Received: 8 June 2020 | Revised: 8 October 2020 | Accepted: 9 October 2020

DOI: 10.1111/1556-4029.14613

JOURNAL OF FORENSIC SCIENCES

PAPER

Digital & Multimedia Sciences

Inter-regional digital forensic knowledge management: needs, challenges, and solutions

Eoghan Casey PhD | **Anna Zehnder MSc**

University of Lausanne, Vaux, Switzerland

Correspondence
Eoghan Casey, University of Lausanne, Vaux 1015, Switzerland.
Email: eoghan.casey@unil.ch

Abstract

Increasing demand for digital evidence in criminal investigations is driving decentralization of forensic capabilities closer to the crime scene. Law enforcement agencies are struggling to keep pace with technological developments, cybercrime growth, and scientific advances. In federated environments, digital forensic knowledge and practices vary widely across regions. To reduce delays, wasted resources, missed opportunities, mistakes, and misinterpretations, there is a pressing need to balance the democratization of digital forensic capabilities with knowledge management and sharing between decentralized regions. There are multiple forms of knowledge to be managed, including procedural, technical, investigative, scientific, behavioral, crime analysis, and forensic intelligence. In addition, there are multiple knowledge producers and consumers, including police investigators, digital forensic practitioners, criminal intelligence analysts, attorneys, and judges. Knowledge management becomes even more challenging when multiple interdependent regions are involved, speaking different languages. Taking all of these factors into consideration, this work presents an inter-regional knowledge management solution for improving the quality, consistency, reliability, efficiency, cost-effectiveness, and return on investment of digital forensic capabilities. The basis of this work is a community-driven initiative of Swiss regional police authorities. Interviews were conducted with 15 digital forensic units to determine their current knowledge management practices and needs. The results were then generalized into a prioritized set of requirements for inter-regional digital forensic knowledge management that may be applicable in other countries. These requirements were used to evaluate knowledge management platforms, and one was selected. Implementation, operations, and maintenance challenges of an inter-regional digital forensic knowledge management platform are discussed.

KEYWORDS
collaboration, communication, digital forensics, digital investigation, efficiency, IT investigation, knowledge management and exchange, optimization

1 | INTRODUCTION

Any crime can involve technology, and the number of criminal investigations requiring digital forensic expertise is growing rapidly [1]. The increasing quantity, diversity, diffusion, structural intricacy, and complexity of use of digital evidence are making it difficult for practitioners to find the most investigatively useful information [2, 3]. As a result, the quality of digital forensic results is decreasing, and comprehension of cybercrime is diminishing. To meet this growing demand, digital forensic capabilities are being put in the hands of police

Presented at the 71st Annual Scientific Meeting of the American Academy of Forensic Sciences, February 13–18, 2019, in Baltimore, MD.

at the regional level. This decentralization movement enables police to fulfill their immediate investigative needs with little assistance from centralized digital forensic laboratories that have traditionally consolidated expertise. As a result, each situation or problem–solution is isolated to the context of an individual investigation [4]. Isolated practitioners have limited experience, treating each situation as a new problem, even when applicable solutions already exist elsewhere. This isolation reduces sharing of knowledge between entities (knowledge gap), reduces curation of knowledge (expertise spillage), and reduces visibility across cases (repetition blindness).

Although authorities are hiring to meet increasing demands, it is difficult to get already highly trained staff, and novice digital forensic personnel have limited training opportunities and professional courses are expensive. Furthermore, it is not feasible for even experienced digital forensic practitioners to know about all advances in technology, for example, online services, mobile apps, Internet of Things (IoT), and new digital forensic methods and criminal uses of technology. When they encounter a new situation, they might not know about relevant processes or tools that have already been developed and are fit for purpose in that specific situation. This challenge is compounded when criminals make innovative use of technology, resulting in novel digital evidence that requires deeper expertise to recognize and understand. For example, when digital forensic practitioners encounter an investigation involving data concealment or destruction, there is a risk that they will miss important digital evidence [5].

Knowledge management can be defined as a systematic discipline and set of approaches to enable information and knowledge to grow, flow, and create value in an organization. This involves people, information, workflows, enabling tools, best practices, alliances, and communities of practice [6]. It has been well-established that digital forensic practitioners need knowledge management solutions to deal with the increasing quantity, diversity, diffusion, structural intricacy, and complexity of use of technology in crime [2]. Past work on knowledge management in digital forensics has proposed models and systems to support individual investigations [7, 8]. Prior efforts to create a national repository of digital forensic knowledge for law enforcement and intelligence practitioners called National Repository of Digital Forensic Intelligence (NRDFI) encountered significant challenges, including the resources required to keep materials up to date and to restrict access to sensitive materials [9]. This system was created in response to the need to share digital forensic best practices and resources across law enforcement and intelligence agencies. The developers of NRDFI, the DoD Cyber Crime Center (DC3) in collaboration with Oklahoma State University, recognized that involving users in the definition of requirements, design, development, and ongoing enhancement of systems is crucial to meeting user needs and achieving user acceptance [10]. Resources curated in NRDFI included template forms for standard operating procedures, legal and technical guidance, digital forensic whitepapers, specialized tools and scripts, and training videos. Although NRDFI was used by law enforcement practitioners, the platform and knowledge were solely funded and populated by DC3 and lacked contributions from the broader digital forensic community. Digital forensic practitioners value personal trust and are team-oriented so, to be successful, the community must have ownership in the knowledge management solution, which requires a community-based approach. Cultivating community engagement requires persistent outreach and "pounding the pavement" to actively involve decentralized digital forensic practitioners in the creation of a knowledge management system. Furthermore, such a system must take into account the social context of knowledge management. Effective knowledge management must take existing knowledge-sharing practices into consideration, including what is shared and how practitioners interact [11].

Highlights

- Blueprint for establishing forensic knowledge management platforms in federated environments.
- Survey of requirements for inter-regional digital forensic knowledge management.
- Support establishment of general acceptance in digital forensic practices.

