Law Enforcement educational challenges for mobile forensics

Georgina Humphries[a], Rune Nordvik[a], Harry Manifavas[b], Phil Cobley[c], Matthew Sorell[d]

[a]*Norwegian Police University College*
[b]*Foundation for Research and Technology Hellas*
[c]*Micro Systemation AB*
[d]*University of Adelaide*

Abstract

Training, tools, and standards are important foundations of mobile forensics. This work focuses on existing curricula and courses in the domain of mobile forensics. In order to identify courses in areas of computing where mobile forensics may be offered, this research utilises open source information gathering, in addition to questionnaire and interviews, to capture additional information and the views and experiences of educators and/or trainers. This research finds that current education and training offerings mainly include topics regarding acquisition and analysis of mobile data. Current education and training do not cover the areas of a complet mobile forensic investigation, from crime scene to court. In addition, trainer opinions on skills shortages include the lack of basic knowledge, generic skills in forensics and investigation, lack of skilled practitioners, and necessary mindsets to critically think, investigate and avoid dependency on Digital Forensic software.

Keywords: Mobile Forensics, Education, Training

1. Introduction

Over the years, education and training provisions have been developed to address a shortage of skilled practitioners in the field of Digital Forensics. In the early days the discipline did not use formal processes, tools, or training, instead relying on ad-hoc, on-the-job training from practitioners skilled in other computing related disciplines [17]. The transition from dead forensics of a simple hard drive to live data forensics has contributed to the challenges experienced by law enforcement today. Furthermore, there have been several challenges which have grown due to advances in technology: stronger security and the need for privacy, large quantities of data, new applications and sensors. Additionally, effective training for handling digital evidence to ensure verification, validity and accuracy would have previously focused on ensuring the data was unaltered and undamaged. However, Law Enforcement Officials (LEOs) now face the challenge of managing live data that is typically at constant risk of being altered. This brings an increased risk of accidental or deliberate data alteration or loss (whether by the user or the system), which may impact the evidential integrity and viability of that data.

The investigation of mobile phones utilises techniques and methods closely associated with computer forensics [30]. However, mobile forensics includes, or should include investigations of other features related only to mobile devices and mobile networks. This could be traces from different kinds of sensors, specific networks used for mobile communications, and data stored by mobile communication service providers.

Within law enforcement there is ever-increasing pressure placed on analysts and investigators to manage a range of devices, platforms, types of crime, masses of data, encryption and decryption, malware, and other components of an investigation. The lack of understanding and ambiguity within the field can cause a range of issues with limited budgets, resourcing (people and technology), skills, and keeping up-to-date with technologies and relevant training.

Challenges for training and education providers, to date, also include issues surrounding the necessary resourcing and skills to teach and train individuals in digital forensics, and most recently mobile forensics, as described by participants of this research. One particular issue discussed by Yannikos et al. [40] includes the problem of providing real data sets. While the authors describe an overview of data corpora for digital forensics [16, 39, 26] it is suggested that using real data sets is problematic since there is no ground truth, proposing the automatic generation of realistic synthetic data by using a Markov chain simulation [40]. Synthetic data provides ground truth, which is very important for digital forensics education and research.

One area which is not covered is the efficacy of education and training for mobile forensics. In particular this research will focus on the evaluation of the coverage of mobile forensics across a range of providers. While this does not address the efficacy of offerings, it may enable the discipline to identify areas which require additional coverage.

1.1. Objectives

The FORMOBILE [15] Training Work Package is a project seeking to identify a novel curriculum in mobile forensics training for law enforcement. This research has one main objective: to identify the degree to which current education and training cover the areas of a complete mobile forensic investigation chain, from crime scene to court.

1.2. Scope

This research described that computer forensics and mobile forensics are related, and the findings of this research are relevant for digital forensics research in general. However, a comparison between these two different domains are out of scope for this paper. The scope of this research focuses on mobile forensics describing the current state of training, to identify gaps, which then can be used to develop new training bridging these gaps.

1.3. Key Findings

This research identifies that mobile forensic course descriptors (education and training) are often broad or brief. Thematic analysis of the topics, descriptions and learning outcomes indicates that acquisition is the topic or category covered most. Phases or elements such as the crime scene, analysis and inquiry/investigation, and the court/decision phase may not be covered in depth. In particular there are few courses which target investigators, prosecution, or management within law enforcement.

Furthermore, this research considers the opinions of trainers and/or educators where responses and discussions revealed challenges with keeping up-to-date (materials, field, processes, techniques, etc.) and the awareness/education of relevant law enforcement stakeholder groups such as, first responders, analysts, investigators, prosecution, judges, management etc. Discussions also identified the challenges education and training are exposed to due to fast-paced advancements such as, security hardening techniques, lack of standard procedures, large volumes of data, and few datasets. Participants also documented skills shortages which were themed among areas of analysis, investigation, forensic readiness, and automation.

This research suggests that mobile forensic training should include courses tailored to relevant law enforcement stakeholder groups. Additionally, education and training offerings in mobile forensics should add more focus on the analysis of data, cloud forensics, network communications, and small scale digital devices and sensors.

The research conducted in this study has been used to inform the design of the FORMOBILE Mobile Forensic Curriculum for law enforcement. Findings have facilitated decision-making processes regarding topical content, levels of awareness and education, stakeholder groups, challenges and resources, and more. The details of the curriculum will be the subject of future publications.

1.4. Organization of this paper

This paper is organised into six sections. The first section has introduced the research and outlined the objectives. In section 2 the current state of the art of scientific publications are summarised. Section 3 describes the methods used in the analysis of current course offerings, and the use of both questionnaires and interviews to collect opinions and experiences. Research findings are presented and analysed in section 4. The results are then separated into three distinct approaches and discussed in section 5, with the conclusion to the research being presented in section 6.

2. Related work and contributions

There has been a significant volume of literature published in relation to education and educational/training methods, but the focus of this paper will be related to the law enforcement needs for mobile forensic training. There is also an abundance of research which focuses on digital forensics education, covering a range of topics including learning styles, needs and techniques, course coverage, development of the discipline, and challenges.

2.1. Surveys

Harichandran et al. [19] performed a literature review and a survey where they found that there is a need for better education/training, support for cloud and mobile forensics, improvement of open source tools, research on encryption, malware and trail obfuscation, revised laws, better communication, and more resources (personnel and funding). Further, they refer to the National Institute of Justice (NIJ), which indicates that first responders do not necessarily know how to properly secure devices. Skills in investigation were the future skills most rated by the respondents, followed by the proficient use of forensic tools, and reverse engineering. The authors [19] also found that the prominent future topics for research within digital forensics should be mobile and cloud forensics.

Tu et al. [38] contribute with a survey covering courses in digital forensics targeting educators and practitioners. The authors [38] note that in 2012 the most investigated cases in the US involved computers, and more than half of those cases involved mobile devices. Proposing course modules based on an analysis of the survey, Tu et al. [38] propose 6 courses; Digital Forensics Fundamentals, Advanced Computer Forensics, Network/Internet Forensics, Mobile Digital Forensics, Professional Projects on Digital Forensics, and Courtroom Experience. The topics of the the Mobile Digital Forensics were wireless security and attacks, and wireless track and investigation, in addition to different cell phones. In order to reduce costs, Tu et al. [38] suggest tackling any issues and adopting suitable approaches of designing online security and digital forensic courses.

