts.

Q3. How do experts gain their experience/knowledge? While many learn through their degree and then gain experience through the job, the survey data shows that practitioners often use online sources and self-learning to enhance their skillset. Although not asked in our survey, we assume that these skills are required to solve a current challenge (i.e., learn as you go). From an educator's perspective, it is essential to teach students how to research and learn, especially from online resources such as blogs, articles, or videos. This may be accomplished by applying techniques from challenge-based learning (Johnson et al., 2009). On the other hand, it is also essential that practitioners keep sharing new methods and artifacts through initiatives such as CASE[8] or AGP (Grajeda et al., 2018).

Q4. Does the job market require certain degrees / training / certifications? The job market seems fairly flexible and often only requires a bachelor's degree (of course a master's degree is a plus) or equivalent practical experience. One reason could be the tense job market and that is is difficult to fill positions. Generally, it was noticeable that many listings asked for work experience which outlines the importance of hands-on education. Certifications are also valued by employers. While they are often a supplement criteria some employers require their applicants to possess certain certificates. This is especially the case when the job requires mastery in certain tasks or tools.

Although the information sources were obtained in limited geographical and temporal contexts, we believe that the findings are relevant to build a DFIR skillmap. The skillmap's goal is to provide a baseline for creating training courses to educate future DFIR professionals. We have shown that much of the existing courses' content is still relevant but that there are gaps that need to be filled—the significant differences between professionals' opinions on required skills and the content of existing courses are mainly in anticipated technical skills. The most prominent example is the skill to analyze encrypted data. On the other hand, we identified courses that provide skills that are not on the professional's priority lists. This can, however, be caused by the limited number of participants in our survey.

Acknowledgments

We like to thank Pavel Laskov from the University of Liechtenstein for valuable discussions and feedback on this article. This material is based upon work supported by the Agentur für Internationale Bildungsangelegenheiten (AIBA) under Agreement No. 2020-1-LI01-KA203-000185 and by Brno University of Technology, Grant No. FIT-S-20-6293. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of funding agencies.

[8] https://caseontology.org (last accessed 2021-02-22).

References

CrowdStrike (2019). What is incident response? https://www.crowdstrike.com/epp-101/incident-response-ir-plan/.

Du, X., Hargreaves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac, N.-A., & Scanlon, M. (2020). SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation. In *The 13th International Workshop on Digital Forensics (WSDF), held at the 15th International Conference on Availability, Reliability and Security (ARES)* ARES '20 (pp. 1–10). New York, NY, USA: ACM.

Forensic Focus (2016). Current challenges in digital forensics. URL: https://www.forensicfocus.com/articles/current-challenges-in-digital-forensics/ [Online; Accessed: 2020-11-04].

Forensic Focus (2018). Findings from the forensic focus 2018 survey. URL: https://www.forensicfocus.com/articles/findings-from-the-forensic-focus-2018-survey/ [Online; Accessed: 2020-11-04].

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digit. Investig.*, *7*, S64–S73. URL: http://dx.doi.org/10.1016/j.diin.2010.05.009. doi:10.1016/j.diin.2010.05.009.

Grajeda, C., Sanchez, L., Baggili, I., Clark, D., & Breitinger, F. (2018). Experience constructing the artifact genome project (agp): Managing the domain's knowledge one artifact at a time. *Digital Investigation*, *26*, S47–S58.

Harichandran, V. S., Breitinger, F., Baggili, I., & Marrington, A. (2016). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security*, *57*, 1–13.

Henry, P., Williams, J., & Wright, B. (2013). The SANS survey of digital forensics and incident response. *SANS Institute InfoSec Reading Room*, .

Johnson, L. F., Smith, R. S., Smythe, J. T., & Varon, R. K. (2009). *Challenge-based learning: An approach for our time*. Technical Report The new Media consortium.

Kessler, G. C. (2007). Online education in computer and digital forensics: A case study. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 264a–264a). IEEE.

Kessler, G. C., & Schirling, M. E. (2006). The design of an undergraduate degree program in computer & digital forensics. *Journal of Digital Forensics, Security and Law*, *1*, 3.

Lee, R. M., & Lee, R. T. (2018). Sans 2018 threat hunting survey results. *SANS Institute Reading Room*, .

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. In *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)* (pp. 9–20). Daytona Beach, FL, USA: ADFSL.

Luciano, L., Baggili, I., Topor, M., Casey, P., & Breitinger, F. (2018). Digital forensics in the next five years. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (pp. 1–14).

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. *Computers & Security*, *23*, 12 – 16. URL: http://www.sciencedirect.com/science/article/pii/S0167404804000100. doi:https://doi.org/10.1016/j.cose.2004.01.003.

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer security incident response team development and evolution. *IEEE Security Privacy*, *12*, 16–26. doi:10.1109/MSP.2014.89.

Stambaugh, H. (2000). *State and local law enforcement needs to combat electronic crime*. US Department of Justice, Office of Justice Programs, National Institute of ....

STN, E. (2005). Iso/iec 17025: 2005: General requirements for the competence of testing and calibration laboratories. *SUTN Bratislava*, (p. 37).

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research*, *17*, 183–194. doi:10.1080/15614263.2015.1128163.

Vishik, C., & Heisel, M. (2015). *Cybersecurity Education snapshot for workforce development in the EU*. Technical Report ENISA.

Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: the diagnostic work of it security incident response. *Information Management & Computer Security*, .

Zan, T. D., & di Franco, F. (2020). *Cybersecurity skills development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database*. Technical Report ENISA.

Zawoad, S., & Hasan, R. (2015). Digital forensics in the age of big data: Challenges, approaches, and opportunities. In *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems* (pp. 1320–1325). IEEE.