Digital forensic practitioners currently rely heavily on conferences, email lists, and Internet searches to learn and solve emerging challenges. Conferences are useful for networking but only for members of the community who are not too busy or resource-constrained to participate, and they are not frequent enough to address all of the time-sensitive problems encountered in each investigation. Email lists are useful for more immediate problems but consist of quick answers that vary depending on who has time to respond and does not support robust knowledge management. Internet searches cannot always be relied on for correct and current information. Although publication in scientific journals is important for advancing the science, there are many types of knowledge that need to be shared more quickly or discretely. This can include handling a new IoT device as a source of evidence, using a particular tool feature, extracting information from a new smartphone application, interpreting information obtained, and investigating new techniques employed by criminals. Some digital forensic units (DFUs) maintain a repository of procedural documents and technical notes containing practical information, but this is not the same as knowledge [12].

There is a pressing need for a systematic solution to this knowledge management problem in digital forensics to reduce the risk of missed or misinterpreted evidence with severe consequences such as dangerous criminals remaining free to commit additional offenses, continued victimization of the organizations and people targeted by offenses, and imprisoning innocent people [4]. An added benefit of knowledge management is the establishment of general acceptance in digital forensic practices, demonstrating that a scientific practice or technical capability has crossed the line between experimental to demonstrable. Generally accepted scientific practices and specialized and technical knowledge are extremely valuable to decision-makers in the criminal justice

system, as demonstrated by admissibility requirements such as those articulated in the Frye test, Daubert standard, and U.S. Federal Rules of Evidence. Establishing general acceptance of a digital forensic method is challenging due to the rapid rate of technological change and the need to develop novel solutions to deal with new types of data sources or devices. A knowledge management platform such as the one presented in this paper can help demonstrate how a digital forensic method has been designed, developed, maintained, curated, and updated, as well as how the method is used by practitioners to treat and interpret evidence. This kind of foundational knowledge is especially valuable in cases involving distinctive datasets/devices or using bespoke methods/tools when "the relevant reliability concerns may focus upon personal knowledge or experience" [13]. Public organizations that provide digital forensic services have the opportunity (perhaps even a duty) to mitigate these problems by systematically distilling and circulating knowledge throughout the decentralized forensic ecosystem [4, 14].

This work advances knowledge management and dissemination among digital forensic practitioners in interdependent regions through a practice-based approach. Specifically, this work details the design and related challenges of an inter-regional digital forensic knowledge management platform called Knowledge and Information Exchange Platform (KIEP). This work takes a bottom-up approach, incorporating interviews with dozens of digital forensic practitioners across Switzerland to gather and prioritize key requirements and engaging DFUs to take ownership of the resulting solution [15, 16]. The results of this work encompass a wide range of issues related to codifying and sharing digital forensic knowledge, including skills, processes, and tools. The aim of defining general requirements for inter-regional digital forensic knowledge management is to help other countries implement such a system. A platform developed by Atlassian called Confluence was selected for implementation. The sustainability of such a consolidated knowledge management platform is also discussed, with mechanisms to motivate digital forensic practitioners to share their knowledge.

2 | VALUE PROPOSITION

Knowledge and Information Exchange Platform is driven in large part by financial factors, including shrinking budgets for training and software purchases. Additionally, KIEP is motivated by the need to improve consistency and quality of digital forensic practices and results. Substantial public resources are being invested to develop digital forensic capabilities to keep pace with the growing number of criminal investigations involving digital evidence. Currently, due to weak knowledge management, there is a significant waste of resources across a federation of independent regions in developing digital forensic capabilities. Effective digital forensic knowledge management within a single organization, and across interdependent regions, can have significant positive impact, including:

- *Do once, benefit many*: Reduce time and cost spent researching and developing new digital forensic solutions by capturing, disseminating, and reusing already developed solutions (reduce duplication of effort—reinventing the wheel).
- *Increase timeliness*: Faster resolution of problems/challenges in investigations involving digital evidence, balanced by forensic-level quality controls and adherence to standards of practice.
- *Retain organization knowledge*: Reduce expertise spillage due to personnel changes (e.g., absence, retirement, and move to private sector) by capturing and disseminating knowledge.
- *Support and reward experts*: Reduce interruption of experts due to responding to frequent questions and requests for assistance. In addition, recognize and reward experts for sharing their knowledge, with the ultimate aim of retaining them as valued members of the organization.
- *Augment training*: Reduce the cost of training new personnel.
- *Mitigate errors and omissions*: Reduce mistakes, misinterpretations, and missed opportunities involving digital evidence.
- *Strengthen results*: Increase thoroughness, consistency, and repeatability of digital forensic results.
- *Improve quality*: Increase overall quality of digital forensic processes and outcomes by ensuring that they abide by standards of practice and thorough treatment of digital evidence to provide trustworthy information of probative value.
- *Demonstrate validity*: Establish general acceptance of digital forensic practices for court admissibility.
- *Situational awareness*: Increased visibility across regions, providing opportunities to detect crime trends and develop strategic solutions to specific crime trends [17].

To realize these benefits, it is necessary to determine what types of knowledge need to be shared and take a practice-based perspective where communication among knowledgeable humans is emphasized and the social context of knowledge sharing is studied [11].

3 | METHOD

Switzerland is a suitable case study to understand the specific challenges for knowledge management involving a federated context. Switzerland has 26 cantons, operating mostly autonomously with different languages. To faithfully capture and reinforce the strengths of such a decentralization system, this study took a bottom-up approach to assessing the needs and gathering requirements across cantons. This study involved structured interviews with 14 out of 26 cantonal police authorities and one city police (15 total), each with different organizational sizes and models, and each with digital forensic capabilities. Small, medium, and large DFUs in both the German- and French-speaking regions were selected to ensure that the results were representative of the most common requirements. These interviews involved 28 members of the 15 participating DFUs, including all of the heads and some of their deputies. It seems that 6 of these practitioners saw themselves more as IT investigators than

digital forensic specialists, but the distinction between these two roles is not always clear.