2.2. Digital Forensics hands on training

Cigoj and Blažič [8] describe a cloud based E-learning tool, EduFors, that can be used for multi-level training in digital forensics. The tool manages the complete process of generating cybercrime scenarios. The supported scenarios are phishing, SQL-based data leakage, and distributed denial-of-service (DDOS) attack. The results from the tool: Digital Forensics Education and Training (DFET) are exploited and further developed by the Cyber Academy, which also aims to include Mobile Device Forensics, Cryptography, Malware analysis, etc. [37].

Oparnica [29] describes the status of training and education of law enforcement officers and prosecution in Eastern Europe, especially Croatia, which do not include topics related to digital forensics. He argues that digital forensic training should be hands-on and that the forensic images have to be realistic. Asserting that forensic experts, first-responders, prosecutors, judges, and defence lawyers need training/education, he argues that education should be developed by academia, but also on the job training by Law Enforcement Agencies (LEAs) is valuable. Important specialisation areas are computer forensics, memory forensics, investigation of mobile platforms (not only cell phones), cloud forensics, Internet and network forensics, social media forensics, and open source intelligence.

2.3. Mobile forensic training

While there is literature which covers digital forensics education, few consider mobile forensics. In particular, there are few literary sources that discuss training in the field of mobile forensics, within education or for law enforcement. One author, Bajramović [5] describes challenges with mobile forensics technologies, methodologies, training, and expenses. Bajramović [5] identifies that first-hand knowledge is necessary to effectively investigate mobile devices, and that developing tools and methods that include the complete investigation of different mobile devices is essential [5]. Bajramović [5] also discusses the challenges which mobile forensic investigations offer, such as:

- the live state of performing a mobile forensic investigation;
- the need for training using updated and realistic materials and forensic tools; and,
- the need for training and increased budgets.

In 2012 Kröger and Creutzburg [24] proposed the concept of traineeships utilising the following structure: objectives of the exercise, the task, theory, rules and regulations, required software and hardware, evaluation, and a sample solution. The authors outline exercises in topics such as: computer forensics, live forensics, mobile forensics, network forensics, DVD forensics, and Linux forensics. Exercises for mobile forensics focused on iOS (with and without jailbreaking), Android (rooted and non-rooted devices), and the use of tools such as Oxygen Forensics [31] and viaExtract [28].

Paullet et al. [32] note in 2016 that there is a gap in courses focusing on mobile forensic security and describe a train-the-trainer program within cyber security education. The authors argue that mobile device security is not matching the rise of malware targeting mobile devices and discuss how attacks on mobile devices are easier since the devices are constantly connected to a network. They argue that, when it comes to security, prevention forms is a core component of risk mitigation. They describe a certificate program at the Robert Morris University consisting of seven courses (four mandatory, three of five available electives). One of the mandatory courses is Mobile Forensics.

Paullet et al. [33] implemented the train-the-trainer program at Robert Morris University, with 20 academic institutions trained as of May 2017. Topics covered included: why teach mobile forensics and security, the evolution of mobile forensics, types of devices and features (smart phones and feature phones), procedures for evidence handling (integrity focus, blocking signals), mobile security overview and policy, introduction to mobile forensic tools (ten hands-on lab assignments, acquisition, sort and search for evidence, documentation), legal concerns for teaching mobile forensics (students needed to sign an agreement to not use the skills learned for illegal activities).

2.4. Law school education in forensics

Alva and Endicott-Popovsky [2] highlight in 2012 that "[t]here is an alarming gap in the legal and judicial community's understanding of digital evidence." In addition, Sanger [34] describes in 2018 that forensics are not taught in Juris Doctor (JD) curriculum, even though elective courses may or may not be available. Sanger suggests a curriculum which also includes a systematic education in forensics, where the aim is to train lawyers and judges to understand the basic process of science, and be able to assess the admissibility of scientific opinions.

Sanger [34] describes that lawyers should learn the basics of forensics, how experiments are performed, how variables are controlled, how hypotheses must be testable and falsifiable. Lawyers also need to understand that nothing is proven, since science deals with uncertainty. How investigations differ from laboratory work, and why the evidence may not be as reliable as a more controlled experiment. They should also learn how forensic investigations work and learn to communicate with the forensic expert, facilitate for avoiding bias, and that opinions are based on science, not speculations or biased by advocacy, arguing that nothing should be admissible if it does not meet the standards of science [p. 22]. The students should master the standards of Frye, Daubert, Kumho Tire and Joiner [p. 23]. The author also argues that law students need statistical knowledge about frequency, random match probability, likelihood, Bayesian analysis or Bayesian networks.

Brenner and Schwerha cited in Flory [14] state that for an effective prosecution, lawyers must possess a level of knowledge in computer forensics and information technology. The survey found that prosecutors "were at least effective in introducing digital evidence", and judges were for the most part able "to understand digital evidence admissibility". An interesting finding in the survey demonstrated that the perception among respondents was that the ability of non-law enforcement officials was greater than the investigating law enforcement practitioners and prosecution for awareness and applicability of digital evidence. Flory also discusses general issues in digital forensics for the law community, such as: communication and collaboration; resources and funding for training opportunities; lack of forensic experts and skilled practitioners; and, self-perceived views on the ability to investigate using digital evidence. Flory also expresses what were classified as emerging technologies at the time, such as "[e]ncryption, wireless technologies, and steganography" as issues which had severe impact on the ability to conduct an investigation, noting, at the time, concerns over the tools' abilities to keep pace with the change and achieve the associated tasks.

2.5. Lack of Standardisation

The debate surrounding standardisation and certification has been longstanding within digital forensics. From the inception of computer forensics there have been several accreditation programs, processes, standards, and best practices presented. Best Practices have included for example, ACPO Good Practice Guidelines [4], ISO 17025 [21], and ENFSI Best practice manual for the forensic examination of digital technology [11], among others. In the early days of best practices the focus was placed on computer forensics. With technological shifts the field has seen a number of developments including the addition of best practice guidelines focusing on investigative processes, forensic readiness, laboratory processes, and topical categories within digital forensics e.g., mobile forensic investigations [35]. In addition, Law Enforcement Agencies (LEAs) implement several Standard Operating Procedures (SOPs) adding another level of standardisation to investigations. Although there is an abundance of literature on forensic investigation processes, and several standards and best practice guidelines, practitioners have experienced mixed approaches with little clarity, which have led to a lack of internationally accepted standards within the field of digital forenscis and mobile forensics for several years [3].

3. Method

This section describes the processes used to examine the current status of education and training offerings for mobile forensics and perform gap analysis. The process involved four main stages.

- Stage 1 - Literature Review: Materials collated were those which focused on digital forensics education and/or training, mobile forensics training, mobile forensics developments and challenges, and law enforcement as a stakeholder within the discipline.
- Stage 2 - Open Source Information Gathering: to identify, collect and analyse existing courses in mobile forensics. The collection of course information followed the Didactic Relationship Model outlined by Hiim & Hippe [20, 36].
- Stage 3 - Educator/Trainer Questionnaire: qualitative survey targeting educators and trainers to supplement information found during stage 2.
- Stage 4 - Interviews: qualitative conversational/ unstructured online and/or telephone interviews.

