



## C4 Inter-Regional Digital Forensic Knowledge and Information Exchange Platform

Eoghan Casey, PhD\*, University of Lausanne, Lausanne, Vaud, SWITZERLAND; Anna Zehnder, Unil, Lausanne 1005, SWITZERLAND

**Learning Overview:** After attending this presentation, attendees will understand: (1) the distinct challenges and requirements associated with sharing information and knowledge across digital forensic practices; (2) the scope of digital forensic information and knowledge to be shared; (3) the sharing priorities as expressed by practitioners; and (4) the challenges of establishing a maintainable inter-regional knowledge management system.

**Impact on the Forensic Science Community:** This presentation will impact the forensic science community by revealing a framework for building an inter-regional digital forensic knowledge and information exchange platform that helps fill knowledge gaps by providing digital forensic scientists easy access to needed information. Such a platform also helps stop knowledge drain by capturing solutions in a form that others can reuse in future cases.

Digital forensic capabilities are being put in the hands of individual investigators, enabling them to process evidence with little assistance from digital forensic science laboratories. As a result, each situation or problem/solution is isolated to the context of an individual investigation. This isolation reduces sharing of knowledge between entities (knowledge gap), reduces curation of knowledge and expertise (knowledge spillage), and reduces visibility across cases (repetition blindness). Forensic science laboratories are in a strong position to address these challenges by playing a pivotal role in managing and disseminating knowledge among digital investigators they support and maintaining the quality of forensic results in a decentralized environment.<sup>1</sup>

It is infeasible for a single digital forensic scientist to know about all advances in technology, new methods, and uses of digital evidence. 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 knowledge problem can result in digital forensic scientists missing relevant information or misinterpreting important evidence. Mistakes and missed opportunities in digital investigations can have severe consequences, including imprisoning innocent people, dangerous criminals remaining free to commit additional offenses, or continued victimization of the organizations and people targeted by offenses.<sup>2</sup>

Digital forensic science laboratories have the opportunity (perhaps even a duty) to mitigate these problems by systematically distilling and circulating knowledge throughout the decentralized forensic ecosystem.<sup>3</sup>

This work details the design and related challenges of an inter-regional digital forensic knowledge management platform called the Knowledge and Information Exchange Platform (KIEP). This work takes a bottom-up approach, incorporating input from dozens of digital forensic practitioners in an effort to identify common needs and general priorities.<sup>4</sup> The results encompass a wide range of issues related to codifying and sharing digital forensic knowledge, including skills, processes and tools. KIEP is motivated in large part by the need in digital forensic science to improve collaboration and communication between investigators and digital forensic scientists, and to keep pace with new technologies and large quantity of data.

The sustainability of such a consolidated knowledge management platform is also discussed, with mechanisms to motivate digital forensic scientists to share their knowledge.

The impact of this work includes: (1) saving time and money and increasing the efficiency of processing digital traces; (2) reducing missed opportunities to utilize digital traces + the risk of overlooked evidence; (3) reducing wasted resources (duplication of effort, reinventing the wheel); (4) reducing the frustration of processing digital traces + increasing collaboration; (5) increasing consistency and repeatability of digital forensic results; and (6) strengthening digital forensics with knowledge from forensic science and intelligence.

### Reference(s):

1. Casey E., Ribaux O., Roux C. The Kodak Syndrome: Risks and Opportunities Created by Decentralization of Forensic Capabilities. *J Forensic Sci.* 2019 (In press - <https://doi.org/10.1111/1556-4029.13849>).
2. Casey E. *Reinforcing the Scientific Method in Digital Investigations Using a Case-Based Reasoning (CBR) System*. PhD dissertation. Belfield, Dublin: University College Dublin, 2013.
3. Casey E., Ribaux O., Roux C. Digital Transformations and the Viability of Forensic Science Laboratories: Crisis-Opportunity Through Decentralization. *Forensic Sci Int.* 2018; 289:e24-e25 (<https://doi.org/10.1016/j.forsciint.2018.04.055>).
4. Zehnder A. *Systematic Management and Exchange of Digital Forensics and its Investigation Knowledge Between Swiss Police Agencies*. Master's thesis. Batochime, Lausanne: University of Lausanne, 2018.

### Digital Forensic Science, Knowledge Management, Information Sharing