Question guidelines were prepared in advance to ensure consistency, and some questions were adjusted based on the earlier interviews to gather additional information. One researcher conducted all initial interviews, and a second researcher reviewed responses, and sometimes, follow-up questions were posed to clarify details. The objective was not to conduct a quantified survey but to have an open discussion with the practitioners about their current knowledge management practices and needs. Despite the diversity of size, structure, and expertise across DFUs, the interviews revealed some common high-priority sharing requirements summarized in the following sections.

3.1 | High-priority knowledge-sharing requirements

Language barriers were mentioned by all DFUs, making this the most common challenge. Some DFUs had already purchased or developed capabilities that other DFUs expressed the need for, but did not know already existed within their federated community. Some DFUs stored and shared solutions internally in an ad hoc manner, for example, using Microsoft OneNote, but expressed the need for a more systematic approach knowledge management. Any solution documented within one DFU was isolated, leaving other DFUs to develop their own solutions to the same problems, leading to duplication of effort and potential inconsistencies in approaches and results. In addition, many DFUs expressed similar knowledge-sharing needs, as summarized in Table 1.

On the basis of these challenges, it was decided that a shared knowledge management platform would help increase knowledge sharing and coordination among police and other supporting organizations.

3.2 | What should be shared on the platform?

Digital forensic knowledge can be shared in various ways, including personal contacts, training, mentoring, email lists, online guides, and tutorials, and codified in specialized tools (Figure 1). In this study, compiled outcomes of interviews revealed the types of information that would be most beneficial for sharing and would increase the collaboration. The most basic barrier to knowledge exchange is that the rapidly growing number of digital forensic practitioners in Switzerland does not know each other personally anymore. To overcome this barrier, it would be beneficial to have a centralized repository of contact details and areas of expertise for the various groups and individuals. Even though the world is becoming more digitalized, people working in the DFUs still prefer personal contacts to collaborate between the regions. The ability to search for competencies within each group and the commercial tools they are using, as well as available in-house tools developed within each group, would help identify who to ask whether there are specific questions.

Another basic need is a FAQ (frequently asked questions) and guidelines for frontline police officers and prosecutors, as well as templates for service provider requests with supporting instructions and tools. Investigative guidelines for crime (e.g., questions to ask and information to request) and research findings (e.g., forensic analysis of SQLite WAL files, drones, smartphone apps, P2P, and eMule) would also be very beneficial.

Digital forensic practitioners also emphasized the value of sharing specialized technical knowledge and best practice guidelines for new technology (e.g., mobile devices and Internet of Things). Practitioners also require a shared tool repository which is easily searchable, as well as tutorials for using specialized digital forensic tools. To avoid the risk of having investigation specific information on KIEP, a separate forensic intelligence system called PICSEL (platform for the analysis of online serial criminality) is being developed to address the high-priority need for case linkage and joint operations [18].

The platform could also facilitate creation of new knowledge. Sharing of effective investigative/forensic practices could lead to new traces being collected which could then lead to traces that could be used in law enforcement investigations. As an example: Fake sextortion demands Bitcoin payment, each case has a small financial impact, so police authorities often do not want to investigate because the damage is too small. However, a correlation of Bitcoin addresses across cases reveals that some cases are linked with an aggregated financial loss that is much larger. This recognition of a larger crime problem could motivate investigations of top offenders, with the goal of determining their identities when they cash out the Bitcoins. Therefore, it is important to inform investigators about new practices, what to collect and correlate to help them construct an effective investigation if such new findings are found. Digital forensic practitioners also indicated that it would be useful for inter-regional meetings to be organized on a regular basis.

It would also help in detecting trends in similar or related cybercrimes in different federated regions, and coordinating nationwide phenomena and to know which authority takes the lead in investigating a bigger phenomenon, so case complexes can be created, and all the related information can be consolidated, increasing the chance of having different investigative approaches that finally could lead to results.

TABLE 1 Common needs expressed by 15 DFUs in Switzerland

Need to educate prosecutors in charge of cases	11/15
Need to obtain information from Service Providers	10/15
Need for case linkage and joint operations	9/15
Need to pool expensive software licenses	8/15
Need to make more effective use of personnel	8/15
Need to contact other digital forensic practitioners	7/15
Need for tutorials/guides to codify knowledge	7/15
Need for programming support/sharing in-house developed tools	6/15