Courses were refined to exclude those providing too little information and those with a security-driven focus rather than digital and/or mobile forensics. Over 300 courses across 30 countries were identified within the fields above. Of these courses 152 were considered to have some relationship to mobile forensics, be it a dedicated training course or, a module at university level. Of the 152 courses, only 94 are considered to provide enough information related to mobile forensic content to be considered for analysis. The qualitative data was processed using thematic analysis [13, p.473] where several codes were formed from the course descriptors/information available, adopting a hierarchical approach.

During stage 3, educator and trainer contact information was collated from all potential courses. The questionnaire was distributed to this contact list and spread using the FORMOBILE [15] media platforms and consortium member contacts. This resulted in 27 responses, of which 21 were from a range of educators and trainers offering courses including mobile forensics. 6 did not include mobile forensics in programmes. 67% (14/21) of the mobile forensic courses were targeting Law Enforcement at a beginner level, or undergraduate/postgraduate students at a beginner level. The remainder of the courses were either targeting all, intermediate, or advanced levels. The questionnaire focused on collecting additional course information from the providers due to relatively broad descriptors found during the course collection in stage 2. The questionnaire was used to extrapolate, more specifically, individual experiences and opinions in relation to current skills shortages, course offerings and the general field of mobile forensics. Responses were analysed thematically, and used as a comparison to results found during the examination of current course offerings collated in stage 2.

The interviews in stage 4 focus on identifying further insight into course packages, educator experiences and engagement with law enforcement. Interviews were transcribed and analysed to capture the interviewee perceptions and experiences. The interviewees' level of experience varied across law enforcement, education establishments and the wider mobile forensic community. The number of courses offerings by each provider ranged between 5 and 40 occurrences per year with some providers having up to eight courses on their portfolios. Courses were typically described to run with a maximum number of 12–15 students. Interviewees recognised that their customers were predominantly law enforcement and were, for example, digital/mobile forensic specialists or analysts.

3.1. Limitations

A particular limitation of stage 2 is the limited information which can be obtained from course descriptors. The largely broad nature of the course coverage allows for little definitive identification of omissions across current offerings in the field. While this limitation is not unfamiliar, it does pose problems in identifying content and depth of mobile forensic courses. In addition, due to access issues this research was limited to the collection of university and commercial studies where in-house training within law enforcement agencies was not considered. While there are limitations with the data collected, this paper argues that the information obtained from the 90+ courses allows for a broad picture of the gaps across education and training solutions to allow for the identification of novel areas for curriculum development aimed at training a range of stakeholders in law enforcement. Another limitation caused by the lack of information from course descriptors, and/or programme specifications, is the lack of details for the depth of the course content, and advancement of topics within each course. Consequently, this reduces the ability of external researchers to examine the content based on the duration, level of advancement and materials, and cannot extend to the pre-knowledge of course participants.

4. Results

4.1. Courses

Firstly, this research looks at the current status quo of education and training courses in the field of mobile forensics across over 30 countries. Of the 94 courses considered in this research during stage 2 of the method (access to freely available materials) the majority were classified as either acquisition, or acquisition with a limited level of analysis included, based upon course information collated including descriptors and where content was available (as depicted in Table 1).

Category	Education	Training	Total
Acquisition	19	30	49
Analysis	12	11	23
Acquisition + Analysis	4	9	13
Various Phases	2	2	4
Acquisition + (Analysis + Reporting)	0	2	2
Acquisition + Analysis + Presentation	0	1	1
Acquisition + National Legislation	0	1	1
Reporting	0	1	1
Total:	94		

Table 1: Table of Courses at first glance categorised by descriptors and course information

These results show that there were 37 educational courses and 57 training courses identified. Categorisation during early stages of course analysis indicated a total of 49 courses which covered the phase of ’Acquisition’. Acquisition included four categories: acquisition with limited analysis ‘Acquisition (Analysis)’; acquisition solely ‘Acquisition’; advanced acquisition ‘Acquisition – advanced’; and, a broad course with attention on acquisition ‘Broad (Acquisition)’. 13 courses focused on Acquisition and Analysis together, while 23 courses in total focused on aspects of Analysis.

More in-depth analysis of the course descriptors and content through thematic analysis shows that topics in relation to analysis, acquisition, automation and networking were categorised the most by the number of codes (i.e. the number of individual keywords that belong to categories/themes), as described in Table 2. However, important topics using the total number of occurrences for all codes in each category (sum of appearances of all codes in a category/theme) demonstrate that acquisition followed by analysis are most prevalent in the current courses available. Looking into the results further, topics which were rarely thematically coded across the available courses, and found to be particularly interesting were: networking fundamentals and mobile network forensics; IoT, wearables, drones, small-scale devices; encryption and decryption; aspects of the cloud in acquisition; crime scene; visualisation; and, evaluation.

Networks consist of 60 codes with a total of 183 occurrences. Even though the mobile phone device has evolved into a powerful pocket computer, connectivity depends on cellular networks, with telephony and messaging remaining as core elements of mobile phone services. We found relatively light emphasis on cellular telecommunications systems, with obsolescent 2G technologies such as GSM and IS-95 continuing to feature. Mobile phone content analysis has evolved in the computer forensic domain, yet telecommunications network billing records and lawful intercept capability remain critical in investigation.

Category	Number of Codes	Total occurrences of Codes
Analysis	173	644
Acquisition	146	948
Automation	64	195
Network	60	183
Security	56	152
Forensic Readiness	46	239
Investigation	39	188
Devices	35	124
Regulative	24	86
Decryption	24	87
Development	24	37
Integrity	24	62
Challenges	20	38
Identifiers	17	104
Communications	16	82
Operating Systems	15	207
Preservation	14	58
Documenting	12	66
Extraction	9	63
Crime Scene	9	48
Evaluation	5	19
Visualisation	3	8
Encryption	3	3
Metadata	2	7
Framework	2	21

Table 2: Table of Categories and total occurrences of all codes per category

Decryption techniques and fundamental knowledge of encryption become essential within the role of a law enforcement data specialist. With the number of devices and manufacturing companies adopting security hardening techniques, it becomes difficult to be able to always acquire the data from devices, in particular mobile devices. Encryption was categorised on 3 occassions, consisting of just 3 codes. In comparison, decryption consisted of 24 codes with a total of 87 occurrences. This is interesting as these techniques are arguably a struggle for the discipline. The limitation of this is that both training providers and educational establishments may provide separate courses focusing on encryption and decryption, often together, in theoretical or practical depth. However, these courses may not be contextualised for mobile forensics and may not focus on how to circumvent mobile device hardening, or utilise the volatile memory of mobile phones in order to identify decryption keys. This may suggest a gap. Some of the reasons for this may be the technical complexity, knowledge and skills necessary, and competence required among a range of stakeholders.

Thematic analysis also demonstrated that cloud forensics was not always mentioned in course descriptions for the courses considered. In fact, aspects relating to “Cloud” often focussed on acquisition, and only accounted for 28 occurences, including codes such as ‘cloud’, ‘iCloud’, ‘cloud security’, ‘cloud forensics’ and ‘DJI Drone Clouds’. There are many reasons why cloud forensics may often be overlooked in course descriptions. One reason may be that the complex nature of such acquisitions make it difficult to comprehensively cover the topic within course time frames, as well as challenges involving logistics and access for trainees [27]. Another reason may arguably consider the variety of legalities surrounding obtaining and utilising cloud data sources across jurisdictions. In some countries the use of cloud data is restricted to ensure protection against unreasonable search and seizure [6]. In addition, courses mentioned the crime scene within descriptors on few occasions. Codes such as search (12), evidence handling (10), bagging (3), tagging (9), collection (5), incident response (5), and crime scene (4) were categorised under the theme crime scene. It may be said that the crime scene was focused on more in educational courses than training courses.

Visualisation was another theme which was covered less across course materials. Topics such as geotagging, triangulation and correlation were grouped into visualisation. What is interesting is that while analysis has a high number of occurrences, and investigation has just below 40, visualisation is not mentioned in-depth within course descriptors overall. Furthermore, evaluation was categorised on far fewer occasions, where this category included, for example, court and courtroom testimonies, explanations, and justification. This may also indicate that audiences such as investigators and prosecution are not ideally covered, as mentioned in previous literature dating back to works as early as 2012 [2] in section 2.4.

4.2. Questionnaire

To supplement the online research conducted, a questionnaire sent out to educators and trainers within the digital forensics field was circulated, with 27 responses, of which 21 covered aspects of mobile forensics. This section highlights some of the results relating to curriculum standards, and the skills shortages identified among respondents.

4.2.1. Standards, Frameworks, or Certifications

As previously described in Related work and contributions there are many standards, procedures and best practice guidelines relating to digital and/or mobile forensics [4, 11, 21, 35]. Furthermore, there are several frameworks and standards relating to education and training across many disciplines. Participants were asked which international standards, frameworks or certified industry bodies the courses followed, if any. Only 33% (7/21) of the courses followed an international standard, framework or were certified by an industry body. These included:

- two respondents that followed the ACPO (Association of Chief Police Officers) guidelines, and one of these followed the ISO 27037 (guidelines for specific activities in the handling of digital evidence) and part of ISO 17025 (general requirements for the competence to carry out tests and/or calibrations, including sampling);
- one respondent that followed the ISO 27001 (Information Security Management System);
- two respondents who referred to the NFQ (Irish National Framework of Qualifications) level 9 (Master's degree) or certification by BCS (British Computer Society); and
- two respondents who referred to tool certifications (Cellebrite, Paraben).

There were no unified practices in utilising standards, frameworks, or certifications for mobile forensic courses. Most (67% of courses) do not utilise any standard, framework, or certification.

4.2.2. Skills shortages

To identify the current status of mobile forensics education and training participants were asked to express, based on their own experiences, skills they felt were absent in the field of mobile forensics. The respondents identified several skills shortages which have been themed into four categories (Table 3). The skills shortages which resonated among these responses highlighted gaps in every aspect, for example, the lack of basic knowledge, generic skills in forensics and investigation, lack of skilled practitioners and necessary mindsets to critically think, investigate and avoid dependency on the tools.

Category	Skills shortage
Forensic Readiness	• Tool testing is missing, because of not enough time • No in-depth knowledge • Lack of trained/skilled officers in using industry standard tools • No practical knowledge about flash boxes, JTAG, In-System Programming, Chip-off, Faraday Isolation • Lack of experience in Mobile forensics • Lack of awareness of Apps not found by the tools • Motivations and mindsets
Automation	• Tool dependence/single tool dependencies • Too much trust in the tools, do not dig deeper • Focus on tool forensics • Lack of programming skills • Not using open source tools • Do not validate the tools
Analysis	• Interpretation of complex digital evidence is missing • Integration of phone and network evidence is missing • Ability to correlate data with user actions is missing • Analysis of raw data (hex level) is missing • Lack of understanding of the limits of data
Investigation	• Lack of investigative skills • Lack of understanding for the mobile forensic examination process • Lack of understanding of OS/Computers, weaknesses, and that malware can leave traces similar to user activity

Table 3: Table of skills shortages from educator/trainer questionnaire respondents

4.2.3. Important Topics

In addition to skills shortages, educators and trainers alike felt there were issues and important topics within mobile forensics. Questionnaire respondents were asked to consider and list the three most important topics for mobile forensics content. Based on their responses several keywords were identified, using thematic analysis. Figure 1 (below) demonstrates the responses themed into several categories, where Analysis, Investigation, Acquisition and Forensic Readiness were considered most.

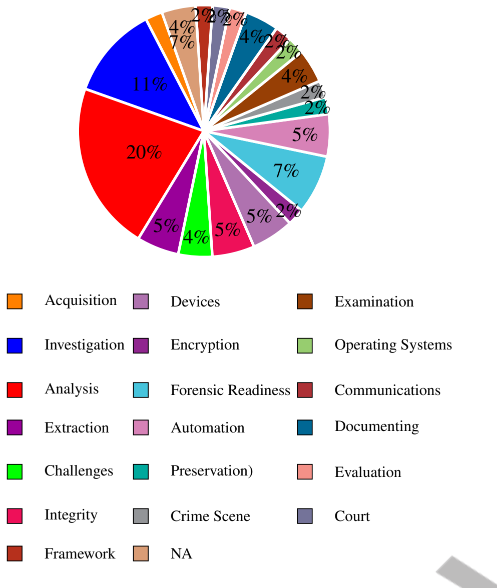

Figure 1: Important Topics Themed from Questionnaire Responses

4.2.4. *Learning Outcomes highlighted in the Questionnaire*

Respondents were asked to separate the learning outcomes into three distinct categories: Knowledge, Skills and Competence. Each learning outcome was coded by keyword and themed into several categories, similar to those created during the open coding (i.e. analysing textual content and labeling concepts, defining and developing categories based on properties) of course data from stage 2. Results show the category *Analysis* as the key focus among the defined learning outcomes, depicted in Figure 2. This demonstrates that of the 21 providers covered by respondents most feel analysis is important and potentially a key aspect of their courses. What this study cannot verify is the depth of analysis which is conducted in these courses. This result is particularly interesting as the authors of this research found courses considered during data collection to be categorised, largely, with the focus on acquisition. However, results show that acquisition, although the second highest category based on themed learning outcomes, has far less attention across the knowledge, skills and competences described. These results show how broad and vague course descriptors and learning outcomes can be when analysing course content and identifying the status quo.

4.3. *Interviews*

Information obtained from the interviews and analysed during this research are outlined in this section. The focus of the courses outlined by those interviewed were training oriented and directed at acquisition and analysis phases within mobile forensics. Courses were split between theory and practical, however, all respondents noted that practice and hands-on approaches to training were essential in the field, so materials adopt this precedent. Courses were identified to cover a range of topics and include examples such as: the fundamentals of mobile forensics, acquisition (including advanced methods using chip-off and JTAG), SQLite and app analysis, encodings, tools and automation, awareness of standards and legislation, documenting/reporting, and less frequently the crime scene.