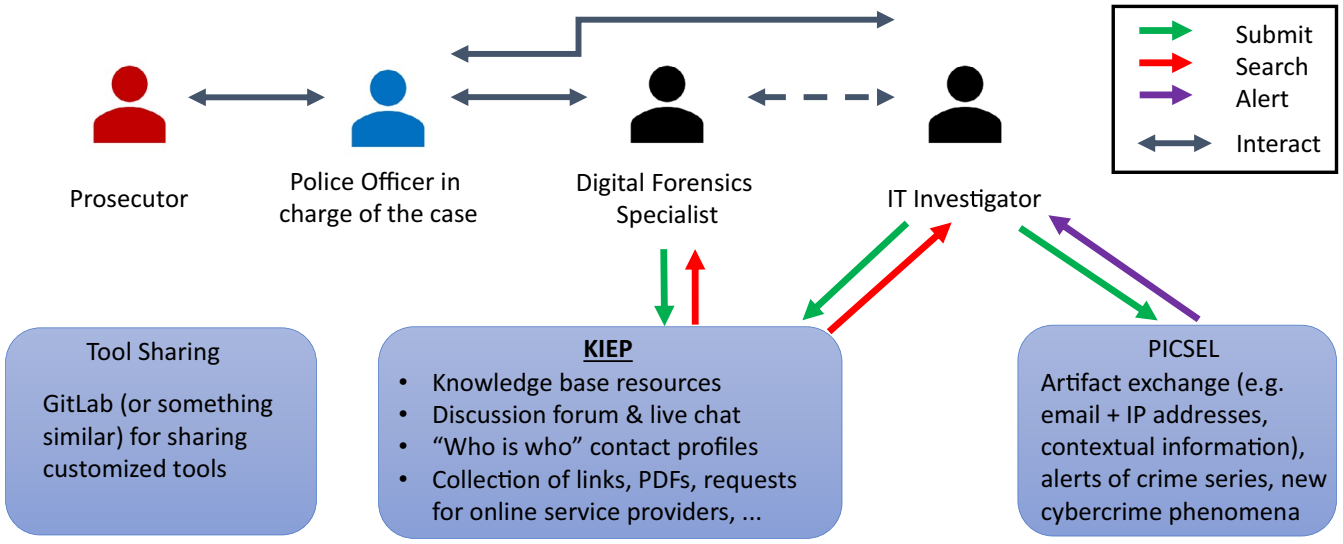

FIGURE 1 KIEP general structure and sharing, linking to PICSEL

3.3 | Knowledge-sharing platform requirements

The requirements and design of KIEP take full account of how digital forensic practitioners currently share knowledge, based on interviews and experience within the social context. In the Swiss federated setting, one of the primary challenges identified was the language barrier between French-, German-, and Italian-speaking regions. Therefore, the platform must absolutely support multiple languages and have a translation plug-in that can be programmed. This could be solved by having an autodetect language function on the browser level as well as translation plug-ins on a page level. There should be individual profiles and group subspaces, which are only reachable for them. There should be a flexible structure, which is intuitive and easy to search. As there is not a lot of budget available, it should be as low cost as possible. Full-text search of PDF and word documents would also be very useful, as it would facilitate injecting knowledge in the platform. If the teams only simply needed to upload their original reports or their work notes, they would do it more often than if they have to respect a certain format or structure.

4 | IMPLEMENTATION AND DEPLOYMENT

In a federated context, the digital forensic knowledge management platform must be flexible, support multi-language interfaces, and be easy to customize, the user rights have to be administrated easily, and it should be as user-friendly as possible. A well-organized yet adaptable structure for controlling sharing between organizations is required as depicted in Figure 2. Each participant, both individuals and groups, has a dedicated virtual space on KIEP with fine-grained access control, enabling them to build reputation and restrict sharing of their resources, that is, with all KIEP members, with select KIEP members, or just within their group.

Regarding the security requirements: The login procedure should be easy, and login should only be possible from certain IP ranges, which should be possible since police authorities often have static IP addresses), via virtual private network (VPN) or a central identity and access management (IAM) solution. In addition, two-factor authentication should also be implemented for increased security. Some of the future users asked for the possibility of having pseudonyms (to not be ashamed to ask "stupid" questions). As it is not needed, no case data should be on the platform, so there should be no problems with personal or sensitive information.

4.1 | Challenges for implementing KIEP

After agreeing on the requirements for digital forensic knowledge management and selecting a suitable platform, there were various hurdles to be surmounted in order to make KIEP viable. There are numerous organizational challenges, as the different police authorities utilize different systems and software. Another identified challenge was the time factor of the implementation, everybody agrees that it would be useful, but discussions about how to implement and who is responsible took over a year. An ongoing issue is money, who pays for the platform software licenses on an ongoing basis. Another major issue that was completely underestimated was who would host the platform. Although it might make sense to host it on a federal level, the legal framework is complicated, and a bottom-up approach was preferred by the regional police agencies as described in the introduction above. Therefore, it was decided that one of the 26 cantons would host the platform, but would not administer the content, which should be done by a "neutral" entity or a federated

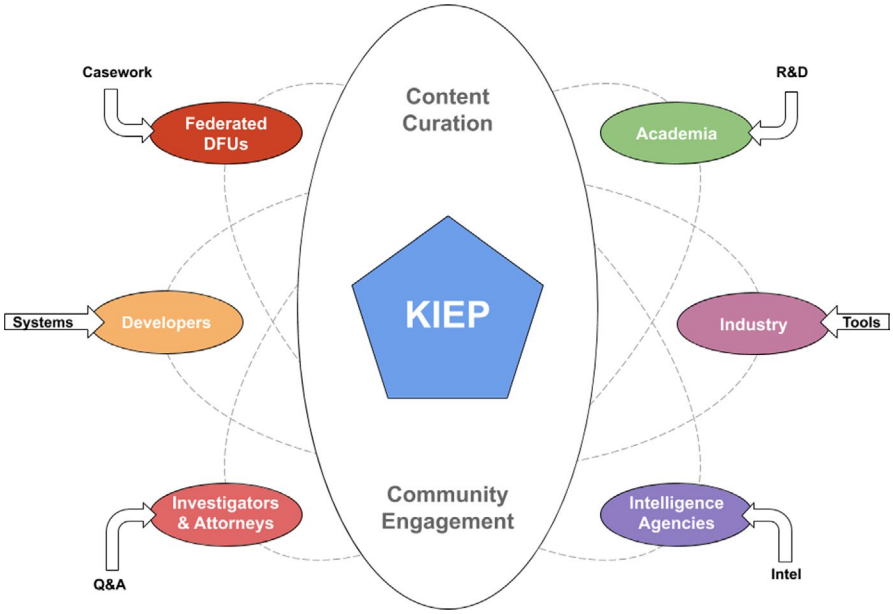

FIGURE 2 KIEP has dedicated virtual spaces within the technology platform for each participant to share digital forensic knowledge in a controlled manner, allowing or limiting access to their areas and resources, however, they decide within their community

network. Although a functional prototype can be deployed, a fully operational solution is not possible until these decisions were made, even if all of the key stakeholders agree that such a platform is required.

4.2 | Platform selection and financing

After some evaluation and trials of knowledge management systems, it was decided to use Atlassian Confluence to implement KIEP. Confluence is widely used across the IT sector to organize and share knowledge and is sufficiently robust and flexible to satisfy the majority of requirements for KIEP. In fact, Confluence is already being used by some participating police agencies internally for different purposes, so they were already familiar with its operation and maintenance.