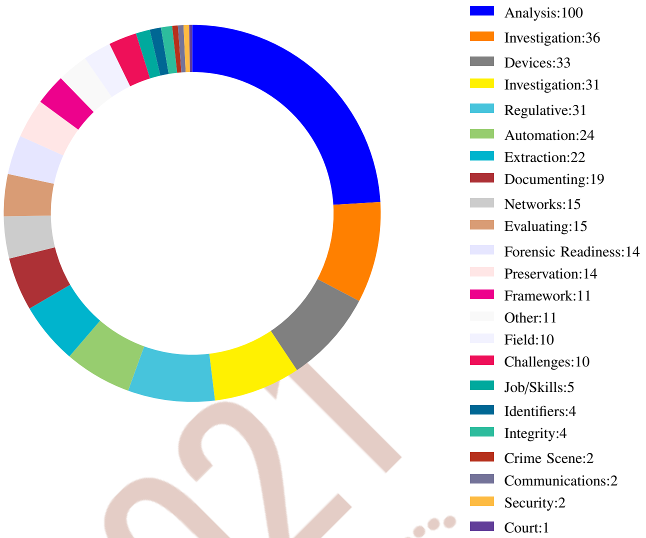

Figure 2: Learning Outcomes Themed from Questionnaire Responses

4.3.1. *Challenges identified by interviewees*

There were a number of challenges identified by the interview respondents that can be observed among five themes demonstrated in Table 4 prior to presentation and analysis below.

Keeping up-to-date:
"It is a fast moving field after all" . . . Challenges discussed included keeping up with cutting-edge technology, software and hardware updates, operating systems, telecommunications, and more generally the field of mobile forensics. Interviewees discussed that it is not only the challenges associated with the technological developments, but this includes the turnaround by consumers for the latest devices, in particular criminals. These issues have to be accounted for within the field (e.g. abilities of the tools) and within the relevance and currency of the education and training offerings available.

When asked how they keep the course training materials up-to-date, all responded with the need to keep abreast of changes, challenges, community discussions and platforms, forums and stakeholder needs. As one interviewee states: "absorbing what is going on, and hopefully consuming it well". The interviewee continues to note "that is a very good question, and it is a big challenge". Each provider interviewed expressed that they regularly update training materials for several reasons including customer needs, feedback and requirements, new technologies,

Theme	Key Points
Keeping up-to-date	• It is a fast paced field/environment • Need to keep abreast with challenges, technologies, advancements, stakeholder needs and so on • Specialisms and skilled educators/trainers required • Continual update of course materials and exercises required
Legislation, standards, principles and procedures	• Lack of standard procedures, principles, legislation, and can differ in every country or across jurisdictions
Awareness and education	• Challenges e.g., large volumes of data, acquisition and extraction, pressures, financial restrictions, training opportunities, and differences across jurisdictions • Education for the wider criminal justice system, including managers and senior officials • First responder abilities/understanding of how to handle mobile devices • Lack of focus on investigators • Little education for lawyers, prosecution and judges for the importance of digital evidence
Tools and automation	• Need for tool agnostic approaches • Balance required between automation and awareness/education • Requirement for understanding what, how, why and not just push-button approach • Practitioner mindset and motivations • Highly skilled practitioners tend to solve the problems on their own and require less training
Security, Encryption and Advancing Technologies	• Challenges getting hold of the data from devices • Security hardening • Future data access problems (e.g. no data ports) • Features which work against law enforcement motivations to reduce and fight crime • Techniques such as Triage may become essential

Table 4: Table of themes among discussions with educators/trainers in interviews

new applications, various challenges, research and development which law enforcement may be unable to be involved with, and more. The fast pace and change of the field also meant that trainers felt the materials were often updated on each offering of a course, not only to suit customer requirements but also due to the continual shift and development within the field and the research surrounding mobile forensics. One trainer also goes as far to say that they "have never started a class and finished it with the same slides" and depending on the class they may change content "as people give [them] new information or ask good questions". Interviewees also touched on the need for experienced trainers, they were often people with experience working, or having worked, in the sector and maybe with involvement in other related projects. One interviewee notes that materials in the field such as "books may be valid for 6 months to a year, maybe", while another notes that the "fast pace of change and fast changes of updates" add to the challenges of keeping materials up-to-date. One trainer expresses that it is challenging particularly when you have multiple courses on offer which you must keep up-to-date, identifying the need to keep "time outside the classroom . . . to keep updates live and the devices up-to-date", likening the process to "balancing plates on sticks at a circus" and being in the "arena [and] committed to going at a certain speed on a treadmill".

Legislation, standards, principles and procedures: Another issue mentioned in section 4.2.1 are the lack of standards and procedures internationally within the field. Two of the participants touch upon this identifying that it is "very difficult to teach [these] as every country will have their own legislation and their own procedures and standard operating procedures". One trainer acknowledging that standard operating procedures and processes can be different among teams and forces within one country, let alone internationally. Arguably, this may often lead to fragmentation within the field. The trainers interviewed identify how they discuss the standards, guidelines and procedures but do not prescribe a specific legislation or standard that practitioners should follow, as one may be less relevant for another depending on the country. Instead, interviewees express how they try to make sure that basic courses cover for example, "handling evidence of digital evidence, proper procedures, first responders, and analysis, as well as identification of devices", and more intermediate and advanced courses focus on extraction and analysis.

Awareness and educating the wider criminal justice system: As described in section 2 there have been cases made that there is little education for lawyers/prosecution and judges on the significance of digital evidence in an investigation. One interviewee notes that awareness and education are one of the biggest challenges for the field. Interviewee responses particularly focus on educating the wider audience in the criminal justice system to:

- "understand the evidence and data . . . that can be of significance, its reliability and how to work with it" e.g. prosecution, lawyers, judges, and investigators
- the abilities to "pick up reports, understand them and analyse them, search and filter [and so on]" e.g. the investigators ability to handle and understand the data extracted - "those people are poorly provided for at the moment"
- addressing and managing peoples' expectations (e.g. managers and senior criminal justice levels) and the issues/ pressures placed on practitioners to clear a specific number of phones at a sufficient rate
- focus on the awareness of managers and the need for them to consider the potential risks associated with pressures placed on practitioners to get through the data/cases quickly, against the need to capture all necessary and relevant data
- wider organisational awareness of the costs and benefits associated with keeping up-to-date with the field, spending money on the resources required to fulfil the tasks (e.g. funds for licenses, training, people, equipment, time etc.) - "it is the mindset that is the problem"

- wider organisational awareness to the importance of digital evidence in all criminal investigations and people's roles and the skills involved in performing these roles and tasks

One interviewee recognises the opportunity and their position to provide training to those stakeholders currently unaccounted for. The interviewee, however, notes "it is just a case of making it happen, particularly when there has not been training of that kind". In addition, the trainer recognises there are challenges with bringing something new to the market especially where people may not recognise they need such training. The interviewee felt that they could not state there was "a widespread acceptance of the fact that other people within the organisations need training and education on how to deal with digital evidence necessarily, but we [the field] will get there". While, for example, funding may not be an issue for all nations, something all interviewees note the field suffers from includes how to get the data off of the devices, and issues with extraction, which may highlight why courses examined in this research focus on acquisition with some analysis.