It was decided that the cantonal police of St. Gallen would host the platform. The ongoing costs of operating and maintaining KIEP were distributed across the participating regions via the inter-cantonal police network to support digital crime investigation and prevention (NEDIK). This cost-sharing model gives participating regions' ownership in KIEP and protects the collective knowledge management activities against disruption if a single source of funding is lost. This approach aligns with the promising practice highlighted in the needs assessment study by U.S. National Institute of Justice involving a national network of regional centers and task forces [3]. In addition, this approach is compatible with the UK tiered approach to national coordination of regional digital forensic capabilities [19]. One exception to this cost-sharing model is involvement of academia, which is essential for bringing new knowledge and fostering workforce development. At a minimum, academic institutions require free access to engage with KIEP and will be more able to contribute if there is some funding for R&D projects.

In May 2020, KIEP was launched and made available to DFUs involved in this initiative to add knowledge and gather feedback, and additional police authorities are being invited to participate.

5 | KNOWLEDGE AND INFORMATION EXCHANGE

In preparation for the development of the fully functional KIEP by the Swiss police, the School of Criminal Sciences at University of Lausanne implemented the system on an internal server. This instantiation of KIEP has become an integral part of daily operations across the organization and provides significant value even on a small scale. Examples from this internal KIEP are provided here to illustrate various aspects of the knowledge management and exchange supported by this system.

5.1 | Curated community collaboration

Knowledge and Information Exchange Platform fulfills the requirement for finding digital forensic practitioners in different regions and organizations with specific competencies and capabilities. Reinforcing this social aspect of knowledge sharing is critical. Each organization has a dedicated team space within KIEP where only their members have access as shown in Figure 3. These team spaces enable organizations to concretize and promote their areas of expertise, to restrict access to certain content within their group, and to share specific information with other members within KIEP.

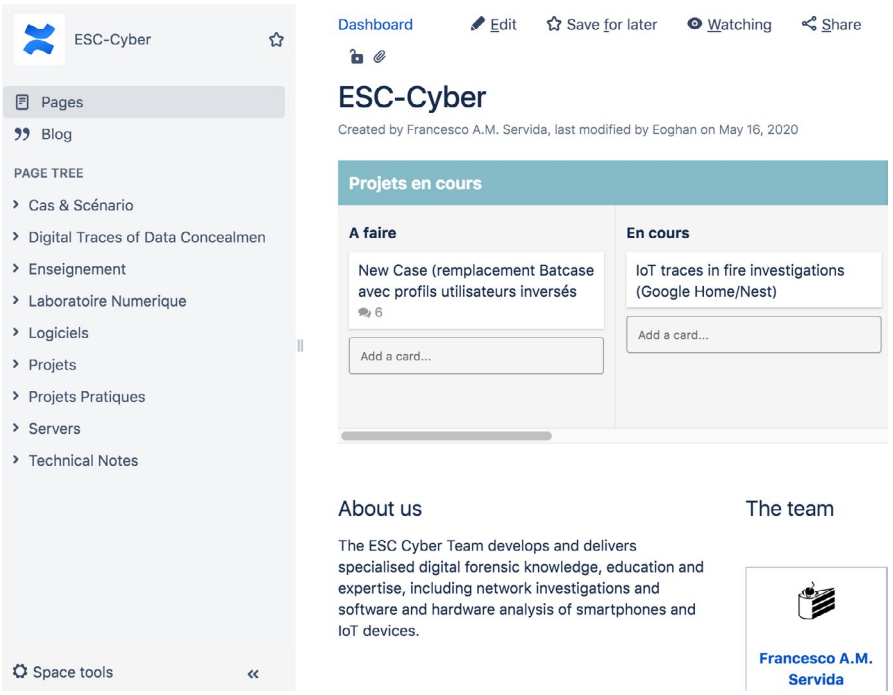

FIGURE 3 Members of an organization or group can define their identity within KIEP and develop their reputation for knowledge exchange in the community

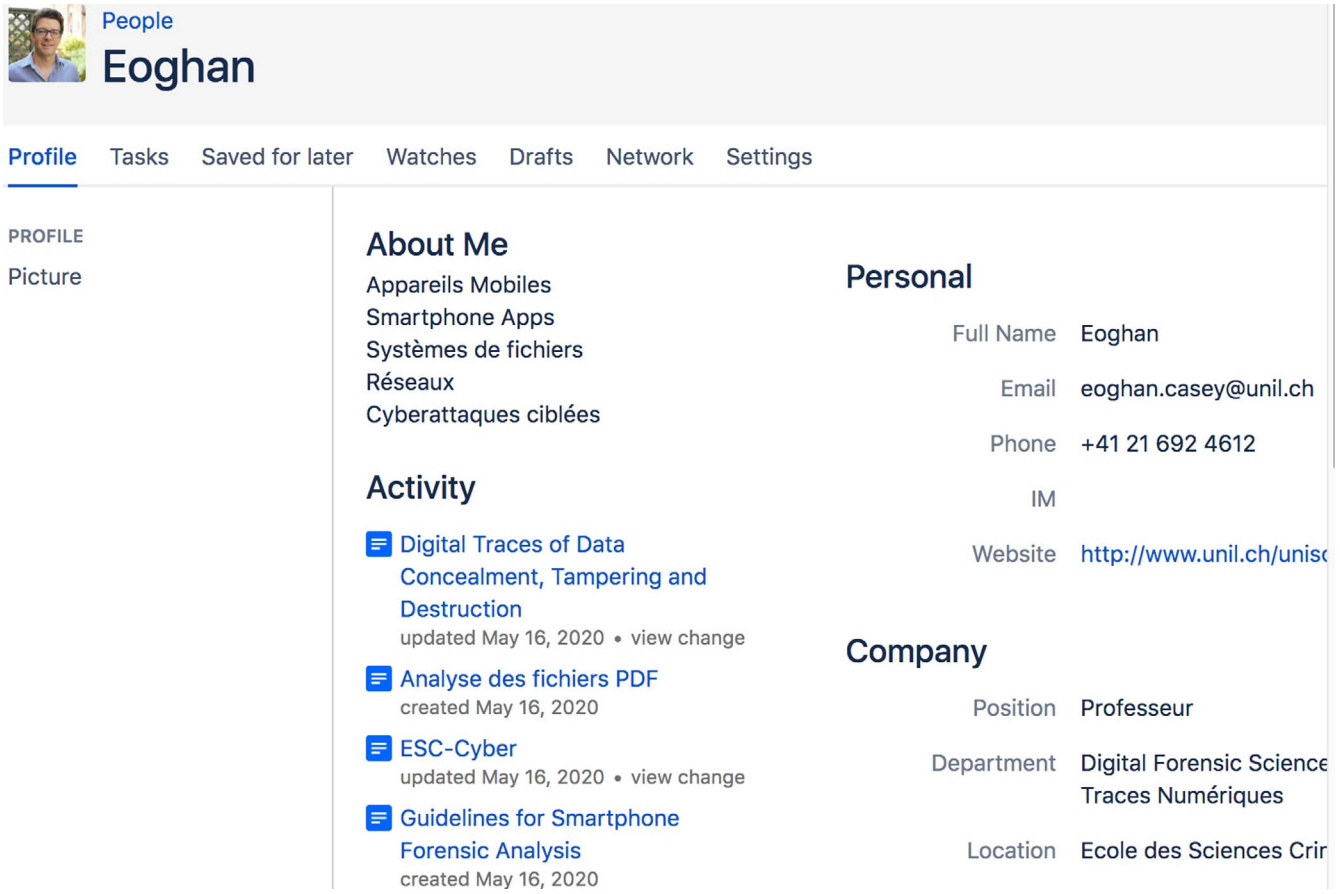

FIGURE 4 Professional profiles enable each member of the community to control their contact details and demonstrate their areas of expertise

Individual members can define their professional profile, providing contact details and highlighting areas of expertise as shown in Figure 4. Confluence automatically organizes the contributions of the individual within the professional profiles with links to the associated content. Other users within KIEP can only access shared content that they have explicitly been granted access to, and all other content is restricted access.

5.2 | Procedural guidelines

Knowledge and Information Exchange Platform fulfills the requirement for collating and disseminating procedural knowledge such as step-by-step guidelines for smartphone forensic analysis and obtaining information from service providers. Separate knowledge-sharing spaces can be organized for specific subjects as shown in Figure 5. Access to these knowledge resources within KIEP can be controlled at the user and group levels. Members from different organizations can be assigned access and responsibility for maintaining a shared resource, thus capturing their collective knowledge. In addition, detailed internal procedural guidelines can be linked with the more general external guidelines maintained by organizations such as the Scientific Working Group on Digital Evidence (SWGDE.org).

5.3 | Technical knowledge

Knowledge and Information Exchange Platform fulfills the requirement for managing knowledge about technical aspects of digital forensic analysis. Content and tutorials dealing with any specialized technical subject can be maintained and updated within KIEP, including analysis of IoT devices, smartphone applications, and digital evidence manipulation (see Figure 6). More basic technical knowledge can be organized within KIEP to meet the needs of different personnel, such as frontline police officers and prosecutors.

5.4 | Tools

KIEP fulfills the requirement for sharing in-house developed tools, providing programming support, and tracking software licenses. Tutorials, links, and license information for specific tools can be managed using individual pages or within dedicated spaces containing multiple shared resources, depending on community demand.

5.5 | Broader impacts

An example of the broader impacts that can result from digital forensic knowledge management emerged from the initial implementation of KIEP. As shown in Figure 6 above, this instantiation of KIEP included collective knowledge about digital evidence concealment, tampering, and destruction. The first version of this shared knowledge resource was specific to Microsoft Windows operating systems, but helped digital forensic practitioners find traces of digital evidence tampering on Linux systems in ongoing casework. The resulting new knowledge was added to KIEP and motivated broader sharing through a presentation at an international conference, which highlights the added value of collaboration between practitioners and the broader digital forensic community, including academia [20].

6 | FUTURE WORK

Knowledge and Information Exchange Platform (KIEP) has been launched by Swiss police with access restricted to participating