Tools and Automation

The trainers interviewed mentioned they were tool agnostic. This means that they are not promoting one particular tool over another and are using the necessary commercial and community driven projects that may be sufficient for specific tasks, and those utilised by law enforcement. Interviewees however mentioned the use of commercial tools suggesting that there needs to be a balance between automation, awareness and education. This is not a new debate in the field and has been something of caution in the general field of digital forensics where authors such as, James and Gladyshev [22] have mentioned the shortfalls of push-button forensics. While other authors such as Casey [7] note that one challenge of smartphones is that they are UNIX-based, when most practitioners have experience with Windows systems and data structures. One trainer states that in the field there are "very powerful toolkits which try to present practitioners with data in mobile phones in a simplified way, and always the same way". The interviewee expresses that this dampens the awareness of practitioners for how the data is stored, and when the "toolkits might not show the reality, or might be a bit wrong". Trainers identified that they want their customers to, for example, "keep an open mind, and be trained to recognise how data is saved and how it is to be correctly interpreted, and to be on the lookout for data that are not presented the right way or data they may be missing". A common theme among trainers was an in-depth understanding of 'how', 'why' and 'what', with manual techniques and a focus on providing solutions when the tools cannot (e.g. unsupported apps and the use of SQLite). One interviewee states that most often you cannot "devote someone who is very knowledgeable and knows how to do this all manually as it is very expensive" so the field must rely on community and commercial tools. Nevertheless practitioners should possess the fundamental understanding and be aware that "automated tools . . . have their place" and that they are necessary, but recognising that practitioners need to know what is happening, what the tools do, and what they might have missed at the same time.

Security, Encryption and Advancing Technologies

One of the issues all the interviewees agree upon is the challenge practitioners have in getting hold of the data from mobile devices. One interviewee states that "every year we have devices that are coming out with encryption which renders some techniques [outdated]". With faster, seamless and default encryption mechanisms, it becomes a big problem for the field of mobile forensics [9]. The trainer argues that the problem may become even bigger with the "potential in the next 2–3 years if Apple release a phone with no ports". The participant highlights that "getting the data will be extremely challenging, and the [security] features will work against law enforcement motivations to reduce and fight crime". Therefore the process of Triage will become more important across law enforcement [25]. Arguably, practitioners and officers will need to have a fundamental understanding of Triage.

5. Discussion

5.1. Course Coverage

There are limitations to the methods used to categorise the courses collated during information gathering such as, the broad nature of course descriptors, titles, and learning outcomes. However, this research highlights that the limitation of concentrating solely on mobile forensic courses or modules, may lead to misinformation in addressing the crime scene. For example, some university courses in digital forensics include a module which concentrates on the crime scene and forensics, and examples like this are not included in this course analysis.

In addition, mobile technologies and communications were identified to be outdated or with little focus on emerging technologies. Legacy mobile forensics, with the emphasis on mobile connectivity through bluetooth, wifi, and evolving satellite, 3G, 4G and 5G data connectivity, remains a critical source of evidence to validate timestamps and identify phone location. A modern mobile phone is also the link to a suite of increasingly complex sensors and features, including accelerometry, gyrometry, magnetometry, global satellite navigation, high definition video, fingerprint and facial recognition, increasingly sophisticated microphones, touch screens and near field communications. An extended definition of a mobile phone - a telecommunications device which connects to a cellular network - draws in smart watches, drones, vehicle telemetry, tablets, home automation and an increasingly diverse range of low power sensors. The feasibility of extensive coverage of these devices is questionable, but an awareness of what is in the market and potential for investigation is critical.

This research also indicates that the phase of decision is rarely covered in course descriptors and may be an area where improvements are needed to support a range of stakeholders from first response, analysts and investigators, and criminal justice officials such as lawyers, prosecution and judges. These results cannot conclude that inquiry/investigation, evaluation and decision phases are not ever included in course content. However, the data can infer they are likely not the fundamental underpinnings to course directions. In most cases the focus is acquisition and analysis.

5.2. Questionnaire

What is interesting about these results are the associations which may be made with the skills shortages identified by academic/trainer responses. 21 respondents to the questionnaire identified several skills shortages within the categories of forensic readiness, automation, analysis and investigation. Focusing on the skills shortages presented within the categories of analysis and investigation, the work package argues that courses may not include, or there are not enough, personnel attending relevant training which cover issues such as: interpretation of digital evidence; network evidence; raw data analysis; data limitations; investigative skills; processes, methodologies and standards; and, mobile forensic fundamentals.

Additionally, there were no standards, frameworks or certifications that were widely adopted across course offerings. This is not uncommon for the field, and has been discussed using literature in section 2. These are often based on the country in question, the processes and procedures adopted, and other challenges.

One must consider here that the skills shortages described by participants may be biased due to trainer experiences of courses delivered at beginner's level, since 11 of the course analysed were beginner or bachelor's courses. Three courses were at master/postgraduate level, which should also be considered as beginner level in mobile forensics. Only four respondents identified courses targeting explicitly intermediate or advanced levels. The three remaining courses were targeting all levels, which we assume is applicable for participants describing multiple courses.

5.3. Themes across Interview Participants

Interview participants highlighted several challenges within the field of mobile forensics for both practitioners and educators. These included challenges with technological advancements such as security hardening, resourcing (funds, people, time, skills), and challenges with acquiring data from a range of devices.

As identified by both the literature in section 2 and interview participants in section 4.3, digital forensics, and more specifically mobile forensics, is costly. Costs attributed include not only the cost of having multiple tools, but the installation, updates, cables and even the staff resources required. In addition, keeping up-to-date with all these as well as the everyday challenges of investigations and the advancing technologies can be a heavy burden and expectation. Particularly in a discipline which, according to educators and trainers, suffers from a lack of awareness and lack of skilled practitioners. Furthermore, these same challenges are identified by educators and trainers in the sense of keeping up-to-date and providing life-like and relevant courses. Arguably, as the field relies more on automation there may be greater requirements for tool validation to ensure efficiency and quality. However, in order to validate the tools and results data specialists and investigators need the fundamental knowledge on how the tools retrieve data artifacts, where these artifacts have been retrieved from, and how they should be interpreted using scientific methods Where possible, discussions should include the need for setting up experiments to define and test hypotheses.

Security hardening such as encryption methods are often implemented in modern day mobile phones from first use. The user has to do very little during the process and sees benefits by way of privacy. Although, such techniques have consequent negative effect for law enforcement when fighting serious crime [23]. While streamlined into devices, the process for acquisition is made far harder and less streamlined than before. This requires expertise in areas, where even commercial tool offerings suffer to provide means of getting to the data. This is good for privacy, but may be a real challenge when investigating serious crime.