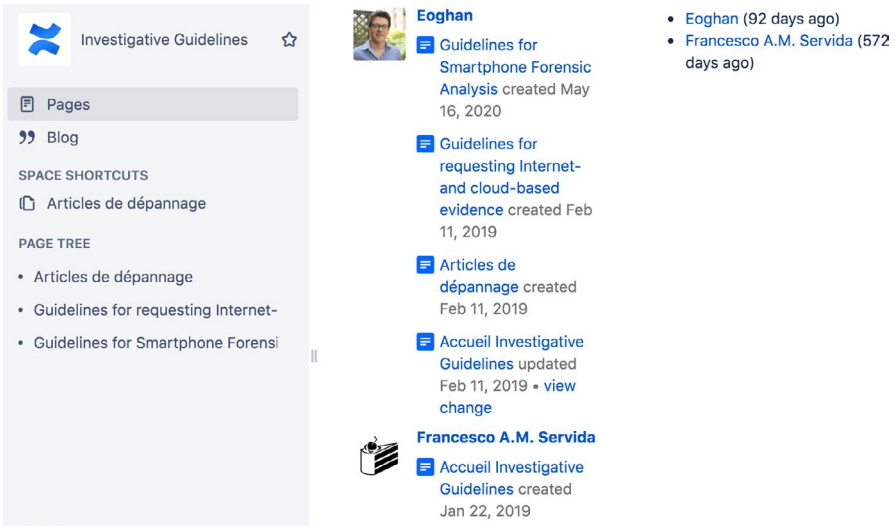

FIGURE 5 KIEP space for investigative guidelines and other procedural knowledge

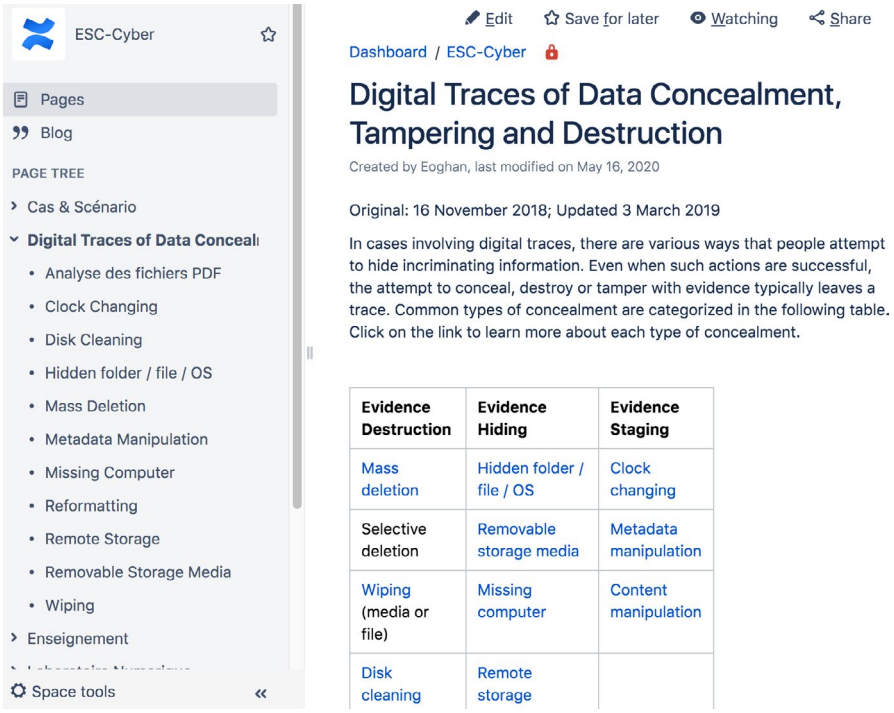

FIGURE 6 Organizing specialized knowledge for performing digital forensic analysis of data concealment, tampering, and destruction

DFUs. As more members join KIEP, including digital forensic practitioners from other government entities, it will be a collective effort to maintain the quality of the content and to update the platform with new knowledge. A general issue with knowledge repositories is incentivizing people to share what they know, which is an area that requires further study [21]. Beyond the recognition by peers and employers, having tangible rewards for significant contributions, such as earning awards or attending specialized training courses, can motivate people to share their knowledge in a system such as KIEP. Further work is needed to study the relative effectiveness of different incentives for motivating contributions to knowledge sharing.

Reviewing, categorizing, and maintaining a knowledge base also takes time, effort, and standards. This process can be made more efficient using modern information retrieval techniques. Existing information retrieval methods can be applied to prioritize relevant information and to downgrade content that is outdated [22]. Involving users in the curation process is critical to maintaining the quality of knowledge in a system such as KIEP. Community-based mechanisms and associated quality/merit badges can be useful for conveying the level of verification performed, such as the three levels provided used by DFIR Review: (1) Methodology Review, (2) Verified Review using Author-Provided Datasets, and (3) Validated Review using Reviewer-Generated Datasets (https://dfir.pubpub.org/review-guidance). Future work includes trying different approaches to assuring quality of knowledge in KIEP, returning most relevant results, and managing stale content.

When new knowledge about a specific source of digital evidence is shared within KIEP, there is an opportunity to capture select details in a standardized form for ease of reference and searching [23]. Such a uniformly structured repository could support automation of digital forensic examinations and tool testing.

The contribution and maintenance of knowledge resources that require consensus such as a FAQ (frequently asked questions) or SOP (standard operating procedure) will require careful coordination. For example, good practices for handling evidence at a crime scene differ from those in a laboratory, and general recommendations must address both contexts. As another example, treatment of mobile devices as a source of digital evidence changes frequently, and guidelines must be updated accordingly. It is necessary to follow a formal process for creating and updating consensus documents. Formal review and approval processes that already work efficiently and effectively in existing collaborative initiatives could be adapted to meet the needs of digital forensic knowledge management.

The broader impact of KIEP could be increased by involving first responders, attorneys, and judges to determine what digital forensic knowledge they require, and then curating specific resources to meet their needs. This would address part of the NIJ Needs Assessment to educate investigators and prosecutors in order to "inform DME requests, increase understanding of the aspects of digital evidence, calibrate expectations, and produce meaningful DME results for developing investigative leads and for court cases." [3]. To reduce the knowledge gap and associated risks of nonspecialists using forensic capabilities outside of DFUs, targeted content in KIEP could be repackaged for convenient access via a smartphone application. In addition to delivering knowledge where and when it is needed, the link between a centralized knowledge repository and decentralized deployments

could be strengthened by observing trends in queries made via a smartphone application connected to KIEP. For instance, if more crime scene investigators are encountering home security systems or smart assistants, this could prioritize development of additional resources to raise awareness and understanding of these systems, their proper handling, and the information they can provide in an investigation.

The collaborative knowledge management activities in KIEP can highlight specific areas that are highly valuable to the broader community and that require more in-depth training or study, which can feed into existing education programs and research projects.

7 | CONCLUSIONS

The system described in this paper has grown from a community of practitioners, in collaboration with academia, to address the ongoing need for knowledge sharing across a decentralized digital forensic ecosystem. Such a system serving a federated community of practice must build on and reinforce the social context of current knowledge sharing. KIEP meets these requirements, promoting collaboration and communication between investigators and digital forensic practitioners in federated environments, and helping them keep pace with new technologies and large quantity of data. This work provides flexible and secure solution for knowledge management that can be adapted to serve digital forensic practitioners in other federated environments to improve the quality, consistency, reliability, efficiency, cost-effectiveness, and return on investment, of digital forensic capabilities. A collaborative cost-sharing model is used to give ownership to participating organizations and protect against major disruptions caused by the loss of a single source of funding.

ACKNOWLEDGMENTS

We thank colleagues in the digital forensics unit of Cantonal Police of Aargau for their support throughout this initiative, especially André Gutknecht for his guidance. We would like to thank all the police agencies who participated in this project with enthusiastic motivation. It is based on their knowledge and experience that this project could be developed, especially René Kully, Hugo Koller, Markus Rüegg and Marcel Mauchle, Steffen Göhrlich, Jonathan Sunier, Steve Christin and Hannes Spichiger, Patrick Rölli, Patrick Ghion, Julien Cartier, Daniel Sémon and Adrian Durrer, Bruno Glauser and Jörg Allenspach, Andreas Rufer and Markus Ruchti, Dr. Alexander Schocker and Martin Graf, Bertrand Schnetz, Gauthier Montavon and Ludovic Stähli, Philippe Roulin, and Antonio Donoso. We wish to convey our many thanks to Francesco Servida for implementing the proof-of-concept platform at University of Lausanne. We also specially thank cantonal police of St. Gallen for hosting the Swiss platform, especially Martin Reut for all the coordination and organization as well as Markus Mächler for his support and knowledge in implementing Confluence.

REFERENCES

1. Casey E. Digital evidence and computer crime: forensic science, computers, and the Internet, 3rd edn. Waltham, MA: Academic Press; 2011.
2. Pollitt M. The hermeneutics of the hard drive: using narratology, natural language processing, and knowledge management to improve the effectiveness of the digital forensic process. PhD Dissertation, Orlando, FL: University of Central Florida; 2011.
3. National Institute of Justice. Needs assessment of forensic laboratories and medical examiner/coroner offices. Report to Congress. Washington, DC: National Institute of Justice; 2019.
4. Casey E, Ribaux O, Roux C. The Kodak syndrome: risks and opportunities created by decentralization of forensic capabilities. J Forensic Sci. 2019;64:127–36. https://doi.org/10.1111/1556-4029.13849.
5. Casey E. Reinforcing the scientific method in digital investigations using a case-based reasoning (CBR) system. PhD Dissertation, Belfield, Dublin: University College Dublin; 2013.
6. Rao M. Knowledge management tools and techniques: practitioners and experts evaluate KM solutions. London, UK: Routledge; 2015.
7. Tanner A, Dampier D. An approach for managing knowledge in digital forensic examinations. Int J Comp Sci Secur. 2010;4(5):451–65.
8. Karie N, Kebande V. Knowledge management as a strategic asset in digital forensic investigations. Int J Cyber-Secur Dig Forensics. 2018;7(1):10–20. https://doi.org/10.17781/P002311.
9. Biros D, Weiser M, Witfield J. Managing digital forensic knowledge an applied approach. In: Valli C, Woodward A, editors. Proceedings of the 5th Australian Digital Forensics Conference; 2007 Dec 3–4; Perth, Western Australia. Perth, Western Australia: Edith Cowan University, 2007.
10. Mathieson K. Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. Inf Sys Res. 1991;2(3):173–91. https://doi.org/10.1287/isre.2.3.173.
11. Ackerman M, Dachtera J, Pipek V, Wulf V. Sharing knowledge and expertise: the cscw view of knowledge management. Comput Supported Coop Work. 2013;22(4):531–73.
12. Alavi M, Leidner DE. Knowledge management and knowledge management systems: conceptual foundations and research issues. MIS Q. 2001;25(1):107–36.
13. Kumho Tire Co. v. Carmichael, 526 U.S. 137, 1999.
14. Casey E, Ribaux O, Roux C. Digital transformations and the viability of forensic science laboratories: crisis-opportunity through decentralisation. Forensic Sci Int. 2018;289:24–5. https://doi.org/10.1016/j.forsciint.2018.04.055.
15. Zehnder A. Systematic management and exchange of digital forensics and IT investigation knowledge between swiss police agencies. Master's thesis, Batochime, Lausanne: University of Lausanne, 2018. https://beast-epfl.hosted.exlibrisgroup.com/primo-explore/search?institution=EPFL&search_scope=all_blended&vid=EPFL&query=any,contains,ebi01_prod011417371. Accessed 9 Oct 2020.
16. Casey E, Zehnder A. Inter-regional digital forensic knowledge and information exchange platform. *Proceedings of the 71st Annual Scientific Meeting of the American Academy of Forensic Sciences*; 2019 Feb 13–18; Baltimore, MD. Colorado Springs, CO: American Academy of Forensic Sciences, 2019.
17. Ribaux O, Crispino F, Roux C. Forensic intelligence: deregulation or return to the roots of forensic science? Aust J Forensic Sci. 2015;47(1):61–71. https://doi.org/10.1080/00450618.2014.906656.
18. Bollé T, Casey E. Using computed similarity of distinctive digital traces to evaluate non-obvious links and repetitions in cyber-investigations. Digit Investig. 2018;24:2–9. https://doi.org/10.1016/j.diin.2018.01.002.

19. National Police Chiefs' Council. Digital forensic science strategy, 2020. https://www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf. Accessed 9 Oct 2020.
20. Casey E, Bollé T, Souvignet T, Polewczyk J, Servida F.Expressing evaluative conclusions in cases involving tampering of digital evidence. DFRWS EU, 2020. http://dfrws.org/wp-content/uploads/2020/06/DFRWS-EU-2020-Expressing-evaluative-conclusions-in-cases-involving-tampering-of-digital-evidence.pdf. Accessed 9 Oct 2020.
21. Hinds P, Pfeffer J. Why organizations don't "know what they know": cognitive and motivational factors affecting the transfer of expertise. In: Ackerman M, Pipek V, Wulf V, editors. Sharing expertise: Beyond knowledge management. Cambridge MA: The MIT Press; 2003. p. 3–26.
22. Dumais S. Better together: an interdisciplinary perspective on information retrieval. *Proceedings of the 2018 Conference on Human Information Interaction & Retrieval*; 2018 March 11–15; New Brunswick, NJ. New York, NY: ACM Press, 2018. https://doi.org/10.1145/3176349.3176571.
23. Casey E, Brady O. Digital trace reference library (DTRL). *Proceedings of the 71st Annual Scientific Meeting of the American Academy of Forensic Sciences*; 2019 Feb 13–18; Baltimore, MD. Colorado Springs, CO: American Academy of Forensic Sciences, 2019.

How to cite this article: Casey E, Zehnder A. Inter-regional digital forensic knowledge management: needs, challenges, and solutions. *J Forensic Sci*. 2020;00:1–11. https://doi.org/10.1111/1556-4029.14613