In addition, a big problem identified pointed to the issues with wider awareness and education of mobile forensics across several stakeholders. These stakeholders include first responders, investigators, managers, and law officials. One stakeholder group within law enforcement who arguably are not addressed are investigators. As discussed in section 4.3, they play a critical role in the chain of an investigation, and it is essential that they understand digital forensics, mobile forensics, the data, techniques and methods, as well as analysis of the findings. Furthermore, there are other stakeholders within the criminal justice system that should require an understanding of digital data. These include the prosecution, defence lawyers and judges who currently lack training in assessing the evidential value of digital data [29, 10, 34, 2], and also how to assess if forensic methods are based on scientific principles. It also includes management in law enforcement to ensure that digital forensic/mobile forensic units are supported not only by funds, but also through realistic expectations and demonstrable awareness. Such awareness includes what these digital forensic roles entail, the skills required, and the time necessary to allow for validation, verification and accuracy. Moreover, first responders (i.e., those who attend the crime scene and identify the potential evidence [1, p. 19]), also require training to educate and provide awareness of not only how to identify potential sources, but how to handle the devices and how to ensure chain of custody. This research has identified that, while some of these areas (e.g. crime scene, analysis, inquiry/investigation and the role in court) are covered within some courses, be it education or training, the extent to which they are covered is unclear. In addition, there were no training courses found to directly aim at stakeholders such as, investigators, managers, or legal representatives, who have particular roles to play in a mobile forensic investigation.

5.3.1. Duration and Advancement of Education and Training

Review has demonstrated that courses may not be directed at several stakeholders/personnel within the chain of digital forensic investigations. Consequently, there may be a lack of direction and/or depth of topical content/important phases of an investigation. However, this research must consider that the duration of both training courses and educational packages alike, can effect the advancement of learning on a course and will certainly affect the depth of content included. This research recognises that it is impossible to cover every aspect of mobile forensics with a course, particularly short-term. Thus, the depth of content will differ depending on short-term (i.e. training) and long-term (i.e. educational) programs. This research has found that the courses examined focus heavily on acquisition, and while it cannot be expected that all personnel should have the technical knowledge of the entire mobile forensic investigation process (e.g., first responders, analysts, prosecution etc.), personnel should have at least an abstract level of understanding for prominent topics, processes, and standards. Subsequently, LEAs should allocate more resources to training personnel with the skill-sets through hands-on training, and contextualised for different stakeholder groups.

5.3.2. Mobile Forensics vs. Computer Forensics

Mobile forensics evolved independently from computer forensics around 2000 [12, 18] once it was realised that a personal handheld device held a trove of evidence useful to investigators, including contacts, message contents, and incoming and outgoing call records. Data extraction from phones and SIM cards was relatively easy, and even supported by applications available to the consumer. The forensic process was dominated by artefacts derived from the phone's interaction with the cellular network. But as phones have become computers in the sense of running an operating system and supporting applications installed on device, so too has phone forensics converged and then been swallowed by conventional computer forensic techniques.

Yet, it is often overlooked that a mobile phone is so much more than a computer. It is a deeply personal device, and the data it carries paints a pattern of life which is unique to the owner. Whereas attribution to someone sitting at a computer is difficult, attribution to the owner of a mobile phone, secured biometrically, is a different story. It is a cellular device, interacting with a complex network, which offers ever faster and more ubiqitous coverage. It is a window to cloud services, including streaming entertainment and off-device processing of health data. It is a suite of sensors, carried with the owner, capturing movement, vision, sound, and location. And, increasingly, it includes a diverse range of form factors, from smart wristwatches to drones and vehicle telemetry.

6. Conclusion and further work

This research found that current courses and training in mobile forensics are not covering the crime scene, but are covering acquisition and analysis. The trainers feel they cover analysis the most, but course descriptors yield acquisition as the most included category. The inquiry/investigation may not be covered in depth, and the training/education for prosecution and court (decision phase) is missing. Based on these findings, this research suggests that future mobile forensic specific training offerings need to be expanded to include the complete investigative process, from the crime scene to the court, and include education and training for all involved stakeholders. This includes: first responders, analysts (common and specialist labs), investigators (e.g. those who have to go through the data), lawyers, defence, prosecution and judges, and managers across law enforcement/criminal justice.

This research demonstrates the opinions of some educators and/or trainers, and provides analysis of relevant course descriptions. Future research will look at these results alongside the needs of law enforcement (e.g., lab specialists, investigators and criminal justice officials) to address the mobile forensic training domain. Further work should also consider Cloud forensics, and the uncertainty about the legal regulations. In addition, education and training offerings should look at how to develop content with the pace of emerging technologies and include content relating to network communications and small scale digital devices and sensors.

7. Acknowledgement

This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800.

References

[1] Aarnes, A., 2017. Digital Forensics. John Wiley & Sons, Ltd.

[2] Alva, A., Endicott-Popovsky, B., . Digital evidence education in schools of law 7. URL: http://commons.erau.edu/jdfsl/vol7/iss2/5/, doi:10.15394/jdfsl.2012.1120.

[3] Arshad, H., Jantan, A.B., Abiodun, O.I., . Digital forensics: Review of issues in scientific validation of digital evidence 14, 346–376. URL: https://doi.org/10.3745/JIPS.03.0095, doi:10.3745/JIPS.03.0095.

[4] Association of Chief Police Officers, . ACPO good practice guide for digital evidence. URL: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

[5] Bajramović, E., . Challenges in Mobile Forensics Technology, Methodology, Training, and Expense. International Journal of Economics & Law 4, 35–39. URL: https://www.semanticscholar.org/paper/Challenges-In-Mobile-Forensics-Technology%2C-And-Bajramovic/84aeb8d370e76ff8ff1abce23bd6467264a6147a.

[6] Bjornson, J., Hunter, A., 2016. Mobile forensics for cloud data: Practical and legal considerations, in: 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp. 203–206. URL: https://ieeexplore.ieee.org/document/7906927, doi:10.1109/PST.2016.7906927. iSSN: null.

[7] Casey, E., . Smartphone incident response 10, 1 – 2. URL: http://www.sciencedirect.com/science/article/pii/S1742287613000339, doi:https://doi.org/10.1016/j.diin.2013.04.004.

[8] Cigoj, P., Blažič, B.J., 2015. An innovative approach in digital forensic education and training, in: Bishop, M., Miloslavskaya, N., Theocharidou, M. (Eds.), Information Security Education Across the Curriculum, Springer International Publishing, Cham. pp. 101–110.

[9] Conlan, K., Baggili, I., Breitinger, F., . Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy 18, S66 – S75. URL: http://www.sciencedirect.com/science/article/pii/S1742287616300378, doi:https://doi.org/10.1016/j.diin.2016.04.006.

[10] Erlandsen, T.E., 2019. Fallacies when Evaluating Digital Evidence Among Prosecutors in the Norwegian Police Service. Master's thesis. Norwegian University of Science and Technology. Gjøvik, Norway. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2617771.

[11] European Network of Forensic Science Institutes, . Best practice manual for the forensic examination of digital technology. URL: http://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf.

[12] Farjamfar, A., Taufik Abdullah, M., Mahmod, R., Izura Udzir, N., . A review on mobile device\'s digital forensic process models 8, 358–366. URL: http://maxwellsci.com/jp/mspabstract.php?jid=RJASET&doi=rjaset.8.981, doi:10.19026/rjaset.8.981.

[13] Flick, U., . An Introduction to Qualitative Research. 6th edn. ed., SAGE. URL: https://books.google.co.uk/books?hl=en&lr=&id=o5l7DwAAQBAJ&oi=fnd&pg=PP1&dq=flick+introduction+to+qualitative+research&ots=Jc2x7u0JE9&sig=LbY3PctjLkrRh5jLs39xmNLDRQ0#v=onepage&q=thematic%20analysis&f=false.

[14] Flory, T., . Digital forensics in law enforcement: A needs based analysis of indiana agencies 11, 7–38. URL: http://commons.erau.edu/jdfsl/vol11/iss1/4/, doi:10.15394/jdfsl.2016.1374.

[15] FORMOBILE, . FORMOBILE project. URL: https://formobile-project.eu/.

[16] Garfinkel, S., Farrell, P., Roussev, V., Dinolt, G., 2009. Bringing science to digital forensics with standardized forensic corpora. Digital Investigation 6, S2 – S11. URL: http://www.sciencedirect.com/science/article/pii/S1742287609000346, doi:https://doi.org/10.1016/j.diin.2009.06.016. the Proceedings of the Ninth Annual DFRWS Conference.

[17] Garfinkel, S.L., 2010. Digital forensics research: The next 10 years. Digital Investigation 7, S64 – S73. URL: http://www.sciencedirect.com/science/article/pii/S1742287610000368, doi:https://doi.org/10.1016/j.diin.2010.05.009. the Proceedings of the Tenth Annual DFRWS Conference.

[18] Grispos, G., Storer, T., Glisson, W.B., . A comparison of forensic evidence recovery techniques for a windows mobile smart phone 8, 23 – 36. URL: http://www.sciencedirect.com/science/article/pii/S1742287611000417, doi:https://doi.org/10.1016/j.diin.2011.05.016.

[19] 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. URL: https://linkinghub.elsevier.com/retrieve/pii/S0167404815001595, doi:10.1016/j.cose.2015.10.007.

[20] Hiim, H., Hippe, E., 2009. Undervisningsplanlegging for yrkesfaglærere [Lesson planning for vocational teachers]. Gyldendal akademiske. URL: https://www.gyldendal.no/Faglitteratur/Pedagogikk-og-laererutdanning/Pedagogikk/Undervisningsplanlegging-for-yrkesfaglaerere.

[21] ISO/CASCO, . ISO - ISO/IEC 17025 — testing and calibration laboratories. URL: https://www.iso.org/standard/66912.html. library Catalog: www.iso.org.

[22] James, J.I., Gladyshev, P., . Challenges with Automation in Digital Forensic Investigations , 17URL: https://arxiv.org/ftp/arxiv/papers/1303/1303.4498.pdf.

[23] Koops, B.J., Kosta, E., . Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark" 34, 890 – 900. URL: http://www.sciencedirect.com/science/article/pii/S0267364918302413, doi:https://doi.org/10.1016/j.clsr.2018.06.003.

[24] Kröger, K., Creutzburg, R., 2012. Conception of a course for professional training and education in the field of computer and mobile forensics. Proc. of SPIE Vol 8406, 84060W–1. URL: https://www.researchgate.net/publication/258332911_Conception_of_a_course_for_professional_training_and_education_in_the_field_of_computer_and_mobile_forensics, doi:10.1117/12.923275.

[25] Marturana, F., Tacconi, S., . A machine learning-based triage methodology for automated categorization of digital media 10, 193–204. URL: http://www.sciencedirect.com/science/article/pii/S1742287613000029, doi:10.1016/j.diin.2013.01.001.

[26] NIST, . Mobile device images. URL: https://www.cfreds.nist.gov/mobile/index.html.

[27] NIST Cloud Computing Forensic Science Working Group, . DRAFT NISTIR 8006, NIST Cloud Computing Forensic Science Challenges. National Institute of Standards and Technology, U.S. Department of Commerce. URL: https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf.

[28] NowSecure, 2012. viaExtract bypasses Android lock if USB debugging enabled. https://www.nowsecure.com/blog/2012/03/02/viaextract-bypasses-android-lock-if-usb-debugging-enabled/. Online; accessed 9 March 2020.

[29] Oparnica, G., 2016. Digital evidence and digital forensic education. Digital Evidence and Electronic Signature Law Review 13. URL: https://journals.sas.ac.uk/deeslr/article/view/2305.

[30] Owen, P., Thomas, P., 2011. An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising acpo & nist guidelines. Digital Investigation 8, 135 – 140. URL: http://www.sciencedirect.com/science/article/pii/S1742287611000211, doi:https://doi.org/10.1016/j.diin.2011.03.002. standards, professionalization and quality in digital forensics.

[31] Oxygen, 2020. Oxygen Forensics - Mobile forensic solutions: software and hardware. https://www.oxygen-forensic.com/en/. Online; accessed 9 March 2020.

[32] Paullet, K., Pinchot, J., Mishra, S., 2016. Mobile Forensics and Security Certificate: An Addition to a Cyber Security Degree, in: Information Systems and Computing Education, Las Vegas, Nevada USA. pp. 3587–3593. URL: http://proc.iscap.info/2016/pdf/4059.pdf.

[33] Paullet, K., Pinchot, J., Mishra, S., 2017. Implementing a Successful Train-the-Trainer Program in Mobile Forensics and Security 18, 7. URL: http://www.iacis.org/iis/2017/1_iis_2017_173-179.pdf.

[34] Sanger, R.M., 2018. Forensics: Educating the Lawyers. SSRN Scholarly Paper ID 3303376. Social Science Research Network. Rochester, NY. URL: https://papers.ssrn.com/abstract=3303376.

[35] Scientific Working Group on Digital Evidence, . SWGDE best practices for mobile device evidence collection & preservation, handling, and acquisition. URL: https://www.swgde.org/documents/published.

[36] Skagen, T., Torras, M., Kavli, S., Mikki, S., 2009. Pedagogical considerations in developing an online tutorial in information literacy. Comminfolit 2, 84. doi:10.15760/comminfolit.2009.2.2.60.

[37] The Cyber Academy, 2020. DFET (Digital Forensics Evaluation and Training). ttps://thecyberacademy.org/about/dfet. Online; accessed 22 February 2020.

[38] Tu, M., Xu, D., Wira, S., Balan, C., Cronin, K., 2012. On the Development of a Digital Forensics Curriculum. Journal of Digital Forensics, Security and Law 7, 13–32. URL: http://commons.erau.edu/jdfsl/vol7/iss3/2/, doi:10.15394/jdfsl.2012.1126.

[39] Woods, K., Lee, C.A., Garfinkel, S., Dittrich, D., Russel, A., Kearton, K., 2011. Creating realistic corpora for forensic and security education. URL: https://calhoun.nps.edu/handle/10945/44250.

[40] Yannikos, Y., Graner, L., Steinebach, M., Winter, C., 2014. Data Corpora for Digital Forensics Education and Research, in: Bayro-Corrochano, E., Hancock, E. (Eds.), Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications. Springer International Publishing, Cham. volume 8827, pp. 309–325. URL: http://link.springer.com/10.1007/978-3-662-44952-3_21, doi:10.1007/978-3-662-44952-3_21.